



KERAJAAN MALAYSIA

**DASAR
KESELAMATAN ICT**
LEMBAGA PEMBANGUNAN LANGKAWI

3 JULAI 2011

VERSI 1.0



KANDUNGAN

TAFSIRAN		6
PENGENALAN		8
OBJEKTIF		8
SKOP		8
PRINSIP-PRINSIP		8
PERKARA 01 : PEMBANGUNAN DAN PENYELENGGARAAN POLISI		
1.1	Pelaksanaan Polisi	10
1.2	Penyebaran Polisi	10
1.3	Penyelenggaraan Polisi	10
1.4	Pengecualian	10
PERKARA 02 - ORGANISASI ICT		
2.1	Pengurus Besar LADA	11
2.2	Ketua Pegawai Maklumat (CIO)	11
2.3	Pengurus ICT	11
2.4	Pegawai Keselamatan ICT (ICTSO)	12
2.5	Pentadbir Sistem ICT	13
2.6	Pengguna	13
2.7	Pembekal, Pakar Runding dan Pihak-pihak Luar Lain	14
PERKARA 03 : PERKAKASAN DAN PERISIAN ICT LEMBAGA PEMBANGUNAN LANGKAWI		
3.1	Perolehan/Pelupusan Perkakasan dan Perisian ICT	15
3.2	Peruntukan/Perkongsian Perkakasan dan Perisian ICT	
	3.2.1 Pencetak	15
	3.2.2 Personal Computer (PC)	15
3.3	Penyelenggaraan Perkakasan dan Perisian ICT	16
PERKARA 04 - PENGURUSAN E-MEL DAN PENGGUNAAN INTERNET		
4.1	Pengurusan E-Mel	17
4.2	Melayari Internet	18
4.3	Laman dan Aplikasi Web	20
PERKARA 05 - SISTEM APLIKASI DAN PANGKALAN DATA		
5.1	Sistem Aplikasi dan Pangkalan Data	21

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	2 DARI 49



PERKARA 06 - PENGGUNAAN DAN PENGURUSAN RANGKAIAN

6.1	Infrastruktur Rangkaian	22
6.2	Pengurusan Alamat IP	22
6.3	Sambungan Rangkaian	22
6.4	Dial-Up dan Rangkaian Tanpa Wayar (Wireless) Internet 3G	23
6.5	FTP	23
6.6	Pengenalan dan Katalaluan	23
6.7	Antivirus	24

PERKARA 07 - KESELAMATAN ICT

7.1	Akauntabiliti Aset	
	7.1.1 Inventori Aset	26
7.2	Pengelasan dan Pengendalian Maklumat	
	7.2.1 Pengelasan Maklumat	26
	7.2.2 Pengendalian Maklumat	26
7.3	Keselamatan ICT dalam Tugas Harian	
	7.3.1 Tanggungjawab Keselamatan	27
7.4	Menangani Insiden Keselamatan ICT	
	7.4.1 Pelaporan Insiden	27
7.5	Pendidikan	
	7.5.1 Program Kesedaran Keselamatan ICT	28
7.6	Tindakan Tatatertib	
	7.6.1 Pelanggaran Polisi	28
7.7	Keselamatan Kawasan	
	7.7.1 Kawasan Larangan	28
7.8	Keselamatan Peralatan	
	7.8.1 Perkakasan	29
	7.8.2 Dokumen	29
	7.8.3 Media Storan	29
	7.8.4 Kabel	30
	7.8.5 Penyelenggaraan	30
	7.8.6 Peminjaman Perkakasan untuk Kegunaan di Luar Pejabat	30
	7.8.7 Peralatan di Luar Pejabat	30
	7.8.8 Pelupusan	31
	7.8.9 Clear Desk dan Clear Screen	31
7.9	Keselamatan Persekitaran	
	7.9.1 Kawalan Persekitaran	31
	7.9.2 Bekalan Kuasa	32
	7.9.3 Prosedur Kecemasan	32

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	3 DARI 49



7.10	Pengurusan Prosedur Operasi	
7.10.1	Pengendalian Prosedur	33
7.10.2	Kawalan Perubahan	33
7.10.3	Prosedur Pengurusan Insiden	33
7.11	Perancangan dan Penerimaan Sistem	
7.11.1	Perancangan Kapasiti	34
7.11.2	Penerimaan Sistem	34
7.12	Perisian Berbahaya	
7.12.1	Perlindungan dari Perisian Berbahaya	34
7.13	Housekeeping	
7.13.1	Penduaan	35
7.13.2	Sistem Log	35
7.14	Pengurusan Rangkaian	
7.14.1	Kawalan Infrastruktur Rangkaian	35
7.15	Pengurusan Media	
7.15.1	Penghantaran dan Pemindahan	37
7.15.2	Prosedur Pengendalian Media	37
7.15.3	Keselamatan Sistem Dokumentasi	37
7.16	Keselamatan Komunikasi	
7.16.1	Internet	37
7.16.2	Mel Elektronik	38
7.17	Kawalan Capaian	
7.17.1	Keperluan Polisi	39
7.18	Pengurusan Capaian Pengguna	
7.18.1	Akaun Pengguna	39
7.18.2	Jejak Audit	40
7.19	Kawalan Capaian Sistem dan Aplikasi	
7.19.1	Sistem Maklumat dan Aplikasi	40
7.20	Peralatan Komputer Mudah Alih	
7.20.1	Penggunaan Peralatan Komputer Mudah Alih	41
7.21	Keselamatan Dalam Membangunkan Sistem Aplikasi	
7.21.1	Keperluan Keselamatan	41
7.22	Fail Sistem	
7.22.1	Kawalan Fail Sistem	42
7.23	Pembangunan dan Proses Sokongan	
7.23.1	Kawalan Perubahan	42
7.24	Kesinambungan Perkhidmatan	
7.24.1	Pelan Kesinambungan Perkhidmatan	43

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	4 DARI 49

**PERKARA 08 - PEMATUHAN**

8.1	Pematuhan dan Keperluan Perundangan	
8.1.1	Pematuhan Polisi	44
8.1.2	Keperluan Perundangan	44

SENARAI LAMPIRAN**Lampiran 1**

Garis Panduan Mengenai Tatacara Memohon Kelulusan Projek ICT

Lampiran 2

Garis Panduan untuk Pembangunan Sistem Aplikasi dan Pangkalan Data

Lampiran 3

Surat Akuan Pematuhan Polisi ICT Lembaga Pembangunan Langkawi

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	5 DARI 49



TAFSIRAN

Tafsiran-tafsiran berikut digunakan dalam Polisi ICT Lembaga Pembangunan Langkawi :

“ICT” bermaksud Teknologi Maklumat dan Komunikasi

“Bahagian” bermaksud Bahagian, Seksyen dan Unit di Lembaga Pembangunan Langkawi

“BTM” bermaksud Bahagian Teknologi Maklumat

“Pegawai Lembaga Pembangunan Langkawi” bermaksud seseorang yang dilantik untuk sesuatu jawatan sama ada secara tetap, sambilan, sementara atau kontrak yang berkhidmat di Lembaga Pembangunan Langkawi

“CIO” bermaksud Ketua Pegawai Maklumat yang bertanggungjawab ke atas perancangan, pengurusan, penyelarasan dan pemantauan program ICT di Lembaga Pembangunan Langkawi

“ICTSO” bermaksud Pegawai Keselamatan ICT yang bertanggungjawab ke atas keselamatan ICT di Lembaga Pembangunan Langkawi

“JPICT” bermaksud Jawatankuasa Pemandu ICT di Lembaga Pembangunan Langkawi (JPICT LADA)

“GCERT” bermaksud Pasukan Tindak balas Insiden Keselamatan ICT Kerajaan (Government Computer Emergency Response Team)

“Pentadbir Sistem” bermaksud pegawai yang bertanggungjawab mengurus, mengawal, memantau dan menyelenggara operasi dan keselamatan pelayan dan data yang disimpan

“Pentadbir Rangkaian” bermaksud pegawai yang bertanggungjawab mengurus, mengawal, memantau dan menyelenggara operasi dan keselamatan rangkaian di Lembaga Pembangunan Langkawi

“Pengguna” bermaksud seseorang sama ada Pegawai Lembaga Pembangunan Langkawi, Pembekal, Pakar Runding atau Pelawat yang dibenarkan menggunakan kemudahan ICT Lembaga Pembangunan Langkawi

“Pembekal” bermaksud seseorang atau kumpulan orang yang dibenarkan membekal sama ada perkhidmatan atau barangan ICT di Lembaga Pembangunan Langkawi

“Pakar Runding” bermaksud seseorang atau kumpulan orang yang dipilih untuk memberi perkhidmatan dalam bentuk khidmat nasihat ICT di Lembaga Pembangunan Langkawi

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	6 DARI 49



“Pihak Ketiga” bermaksud pembekal atau pakar runding

“Aset” bermaksud harta benda kepunyaan atau milikan atau di bawah kawalan Kerajaan yang dibeli atau yang disewa beli dengan wang Kerajaan, yang diterima melalui sumbangan atau hadiah atau diperoleh melalui proses perundangan

“Aset ICT” termasuk, tetapi tidak terhad kepada sistem komputer peribadi, terminal, alat-alat periferal komputer, peralatan komunikasi, rangkaian komunikasi, perisian komputer, dokumentasi bantuan, peralatan storan, kemudahan sokongan dan sumber tenaga. Kemudahan terhad kepada kemudahan yang dibeli, disewa, dipajak, dimiliki atau dipinjamkan kepada LADA. Ia termasuk semua kemudahan, maklumat dan sistem aplikasi

“Perkakasan” bermaksud peralatan dan komponen ICT seperti komputer, notebook, pencetak dan sebagainya

“Komputer Server” bermaksud komputer yang mempunyai keupayaan tinggi yang memberi perkhidmatan berpusat

“Peralatan Rangkaian” bermaksud peralatan dan komponen yang digunakan dalam sistem rangkaian seperti switch, hub, router dan sebagainya

“IP” bermaksud *Internet Protocol*

“Penyulitan” bermaksud proses untuk mengaburkan maklumat supaya tidak dapat dibaca tanpa pengetahuan khusus (*encryption*)

“Pelupusan” bermaksud satu proses untuk mengeluarkan aset dari milikan, kawalan, simpanan dan rekod mengikut kaedah yang ditetapkan

“Hapus Kira” ialah satu proses untuk membatalkan rekod aset yang hilang

“Kehilangan” bermaksud aset yang tiada lagi dalam simpanan disebabkan oleh kecurian, kemalangan, kebakaran, bencana alam, kesusutan, penipuan atau kecuaiian pegawai awam

“Tugas-Tugas Dalaman” bermaksud tugas-tugas yang menyokong fungsi-fungsi Lembaga Pembangunan Langkawi

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	7 DARI 49



PENGENALAN

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

OBJEKTIF

Polisi ICT Lembaga Pembangunan Langkawi diwujudkan untuk menjamin kerahsiaan, integriti dan kebolehsediaan urusan maklumat Lembaga Pembangunan Langkawi melalui kemudahan ICT dengan meminimumkan kesan insiden keselamatan ICT.

SKOP

Polisi ini meliputi semua sumber atau aset ICT yang digunakan seperti maklumat (contoh: fail, dokumen dan data elektronik), perisian (contoh: aplikasi dan sistem perisian) dan perkakasan (contoh: komputer, peralatan komunikasi dan media magnet). Polisi ini adalah terpakai untuk semua pengguna di Lembaga Pembangunan Langkawi termasuk pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT Lembaga Pembangunan Langkawi.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Polisi ICT Lembaga Pembangunan Langkawi dan perlu dipatuhi adalah seperti berikut:

A. AKAUNTABILITI

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya ke atas aset ICT Lembaga Pembangunan Langkawi;

B. PEMATUHAN

Polisi ICT Lembaga Pembangunan Langkawi hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan aset ICT Lembaga Pembangunan Langkawi;

C. 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;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	8 DARI 49



D. HAK AKSES MINIMUM

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

E. PENGASINGAN

Prinsip pengasingan bermaksud bahawa semua tugas-tugas mewujudkan, memadam, mengemas kini, mengubah dan mengesahkan data diasingkan. Ia bertujuan untuk mengelak akses yang tidak dibenarkan dan melindungi aset ICT daripada kesilapan, kebocoran maklumat terperinci, di manipulasi dan seterusnya, mengekalkan integriti dan kebolehsediaan;

F. PENGAUDITAN

Pengauditan adalah tindakan untuk mengenal pasti tahap keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan atau jejak audit. Oleh itu, rekod audit hendaklah dilindungi dan tersedia untuk penilaian atau tindakan serta merta; dan

G. PEMULIHAN

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	9 DARI 49



PERKARA 01 : PEMBANGUNAN DAN PENYELENGGARAAN POLISI

1.1 Pelaksanaan Polisi

Pelaksanaan Polisi ini akan dijalankan oleh PB dibantu oleh Pasukan Pengurusan ICT yang terdiri daripada CIO, ICTSO dan semua Pegawai Bahagian. PB

1.2 Penyebaran Polisi

Polisi ini perlu disebar kepada semua Pengguna. BTM

1.3 Penyelenggaraan Polisi

Polisi adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan arahan serta keperluan semasa. Berikut adalah prosedur berhubung dengan penyelenggaraan Polisi ini: BTM

- a. kenal pasti dan tentukan perubahan yang diperlukan;
- b. kemukakan cadangan pindaan untuk persetujuan Mesyuarat Jawatankuasa Pemandu ICT Lembaga Pembangunan Langkawi (JPICT LADA) ; dan
- c. perubahan yang telah dipersetujui oleh JPICT dimaklumkan kepada semua pengguna dan polisi ini hendaklah dikaji semula sekurang-kurangnya sekali setahun.

1.4 Pengecualian

Polisi adalah terpakai kepada semua Pengguna dan tiada pengecualian Semua diberikan.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	10 DARI 49



PERKARA 02 : ORGANISASI ICT

2.1 Pengurus Besar

Peranan dan tanggungjawab PB adalah seperti berikut:

PB

- a. memastikan semua Pengguna memahami peruntukan-peruntukan di bawah Polisi;
- b. memastikan semua Pengguna mematuhi Polisi;
- c. memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; dan
- d. memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Polisi ICT Lembaga Pembangunan Langkawi.

2.2 Ketua Pegawai Maklumat (CIO)

Timbalan Pengurus Besar (Pengurusan) adalah merupakan Ketua CIO. CIO bertanggungjawab ke atas perancangan, pengurusan, penyelarasan dan pemantauan program ICT di Lembaga Pembangunan Langkawi.

CIO

2.3 Pengurus Komputer

Pegawai Teknologi Maklumat (PTM) adalah merupakan Pengurus Komputer Lembaga Pembangunan Langkawi. Peranan dan tanggungjawab Pengurus Komputer adalah seperti berikut:

PTM

- a. merangka, merumus dan menguatkuasakan Polisi ICT Lembaga Pembangunan Langkawi;
- b. menentukan semua pengguna mendapat pendedahan, bantuan dan mematuhi Polisi ICT Lembaga Pembangunan Langkawi;
- c. menetapkan prosedur pendaftaran dan pembatalan kebenaran kepada pengguna untuk mencapai maklumat dan perkhidmatan;
- d. menentukan kawalan akses semua Pengguna terhadap Aset ICT Lembaga Pembangunan Langkawi;
- e. memastikan kawalan capaian ke atas aset ICT termasuk maklumat, perkhidmatan rangkaian dan kemudahan-kemudahan yang berkaitan diwujudkan dan dilaksanakan dengan berkesan berasaskan keperluan urusan dan keselamatan;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	11 DARI 49



- f. mengkaji semula dan memperhalus pengurusan kerahsiaan maklumat dan kawalan capaian secara berkala;
- g. memastikan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT Lembaga Pembangunan Langkawi disimpan; dan
- h. merangka, membangun dan merumus pelan kesinambungan perkhidmatan Lembaga Pembangunan Langkawi yang menyeluruh untuk menjamin perkhidmatan tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

2.4 Pegawai Keselamatan ICT (ICTSO)

Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut:

ICTSO

- a. mengurus keseluruhan program-program keselamatan ICT Lembaga Pembangunan Langkawi;
- b. menguatkuasakan Polisi Keselamatan ICT Lembaga Pembangunan Langkawi;
- c. memberi penerangan dan pendedahan berkenaan Polisi Keselamatan ICT Lembaga Pembangunan Langkawi kepada semua pengguna;
- d. mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi Keselamatan ICT Lembaga Pembangunan Langkawi;
- e. menjalankan pengurusan risiko;
- f. menjalankan audit, mengkaji semula, merumus tindak balas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya;
- g. memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;
- h. melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT Sektor Awam (GCERT) dan memaklumpkannya kepada CIO;
- i. bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	12 DARI 49



- j. memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Polisi Keselamatan ICT LADA; dan
- k. menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.

2.5 Pentadbir Sistem ICT

Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut : BTM

- a. mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti panjang atau berlaku perubahan dalam bidang tugas;
- b. menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi ICT Lembaga Pembangunan Langkawi;
- c. memantau aktiviti capaian harian Pengguna;
- d. mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikanannya dengan serta merta;
- e. menyimpan dan menganalisis rekod jejak audit; dan
- f. menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala.

2.6 Pengguna

Peranan dan tanggungjawab Pengguna adalah seperti berikut: Pengguna

- a. membaca, memahami dan mematuhi Polisi ICT Lembaga Pembangunan Langkawi;
- b. lulus tapisan keselamatan;
- c. melaksanakan prinsip-prinsip Polisi ICT Lembaga Pembangunan Langkawi dan menjaga kerahsiaan maklumat LADA;
- d. melaksanakan langkah-langkah perlindungan seperti berikut :
 - i. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	13 DARI 49



- ii. memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
 - iii. menentukan maklumat sedia untuk digunakan;
 - iv. menjaga kerahsiaan kata laluan;
 - v. mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
 - vi. memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
 - vii. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.
- e. melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;
 - f. menghadiri program-program mengenai ICT; dan
 - g. menandatangani Surat Akuan Pematuhan Polisi ICT Lembaga Pembangunan Langkawi sebagaimana Lampiran 3.

2.7 Pembekal, Pakar Runding dan Pihak-Pihak Luar Lain

Peranan dan tanggungjawab Pihak Luar/Asing adalah seperti berikut:

- a. membaca, memahami dan mematuhi Polisi ICT Lembaga Pembangunan Langkawi di mana berkenaan;
- b. bertanggungjawab ke atas sebarang pelanggaran keselamatan disebabkan tindakannya sendiri;
- c. melaporkan insiden keselamatan ICT dengan kadar segera kepada Ketua Unit Keselamatan ICT Lembaga Pembangunan Langkawi; dan
- d. menjaga kerahsiaan data dan maklumat Lembaga Pembangunan Langkawi.

Pembekal,
Pakar
Runding
dan Pihak
-
Pihak
Luar
Lain

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	14 DARI 49



PERKARA 03 : PERKAKASAN DAN PERISIAN ICT LEMBAGA PEMBANGUNAN LANGKAWI

3.1 Perolehan/Pelupusan Perkakasan dan Perisian ICT

Tatacara perolehan dan pelupusan perkakasan dan perisian ICT hendaklah merujuk kepada pekeliling terpakai sedia ada.

Garis panduan untuk perolehan dan pelupusan perkakasan dan perisian ICT Lembaga Pembangunan Langkawi adalah seperti di Lampiran1.

3.2 Peruntukan / Perkongsian Perkakasan dan Perisian ICT

3.2.1 Pencetak

Perkara yang perlu dipatuhi adalah seperti berikut:

Semua

- a. Setiap Bahagian layak diperuntukkan satu unit pencetak warna untuk diguna sama di kalangan pegawai dan kakitangan.
- b. Pencetak berwarna jenis kapasiti tinggi yang dibekalkan di LADA adalah untuk diguna sama oleh Bahagian-bahagian.
- c. Pegawai gred 41 ke atas layak dan boleh dibekalkan dengan sebuah pencetak light duty setiap pegawai.
- d. Untuk pegawai-pegawai lain, pencetak perlulah diguna secara 'pool' dengan nisbah yang difikirkan sesuai untuk kelancaran kerja dan jenis kerja yang dilakukan seperti kerahsiaan maklumat, kedudukan tempat dan proses kerja.

3.2.2 Personal Computer (PC)

Perkara yang perlu dipatuhi adalah seperti berikut:

Semua

- a. Setiap pegawai layak diperuntukkan 1 unit PC mengikut keperluan dan jenis yang sesuai.
- b. Peralatan-peralatan seperti Notebook dan LCD Projector perlu diguna secara guna sama di bahagian-bahagian.
- c. Pegawai yang membuat peminjaman peralatan guna sama haruslah bertanggungjawab sepenuhnya terhadap keselamatan peralatan yang dipinjam.
- d. Peralatan mobile layak dibekalkan kepada pegawai mengikut justifikasi keperluannya.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	15 DARI 49



3.2.3 Penyelenggaraan Perkakasan dan Perisian ICT

Perkara yang perlu dipatuhi adalah seperti berikut:

Semua

- a. Penyelenggaraan peralatan perkakasan ICT di bahagian-bahagian perlulah di selaras oleh BTM bagi memudahkan pemantauan dan inventori.
- b. Perisian sistem pengoperasian bagi perkakasan ICT di Bahagian-bahagian, dikonfigur supaya dikemas kini patches dan dinaiktarafkan (upgrades) kepada versi terkini secara automatik.
- c. Bantuan teknikal/aduan tentang masalah-masalah yang dihadapi dalam penggunaan ICT perlu diajukan kepada BTM.
- d. Perisian-perisian ICT yang disokong oleh BTM untuk pemasangan, penyelenggaraan dan latihan adalah termasuk:
 - i. MS Office yang terdiri daripada:
 - MS Word
 - MS Excel
 - MS Powerpoint
 - ii. Internet Explorer
 - iii. Mozilla Firefox
 - iv. Google Chrome
 - v. Acrobat Reader
 - vi. Antivirus
 - vii. E-Kamus
- e. Sokongan untuk perisian yang tidak tersenarai di item (d) hanya akan diberikan sekiranya ada tenaga kepakaran di BTM.
- f. Perisian ICT yang tidak berdaftar, berlesen ataupun cetak rompak tidak dibenarkan diguna pakai. Pihak BPTM berhak membuang (uninstall) perisian tersebut.
- g. Pengguna mesti memastikan media storan (disket, CD/DVD atau thumb drive) yang menyimpan dokumen terperingkat disimpan di tempat yang selamat.
- h. Pengguna mesti memastikan maklumat rahsia rasmi yang terkandung dalam media storan seperti pita magnetik, cakera keras, CD/DVD, optical disk, removal disk (thumb/PenDrive) dan lain-lain, dikawal dan dilindungi dengan perisian penyulitan (encryption) yang dibenarkan oleh BPTM.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	16 DARI 49



PERKARA 04 : PENGURUSAN E-MEL DAN PENGGUNAAN INTERNET

4.1 Pengurusan E-Mel

Perkara yang perlu dipatuhi adalah seperti berikut:

Semua

- a. Akaun e-mel bukanlah hak mutlak seseorang. Ia adalah kemudahan yang tertakluk kepada peraturan jabatan dan boleh ditarik balik jika penggunaannya melanggar peraturan.
- b. Warga LADA adalah bertanggungjawab kepada e-mel masing-masing.
- c. LADA tidak akan bertanggungjawab ke atas sebarang kesalahan jenayah dan seumpamanya berkaitan e-mel.
- d. Warga LADA boleh menggunakan e-mel sebagai saluran rasmi dalam urusan rasmi dan urusan pentadbiran harian.
- e. Pengguna harus menggunakan perisian penyulitan yang dibenarkan oleh BTM untuk menghantar dokumen dan maklumat terperingkat melalui e-mel.
- f. Warga LADA dikehendaki merahsiakan nama pengenalan dan kata laluan dari pengetahuan orang lain.
- g. Warga LADA diminta menukarkan kata laluan masing-masing sekurang-kurangnya enam bulan sekali bagi mengelakkan akaun mereka dicerobohi.
- h. Warga LADA tidak dibenarkan menggunakan kemudahan e-mel percuma seperti Hotmail, GMail dan Yahoo untuk tujuan rasmi.
- i. Setiap alamat e-mel yang disediakan adalah untuk kegunaan individu berkenaan sahaja dan tidak boleh digunakan oleh pihak lain sama ada dengan kebenaran atau tanpa kebenaran.
- j. Warga LADA adalah dinasihatkan menggunakan kemudahan emel secara rutin sekurang-kurangnya sekali sehari.
- k. Mana-mana e-mel rasmi yang dihantar dan diterima perlu di archive sendiri oleh Warga LADA.
- l. Elakkan dari menerima dan membuka e-mel di mana penghantarnya tidak diketahui dan diragui dan pengguna perlulah memadam terus e-mel tersebut.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	17 DARI 49



- m. Had muatan kotak e-mel setiap pengguna adalah tidak melebihi 1GB, manakala had penghantaran bahan kepilang tidak melebihi 10 MB dalam satu masa.
- n. Bagi Warga LADA yang akan bercuti atau berkursus dalam tempoh yang panjang (melebihi 30 hari) atau bertukar tempat kerja, maklumkan kepada pentadbir e-mel dengan segera supaya kerja-kerja penyelenggaraan e-mel dapat dilaksanakan.
- o. Warga LADA yang tidak lagi berkhidmat di LADA akan dihapus id dan capaiannya kepada e-mel dalam masa 1 bulan.
- p. Warga LADA hendaklah sentiasa mengimbas fail dalam kotak e-mel dengan perisian antivirus.
- q. Warga LADA juga hendaklah memastikan fail yang akan dihantar melalui kepilang (attachment) bebas dari virus.
- r. Aktiviti spamming, penyebaran virus, bahan-bahan negatif dan surat berantai adalah dilarang. Jika didapati aktiviti ini dilakukan oleh Warga LADA, akaun mereka akan dibatalkan tanpa sebarang notis.
- s. Pentadbir Sistem berhak memasang sebarang jenis perisian atau perkakasan penapisan e-mel dan virus yang difikirkan sesuai dan boleh menggunakannya untuk mencegah, menapis, menyekat atau menghapuskan mana-mana e-mel yang disyaki mengandungi virus atau berunsur spamming daripada memasuki komputer.
- t. Menyebar perisian cetak rompak atau maklumat berbau politik, hasutan atau perkauman atau apa-apa maklumat yang menjejaskan reputasi LADA dan Perkhidmatan Awam melalui kemudahan emel LADA adalah dilarang.
- u. Pengguna dilarang melakukan pencerobohan atau percubaan untuk mencero boh masuk ke mana-mana akaun Pengguna lain.
- v. Pihak Pengurusan atau Pentadbir Sistem boleh memantau semua e-mel LADA jika perlu tanpa mendapat kebenaran Warga LADA.

4.2 Melayari Internet

Perkara yang perlu dipatuhi adalah seperti berikut :

Semua

- a. Pengguna yang melayari aplikasi dan laman web adalah bertanggung jawab sepenuhnya ke atas maklumat yang dikunci masuk serta capaian yang dilakukan.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	18 DARI 49



- b. Pengguna tidak digalakkan menggunakan rangkaian dail-up, 3G dan seumpamanya untuk melayari aplikasi dan laman web tanpa kebenaran daripada BTM.
- c. Penghantaran dokumen yang mengandungi maklumat rahsia rasmi melalui internet tidak dibenarkan sama sekali tanpa perisian penyulitan (encryption) yang dibenarkan oleh BTM.
- d. Pengguna tidak di benar menyumbangkan perkara-perkara bertentangan dengan Perintah Am Kerajaan kepada mana-mana laman web tanpa kebenaran Ketua Jabatan.
- e. Penghantaran dan penerimaan dokumen yang mengandungi maklumat rahsia rasmi melalui internet tidak dibenarkan sama sekali tanpa perisian penyulitan yang dibenarkan oleh BTM.
- f. Pengguna tidak dibenarkan membuat capaian kepada bahan-bahan terlarang dan menggunakan sebarang perisian judi atau seumpamanya dengan menggunakan kemudahan pejabat.
- g. Capaian laman yang berbentuk hiburan, permainan komputer online, radio online dan video streaming yang membebaskan rangkaian LADA adalah tidak dibenarkan.
- h. Pengguna tidak dibenarkan melanggan kepada mana-mana mailing list yang tidak berkaitan dengan tugas.
- i. Aktiviti chatting adalah tidak dibenarkan melainkan menggunakan perisian yang dibangunkan oleh BTM.
- j. Aktiviti muat turun (download) atau muat naik (upload) sebarang perisian cetak rompak adalah dilarang.
- k. Penggunaan Internet Proxy untuk capaian ke internet adalah tidak dibenarkan.
- l. Pengguna tidak dibenarkan melayari laman-laman yang tidak berkaitan dengan tugas di waktu pejabat.
- m. Pentadbir Rangkaian di LADA adalah diberi kuasa untuk menjana laporan capaian rangkaian dan internet setiap pengguna kepada pihak pengurusan.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	19 DARI 49



- n. Pentadbir Rangkaian berhak menyediakan dan memasang perisian penapisan isi kandungan internet.
- o. Pentadbir Rangkaian berhak menapis, menghalang dan menegah penggunaan mana-mana laman web yang tidak sesuai.

4.3 Laman dan Aplikasi Web

Perkara yang perlu dipatuhi adalah seperti berikut:

Semua

- a. Semua maklumat yang hendak dimuatkan ke dalam laman web LADA mestilah mendapat kelulusan Ketua Bahagian/Jabatan.
- b. Maklumat yang terkandung dalam laman web adalah di bawah tanggungjawab Bahagian masing-masing.
- c. Laman web syarikat atau individu yang memerlukan pautan ke Laman Web LADA atau sebaliknya mestilah mendapat kebenaran Ketua Jabatan.
- d. Pencerobohan atau percubaan untuk menggodam laman web LADA adalah di larang.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	20 DARI 49



PERKARA 05 : SISTEM APLIKASI DAN PANGKALAN DATA

5.1 Sistem Aplikasi dan Pangkalan Data

Perkara yang perlu dipatuhi adalah seperti berikut :

Semua

- a. Bahagian-bahagian hendaklah memohon secara rasmi kepada BPTM untuk membangunkan sesuatu sistem aplikasi.
- b. Bahagian perlu memohon kepada JPICT kebenaran untuk membangunkan sistem aplikasi. Permohonan ini hendaklah lengkap meliputi spesifikasi teknikal, anggaran kos yang terlibat, guna tenaga dan juga skop perluasan aplikasi tersebut.
- c. Sesuatu aplikasi perlu mempunyai Pemilik (owner) iaitu sesuatu Bahagian atau pengguna utama (yang paling banyak menggunakan sistem atau yang paling banyak memiliki data).
- d. Pengguna yang bertukar bidang tugas atau tidak lagi berkhidmat di LADA akan dihapus id dan capaiannya ke aplikasi dalam masa 30 hari.
- e. Bahagian yang memohon akan menjadi Pemilik (owner) kepada sistem tersebut dan hendaklah melantik champion bagi melancarkan pelaksanaan sistem. Champion seboleh-sebolehnya di peringkat TSUB dan mendapat mandat daripada TKSP yang berkaitan.
- f. Pemilik (owner) sistem aplikasi perlu membuat pelaporan kepada JPICT secara berkala bagi kemajuan (progress) sistem tersebut.
- g. Pembangunan sistem aplikasi hendaklah mengambil kira sistem sedia ada di agensi berkenaan dan agensi lain bagi mengelakkan pertindihan pembangunan sistem aplikasi yang sama. Sebagai contoh pembangunan sistem yang berkaitan sumber manusia hendaklah dielakkan kerana HRMIS telah sedia untuk diguna pakai.
- h. Pembangunan sistem aplikasi harus mengambil kira keperluan aspek keselamatan yang ditetapkan pada setiap peringkat perolehan, pembangunan dan penyelenggaraan.
- i. Sebarang pembangunan aplikasi mestilah mengguna pakai kod-kod yang standard di bawah Data Dictionary Sektor Awam (DDSA).

Garis panduan untuk pembangunan sistem aplikasi dan pangkalan data adalah seperti di **Lampiran 2**.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	21 DARI 49



PERKARA 06 : PENGGUNAAN DAN PENGURUSAN RANGKAIAN

6.1 Insfratraktur Rangkaian

Perkara yang perlu dipatuhi adalah seperti berikut :

Semua

- a. Sambungan ke Internet – Semua komunikasi antara sistem ICT dengan sistem luar hendaklah melalui mekanisme pusat untuk mengurus, menguatkuasakan dan mengawas sebarang bahaya keselamatan.
- b. Hanya Pengguna sahaja yang dibenarkan mengguna rangkaian LADA.
- c. Pengguna luar yang hendak menggunakan kemudahan rangkaian LADA hendaklah mendapat kebenaran BTM.

6.2 Pengurusan Alamat IP

Perkara yang perlu dipatuhi adalah seperti berikut :

Semua

- a. Sebarang permohonan untuk menggunakan IP statik hendaklah melalui BTM dengan mengisi borang yang disediakan.
- b. Pengguna adalah dilarang sama sekali untuk menukar atau meletakkan IP di dalam komputer masing-masing tanpa kebenaran.
- c. Sebarang pertukaran Pengguna yang diperuntukkan IP statik hendaklah memaklumkan kepada pihak BTM.
- d. IP statik yang diberikan kepada Pengguna tidak boleh digunakan untuk kepentingan sendiri. Sekiranya Pengguna didapati menyalahgunakan IP statik dengan menukar konfigurasi PC kepada server tanpa memaklumkan kepada BTM, PC Pengguna berkenaan akan dikeluarkan dari rangkaian.

6.3 Sambungan Rangkaian

Perkara yang perlu dipatuhi adalah seperti berikut :

Semua

- a. Semua permohonan baru untuk mendapatkan sambungan rangkaian mestilah melalui BTM.
- b. Pengguna tidak dibenarkan menyambung sebarang peralatan peribadi ke dalam rangkaian LADA.
- c. Pengguna tidak dibenarkan memasang sebarang access point untuk capaian secara tanpa wayar (wireless) ke dalam rangkaian LADA.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	22 DARI 49



- d. Pengguna tidak dibenarkan memutuskan/ menyambung sambungan kabel UTP pada mana-mana port dalam rak peralatan rangkaian tanpa kebenaran dari pihak BTM.
- e. Pengguna tidak dibenarkan menukar maklumat yang terdapat pada faceplate (UTP port).
- f. Perbuatan yang boleh merosakkan UTP port, kabel UTP atau rak peralatan rangkaian serta peralatannya adalah dilarang.
- g. Sebarang kerosakan pada kabel UTP, network point dan network port pada manamana switch/hub hendaklah dilaporkan kepada BTM.

6.4 Dial-Up dan Rangkaian Tanpa Wayar (Wireless) Internet 3G

Perkara yang perlu dipatuhi adalah seperti berikut :

Semua

- a. Kemudahan dial-up, 3G dan seumpamanya hanya diberikan untuk tujuan rasmi.
- b. Permohonan menggunakan kemudahan dial-up, 3G dan seumpamanya adalah dengan mengisi borang yang disediakan.
- c. Pengguna yang hendak menggunakan kemudahan dial-up, 3G dan seumpamanya pada waktu pejabat hendaklah memutuskan (disable/ disconnect) sambungan ke rangkaian LADA terlebih dahulu. Setelah menggunakan kemudahan tersebut pengguna dikehendaki mengimbas keseluruhan komputer yang digunakan sebelum menyambung semula (enable/connect) ke rangkaian LADA bagi memastikan tiada virus masuk ke rangkaian LADA.

6.5 FTP

- a. Fail bersaiz besar yang dimuat turun hendaklah dilakukan selepas waktu pejabat.
- b. Fail yang mengandungi maklumat rahsia rasmi yang menggunakan penghantaran muat turun (FTP) harus melalui proses penyulitan (encryption) sebelum penghantaran maklumat dibuat.

Semua

6.6 Pengenalan dan Kata Laluan

Perkara yang perlu dipatuhi adalah seperti berikut :

Semua

- a. Semua Pengguna baru hendaklah memohon id pengguna dengan mengisi borang yang disediakan.
- b. ID pengguna yang tidak aktif selepas 3 bulan akan dibekukan dan seterusnya dimansuhkan kecuali telah dimaklumkan kepada BTM.
- c. Kata laluan hendaklah tidak dipaparkan semasa input.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	23 DARI 49



- d. Penukaran kata laluan perlulah dibuat oleh Pengguna setiap 3 bulan.
- e. Panjang kata laluan sekurang-kurangnya 12 aksara.
- f. Kata laluan mesti menggunakan kombinasi daripada aksara, angka dan simbol-simbol lain.
- g. Kata laluan tidak boleh dikongsi dengan orang lain.
- h. Menggunakan kata laluan yang selamat dan tidak mudah dicerobohi. Penggunaan kata laluan yang sukar diramal oleh penggadam adalah digalakkan.
- i. Fail kata laluan untuk semua sistem aplikasi hendaklah disimpan berasingan daripada data.
- j. Cubaan capaian dihadkan kepada tiga (3) kali sahaja. Id pengguna berkenaan akan digantung (suspended) selepas tiga (3) kali cubaan gagal yang berturutan. Penggantungan hanya boleh dibatalkan dengan mengemukakan permohonan kepada pentadbir sistem.
- k. Pengguna dilarang menggunakan kata laluan yang sama dengan id pengguna.
- l. Kata laluan hendaklah diingat dan tidak digalakkan dicatat, disimpan atau didedahkan dengan apa cara sekalipun.

6.7 Antivirus

Perkara yang perlu dipatuhi adalah seperti berikut :

Semua

- a. Kesemua perkakasan seperti PC yang bersambung ke rangkaian LADA mesti mempunyai antivirus yang dibekalkan oleh BPTM dan dipasang, diaktifkan dan dikemaskinikan paten dan perisian antivirus tersebut.
- b. Setiap PC mempunyai hanya satu (1) perisian antivirus yang dibekalkan oleh BTM. Pengguna tidak dibenarkan memasang antivirus lain selain yang dibekalkan oleh BTM.
- c. Sebarang perkakasan yang didapati menyebarkan virus dan setara dengannya, akan diputuskan hubungan ke rangkaian LADA sehinggalah virus berkenaan dihapuskan.
- d. Semua Pengguna hendaklah membuat scanning semua fail yang telah dimuat turun dari mana-mana sumber termasuklah e-mel.
- e. Sebarang media seperti disket, thumb drive dan CD/DVD perlu diimbis sebelum sebarang fail dibaca atau disalin ke PC masing-masing.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	24 DARI 49



- f. Mana-mana pegawai yang didapati menjadi pembawa atau pembuat virus akan dilaporkan terus kepada pihak pengurusan.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	25 DARI 49



PERKARA 07 : POLISI KESELAMATAN ICT

7.1 Akauntabiliti Aset

Objektif: Memberi perlindungan yang bersesuaian ke atas semua aset ICT LADA.

7.1.1 Inventori Aset

Semua aset ICT LADA hendaklah direkodkan. Ini termasuklah mengenal pasti aset, mengklasifikasikan aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik serta dikemas kini secara berkala.

Setiap Pengguna adalah bertanggung jawab ke atas semua aset ICT di bawah kawalannya.

7.2 Pengelasan dan Pengendalian Maklumat

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

7.2.1 Pengelasan Maklumat

Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: Semua

- i. Rahsia Besar ;
- ii. Rahsia ;
- iii. Sulit ; atau
- iv. Terhad.

7.2.2 Pengendalian Maklumat

Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnahkan hendaklah mengambil kira langkah-langkah keselamatan berikut : Semua

- a. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
- b. memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
- c. menentukan maklumat sedia untuk digunakan;
- d. menjaga kerahsiaan kata laluan;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	26 DARI 49



- e. mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
- f. penyulitan maklumat sebelum penduaan (backup) dan transmisi;
- g. mengendalikan penduaan maklumat, sistem dan data pada server dan disimpan di luar kawasan (off site) secara berkala;
- h. memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
- i. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

7.3 Keselamatan ICT dalam Tugas Harian

Objektif: Meminimumkan risiko seperti kesilapan, kecuaiian, kecurian, penipuan dan penyalahgunaan aset ICT LADA.

7.3.1 Tanggungjawab Keselamatan

Peranan dan tanggungjawab Pengguna terhadap keselamatan ICT mestilah lengkap, jelas, di rekod, dipatuhi dan dilaksanakan serta dinyatakan di dalam Fail Meja atau kontrak. Semua

Keselamatan ICT merangkumi tanggungjawab Pengguna dalam menyediakan dan memastikan perlindungan ke atas semua aset atau sumber ICT yang digunakan di dalam melaksanakan tugas harian.

7.4 Menangani Insiden Keselamatan ICT

Objektif : Meminimumkan kesan insiden keselamatan ICT.

7.4.1 Pelaporan Insiden

Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera: Semua

- a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau disyaki hilang;
- b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;
- c. Kata laluan atau mekanisme kawalan akses hilang, dicuri, didedahkan atau disyaki hilang;
- d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	27 DARI 49



- e. Berlaku percubaan mencerooboh, penyelewengan dan insiden-insiden yang tidak diingini.

Nota :

Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan ICT” mengenainya boleh dirujuk.

7.5 Pendidikan

Objektif : Meningkatkan pengetahuan dan kesedaran mengenai kepentingan keselamatan ICT.

7.5.1 Program Kesedaran Keselamatan ICT

Setiap Pengguna di LADA perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. ICTSO

Program menangani insiden juga dilihat penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT LADA.

7.6 Tindakan Tatatertib

Objektif : Meningkatkan kesedaran dan pematuhan ke atas Polisi ICT LADA.

7.6.1 Pelanggaran Polisi

Pelanggaran Polisi ICT LADA akan dikenakan tindakan tatatertib. Semua

7.7 Keselamatan Kawasan

Objektif: Mencegah akses fizikal yang tidak dibenarkan, kerosakan dan gangguan kepada premis dan maklumat.

7.7.1 Kawasan Larangan

Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut.. Akses kepada kawasan tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja: Semua

- a. Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik, supaya boleh digunakan bila perlu. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal. Mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; dan
- b. Semua penggunaan peralatan yang melibatkan penghantaran, kemas kini dan penghapusan maklumat rasmi hendaklah dikawal dan mendapat kebenaran daripada BTM.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	28 DARI 49



7.8 Keselamatan Peralatan

Objektif: Melindung peralatan dan maklumat.

7.8.1 Perkakasan

Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu : Semua

- a. Setiap Pengguna hendaklah menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan sempurna;
- b. Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan;
- c. Setiap Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; dan
- d. Sebarang bentuk penyelewengan atau salah guna perkakasan hendaklah dilaporkan kepada ICTSO.

7.8.2 Dokumen

Bagi memastikan integriti maklumat, langkah - langkah pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi: Semua

- a. memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin;
- b. menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka kepada dokumen;
- c. menggunakan penyulitan (encryption) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik; dan
- d. memastikan dokumen yang mengandungi bahan atau maklumat sensitif diambil segera dari pencetak.

7.8.3 Media Storan

Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar. Semua

Langkah-langkah pencegahan seperti berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat:

- a. penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	29 DARI 49



- b. akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada mereka atau pengguna yang dibenarkan sahaja;
- c. penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; dan
- d. Pergerakan media storan hendaklah direkodkan.

7.8.4 Kabel

Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut :

- a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; dan
- b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan.

7.8.5 Penyelenggaraan

Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan dan integriti. Semua

- a. Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan;
- b. Perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; dan
- c. Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan.

7.8.6 Peminjaman Perkakasan untuk Kegunaan di Luar Pejabat

Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan perkakasan :

- a. Peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai atasan dan tertakluk kepada tujuan yang dibenarkan; dan
- b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan.

7.8.7 Peralatan di Luar Pejabat

Bagi perkakasan yang dibawa keluar dari premis LADA, langkah-langkah keselamatan hendaklah diadakan dengan mengambil kira risiko yang wujud di luar kawalan LADA :

- a. Peralatan perlu dilindungi dan dikawal sepanjang masa; dan

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	30 DARI 49



- b. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.

7.8.8 Pelupusan

Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan LADA : Semua

- 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; dan
- c. Maklumat lanjut pelupusan bolehlah merujuk kepada Pekeliling Perbendaharaan Bilangan 5 Tahun 2007 bertajuk "Tatacara Pengurusan Aset Alih Kerajaan".

7.8.9 Clear Desk dan Clear Screen

Semua maklumat dalam apa jua bentuk media hendaklah di simpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. Clear Desk bermaksud tidak meninggalkan dokumen terperingkat terdedah sama ada atas meja warga atau di paparan skrin apabila anggota LADA tidak berada di tempatnya :

- a. Gunakan kemudahan password screen saver atau log keluar apabila meninggalkan komputer; dan
- b. Dokumen terperingkat hendaklah disimpan dalam laci atau kabinet fail yang berkunci.

7.9 Keselamatan Persekitaran

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

7.9.1 Kawalan Persekitaran

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, mengubahsuai atau pembelian hendaklah dirujuk terlebih dahulu kepada PB. Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil: Semua

- a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	31 DARI 49



- b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;
- c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan;
- d. Semua kawasan larangan khususnya bilik pemprosesan maklumat dan perkakasan ICT yang menyimpan data dan maklumat rasmi tidak boleh dilabel. Ia perlu dilindungi dari sebarang pendedahan dan akses oleh individu yang tidak dibenarkan;
- e. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT;
- f. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT;
- g. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; dan
- h. 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.

7.9.2 Bekalan Kuasa

- a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT;
- b. Peralatan sokongan seperti UPS (Uninterruptable Power Supply) dan penjana (generator) boleh digunakan bagi perkhidmatan kritikal supaya mendapat bekalan kuasa berterusan; dan
- c. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.

Penyenggara
Bangunan
dan BTM

7.9.3 Prosedur Kecemasan

- a. Setiap Pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan Perbendaharaan 2004; dan
- b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan LADA.

Semua

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	32 DARI 49



7.10 Pengurusan Prosedur Operasi

Objektif : Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat.

7.10.1 Pengendalian Prosedur

- a. Semua prosedur keselamatan ICT yang ditetapkan dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; Semua
- b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan
- c. Semua prosedur hendaklah disemak dan dikemas kini dari masa ke semasa atau mengikut keperluan.

7.10.2 Kawalan Perubahan

- a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; Semua
- b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;
- c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan
- d. Semua aktiviti perubahan atau pengubahsuaian hendaklah di rekod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.

7.10.3 Prosedur Pengurusan Insiden

Bagi memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan, prosedur pengurusan insiden mestilah mengambil kira kawalan-kawalan berikut : ICTSO

- a. Mengenal pasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran;
- b. Menyedia pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	33 DARI 49



- c. Menyimpan jejak audit dan memelihara bahan bukti; dan
- d. Menyediakan tindakan pemulihan segera.

7.11 Perancangan dan Penerimaan Sistem

Objektif : Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

7.11.1 Perancangan Kapasiti

- a. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, Pentadbir
diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi S i s t e m
memastikan keperluannya adalah mencukupi dan bersesuaian untuk ICT dan
pembangunan dan kegunaan sistem ICT pada masa akan datang; ICTSO
dan
- b. 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.

7.11.2 Penerimaan Sistem

Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. BTM

7.12 Perisian Berbahaya

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

7.12.1 Perlindungan dari Perisian Berbahaya

- a. Memasang sistem keselamatan untuk mengesan perisian atau Semua
program berbahaya seperti antivirus dan Intrusion Detection System
(IDS) dan mengikut prosedur penggunaan yang betul dan selamat;
- b. Memasang dan menggunakan hanya perisian yang berdaftar dan
dilindungi di bawah Akta Hak Cipta (Pindaan) Tahun 1997;
- c. Mengimbas semua perisian atau sistem dengan antivirus sebelum
menggunakannya;
- d. Menyemak kandungan sistem atau maklumat secara berkala bagi
mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan
maklumat;
- e. Menghadiri program kesedaran mengenai ancaman perisian
berbahaya dan cara mengendalikannya;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	34 DARI 49



- f. Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;
- g. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan
- h. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.

7.13 Housekeeping

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

7.13.1 Penduaan

Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan hendaklah dilakukan setiap kali konfigurasi berubah. Salinan penduaan hendaklah direkodkan dan di simpan off site. Semua

- a. Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;
- b. Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi; dan
- c. Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan.

7.13.2 Sistem Log

- a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian Pengguna; BTM
- 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 tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.

7.14 Pengurusan Rangkaian

Objektif : Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

7.14.1 Kawalan Infrastruktur Rangkaian

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	35 DARI 49



Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah-langkah yang perlu dipertimbangkan: BTM

- a. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;
- b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk;
- c. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;
- d. Peralatan rangkaian harus di selenggara secara berkala oleh kakitangan atau pihak yang dibenarkan sahaja;
- e. Peralatan rangkaian yang kritikal harus mempunyai kontrak penyelenggaraan yang menyeluruh dan berkala;
- f. Semua peralatan mestilah melalui proses Factory Acceptance Check (FAC) semasa pemasangan dan konfigurasi;
- g. Semua trafik keluar dan masuk hendaklah melalui Firewall di bawah kawalan LADA;
- h. Semua perisian sniffer atau network analyser adalah dilarang dipasang pada komputer Pengguna kecuali mendapat kebenaran ICTSO;
- i. Memasang perisian Intrusion Detection System (IDS) bagi mengesan sebarang cubaan mencero boh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat LADA;
- j. Memasang Web Content Filter pada Internet Gateway untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan”;
- k. Sebarang penyambungan rangkaian yang bukan di bawah kawalan LADA hendaklah mendapat kebenaran ICTSO;
- l. Semua Pengguna hanya dibenarkan menggunakan rangkaian LADA sahaja. Penggunaan modem adalah dilarang sama sekali; dan
- m. Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	36 DARI 49



7.15 Pengurusan Media

Objektif : Melindungi aset ICT dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal.

7.15.1 Penghantaran dan Pemindahan

Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu. Semua

7.15.2 Prosedur Pengendalian Media

- a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; Semua
- b. Mengehadkan dan menentukan capaian media kepada pengguna yang sah sahaja;
- c. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan;
- d. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan;
- e. Menyimpan semua media di tempat yang selamat; dan
- f. Media yang mengandungi maklumat rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat.

7.15.3 Keselamatan Sistem Dokumentasi

- a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan;
- b. Menyedia dan memantapkan keselamatan sistem dokumentasi; dan
- c. Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.

7.16 Keselamatan Komunikasi

Objektif : Melindungi aset ICT melalui sistem komunikasi yang selamat.

7.16.1 Internet

- a. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh CIO; Semua
- b. Bahan yang diperolehi dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendaklah dinyatakan;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	37 DARI 49



- c. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada PTM sebelum dimuat naik ke Internet;
- d. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;
- e. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh LADA;
- f. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti newsgroup dan bulletin board; dan
- g. Maklumat lanjut mengenai keselamatan Internet bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”.

7.16.2 Mel Elektronik

- a. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh LADA sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; Semua
- b. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh LADA;
- c. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;
- d. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul;
- e. Pengguna dinasihatkan menggunakan fail kepilan sekiranya perlu, tidak melebihi sepuluh (10) MB semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;
- f. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;
- g. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui emel;
- h. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan;
- i. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	38 DARI 49



- j. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; dan
- k. Maklumat lanjut mengenai keselamatan emel bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”.

7.17 Kawalan Capaian

Objektif : Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT LADA.

7.17.1 Keperluan Polisi

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong polisi kawalan capaian pengguna sedia ada.

Semua

7.18 Pengurusan Capaian Pengguna

Objektif : Mengawal capaian pengguna ke atas aset ICT LADA.

7.18.1 Akaun Pengguna

Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi :

Semua

- a. Akaun yang diperuntukkan oleh LADA sahaja boleh digunakan;
- b. Akaun Pengguna mestilah unik;
- c. Akaun Pengguna yang di wujud pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu;
- d. Pemilikan akaun Pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;
- e. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;
- f. Pentadbir sistem ICT harus menyemak akaun pengguna dan hak aksesnya bagi menentukan ketepatan dan kesempurnaan sesuatu tahap capaian secara berkala; dan

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	39 DARI 49



- g. Pentadbir sistem ICT boleh menggantung (suspended) dan menamatkan akaun pengguna atas sebab-sebab berikut :
- i. Bertukar bidang tugas kerja;
 - ii. Bertukar ke agensi lain;
 - iii. Bersara; atau
 - iv. Ditamatkan perkhidmatan.

7.18.2 Jejak Audit

Jejak audit akan merekodkan semua aktiviti sistem. Jejak audit juga adalah penting dan digunakan untuk tujuan penyiasatan sekiranya berlaku kerosakan atau penyalahgunaan sistem.

Pentadbir
S i s t e m
I C T

Aktiviti jejak audit mengandungi:

- a. Maklumat identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan program yang digunakan;
- b. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan
- c. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. 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.

7.19 Kawalan Capaian Sistem dan Aplikasi

Objektif : Melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.

7.19.1 Sistem Maklumat dan Aplikasi

Capaian sistem dan aplikasi di LADA adalah terhad kepada Pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi:

BTM

- a. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan;
- b. Setiap aktiviti capaian sistem maklumat dan aplikasi Pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	40 DARI 49



- c. Memaparkan notis amaran pada skrin komputer Pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan;
- d. Mengehadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan Pengguna akan disekat;
- e. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan
- f. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.

7.20 Peralatan Komputer Mudah Alih

Objektif : Memastikan keselamatan maklumat apabila menggunakan kemudahan atau peralatan komputer mudah alih.

7.20.1 Penggunaan Peralatan Komputer Mudah Alih

- a. Merekodkan aktiviti keluar masuk penggunaan peralatan komputer mudah alih bagi mengesan kehilangan atau pun kerosakan; dan Semua
- b. Komputer mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.

7.21 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

Objektif : Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

7.21.1 Keperluan Keselamatan

- a. Pembangunan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; Pemilik Sistem dan BTM
- b. Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul/ sempurna dan sistem output untuk memastikan data yang telah diproses adalah tepat; dan

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	41 DARI 49



- c. Sebaiknya-baiknya, semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan. Ujian tahap keselamatan harus merangkumi Penilaian Kerentanan (Vulnerability Assessment) oleh pihak berkenaan sebelum pengaktifan sistem.

7.22 Fail Sistem

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

7.22.1 Kawalan Fail Sistem

- a. Proses pengemaskinian fail sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; Pentadbir Sistem ICT
- 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; dan
- d. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.

7.23 Pembangunan dan Proses Sokongan

Objektif : Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

7.23.1 Kawalan Perubahan

Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai.

7.24 Kesinambungan Perkhidmatan

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

7.24.1 Pelan Kesenambungan Perkhidmatan

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	42 DARI 49



Pelan kesinambungan perkhidmatan 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 JPIC dan perkara - perkara berikut perlu diberi perhatian: ICTSO

- a. Pelan Kesinambungan Perkhidmatan LADA harus dibentuk dengan menggunakan pendekatan “berpasukan” di mana pasukan tersebut harus diwakili oleh semua Bahagian di LADA;
- b. Penilaian kegagalan keselamatan dan kerugian dalam perkhidmatan akibat bencana harus di analisa;
- c. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;
- d. Perancangan kecemasan harus dibina dan dilaksanakan untuk memastikan proses operasi boleh dijalankan semula di dalam tempoh masa yang diperlukan. Perancangan tersebut harus di selenggara dan diamalkan untuk menjadi asas proses pengurusan yang lain;
- e. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam tempoh yang telah ditetapkan;
- f. Mendokumentasikan proses dan prosedur yang telah dipersetujui;
- g. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;
- h. Membuat penduaan; dan
- i. Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.

8.1 Pematuhan dan Keperluan Perundangan

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	43 DARI 49



PERKARA 08 : PEMATUHAN

Objektif : Meningkatkan tahap penggunaan ICT bagi mengelak dari pelanggaran kepada Polisi ICT LADA.

8.1.1 Pematuhan Polisi

Setiap Pengguna di LADA hendaklah membaca, memahami dan mematuhi Polisi ICT LADA dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua

Semua aset ICT di LADA termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua Jabatan berhak untuk memantau aktiviti Pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.

8.1.2 Keperluan Perundangan

Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua Pengguna di LADA : Semua

- a. Arahan Keselamatan;
- b. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”;
- c. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS);
- d. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
- e. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”;
- f. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
- g. Akta Tanda Tangan Digital 1997;
- h. Akta Jenayah Komputer 1997;
- i. Akta Hak Cipta (Pindaan) Tahun 1997;
- j. Akta Komunikasi dan Multimedia 1998; dan
- k. Akta Aktiviti Kerajaan Elektronik 2007.

Garis Panduan Mengenai Tatacara Memohon Kelulusan Projek ICT

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	44 DARI 49



LAMPIRAN 1

1. Skop projek ICT yang perlu mendapatkan kelulusan Jawatankuasa Pemandu ICT Kementerian LADA (JPICT LADA) adalah seperti berikut:

(a) Projek Baru

Projek baru bermaksud projek pengkomputeran yang melibatkan salah satu atau gabungan aktiviti-aktiviti perolehan perkakasan, perisian dan/atau perkhidmatan ICT, untuk membangunkan projek ICT agensi.

- i. Perkakasan komputer yang dimaksudkan merangkumi semua jenis alat-alat input/output (contoh: pencetak dan pengimbas), pemprosesan, storan data, peralatan rangkaian dan multimedia (contoh: persidangan video (video conferencing)) kecuali alat-alat seperti komponen alat ganti, barang pakai habis (consumable item), aksesori dan perabot komputer.
- ii. Perisian komputer yang dimaksudkan merangkumi semua jenis perisian sistem dan perisian aplikasi. Perisian sistem merangkumi sistem operasi, pangkalan data dan perisian bagi membangunkan sistem. Perisian aplikasi adalah sistem aplikasi yang dibangunkan ataupun pakej sedia ada (off-the-shelf) untuk kegunaan tertentu (contoh: Sistem Perakaunan, Sistem Personel dan Sistem Pengurusan Inventori) dan perisian yang digunakan untuk menyokong kerja-kerja harian seperti penyediaan dokumen.
- iii. Perkhidmatan ICT yang dimaksudkan merangkumi semua jenis perkhidmatan teknikal yang diperolehi daripada syarikat perunding swasta, kontraktor dan syarikat-syarikat lain yang berkaitan seperti pembangunan sistem, pemasangan sistem, infrastruktur rangkaian, talian internet, web hosting, kemasukan data, pemindahan data, migrasi sistem, pemulihan data, langganan maklumat dalam talian dan seumpamanya.

(b) Peningkatan Sistem

Peningkatan sistem bermaksud mempertingkatkan keupayaan perkakasan, perisian, rangkaian dan/atau perkhidmatan ICT. Contoh peningkatan sistem adalah seperti peningkatan perkakasan dari segi konfigurasi dan kapasiti. Peningkatan perisian merangkumi pengemaskinian fungsi-fungsi di dalam sistem ICT sedia ada kepada tahap yang lebih baik. Contoh peningkatan rangkaian adalah seperti peningkatan saiz jalur lebar (bandwidth), peluasan rangkaian dan seumpamanya. Peningkatan perkhidmatan pula merangkumi pertambahan skop perkhidmatan yang sedia ada.

(c) Pertambahan Peralatan

Pertambahan peralatan bermaksud menambahkan bilangan bagi mana-mana perkara di bawah kategori perkakasan, perisian dan/atau rangkaian bagi projek ICT sedia ada.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	45 DARI 49



(d) Perluasan Sistem

Perluasan (roll-out) sistem bermaksud memperkembangkan pelaksanaan projek ICT daripada lokasi sedia ada ke lokasi-lokasi lain atau dengan menambah bilangan pengguna di lokasi yang sama ataupun kedua-duanya sekali.

2. Skop dan had nilai projek ICT yang memerlukan kelulusan JPICT adalah seperti berikut:

(a) Bagi Permohonan Projek ICT yang MELIBATKAN pembangunan Sistem Aplikasi :

- i. Perolehan ICT yang bernilai RM500,000 atau lebih hendaklah mendapat kelulusan teknikal JTICT MAMPU; dan
- ii. Perolehan ICT yang bernilai kurang daripada RM500,000 hendaklah mendapat kelulusan JPICT MOF.

(b) Bagi Permohonan Projek ICT yang TIDAK MELIBATKAN pembangunan Sistem Aplikasi:

- i. Perolehan ICT yang bernilai RM3 juta atau lebih hendaklah mendapat kelulusan teknikal JTICT MAMPU;
 - ii. Perolehan ICT bernilai RM500,000 dan kurang daripada RM3 juta hendaklah mendapat kelulusan teknikal daripada JPICT MOF;
 - iii. Perolehan ICT bernilai lebih daripada RM50,000 dan kurang daripada RM500,000 hendaklah mendapat kelulusan teknikal daripada JPICT LADA;
 - iv. Perolehan ICT bernilai sehingga RM50,000 hendaklah mendapat kelulusan daripada Ketua Agensi dan tertakluk kepada Surat Pekeliling Perbendaharaan Bil. 12 Tahun 2007 mengenai Had Nilai dan Syarat-syarat Pembelian Terus Bagi Bekalan dan Perkhidmatan. Pandangan teknikal daripada Bahagian Teknologi Maklumat LADA hendaklah diperoleh terlebih dahulu bagi perolehan yang memerlukan kepakaran teknikal; dan
 - v. Agensi hendaklah memastikan supaya mekanisme pemantauan pelaksanaan perolehan ICT diperkemas supaya perolehan yang dibuat adalah berdasarkan kepada keperluan sebenar dan dengan perbelanjaan yang berhemah serta mematuhi peraturan-peraturan semasa yang berkaitan.
3. Projek-projek ICT yang hendak dikemukakan kepada JPICT MOF perlu mendapat kelulusan daripada JPICT agensi terlebih dahulu.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	46 DARI 49



4. Semua perolehan ICT yang telah diluluskan di peringkat JPICT dan memerlukan kelulusan teknikal JTICT di MAMPU hendaklah dikemukakan melalui Urus setia JPICT.
5. Semua perolehan ICT sewajarnya berdasarkan kepada Pelan Strategik ICT (ISP). JPICT akan memberi keutamaan kepada projek ICT yang telah dirancang di dalam ISP.
6. Untuk projek-projek yang diluluskan oleh JPICT, agensi-agensi yang memohon perlu mengemukakan laporan kemajuan kepada Urus setia JPICT setiap enam (6) bulan dari tarikh kelulusan sehingga projek selesai.
7. Tempoh sah laku kelulusan JPICT adalah selama tiga (3) tahun dari tarikh surat kelulusan. Sekiranya projek yang diluluskan tidak dilaksanakan dalam tempoh tersebut, agensi hendaklah memohon semula kelulusan JPICT sebelum melaksanakan projek ICT tersebut.
8. Semua agensi hendaklah mematuhi garis panduan yang dikemukakan di dalam memohon kelulusan teknikal perolehan ICT daripada JPICT.

Sebarang pertanyaan lanjut mengenai permohonan projek ICT boleh menghubungi terus Urus setia JPICT MOF melalui e-mel jpictmof@treasury.gov.my.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	47 DARI 49



LAMPIRAN 2

Garis Panduan untuk Pembangunan Sistem Aplikasi dan Pangkalan Data

1. Bahagian (pengguna utama) hendaklah memperuntukkan seorang atau lebih kakitangan sebagai wakil tetap yang dapat meluangkan masa yang cukup sepanjang proses pembangunan dan kerja-kerja berkaitan dengan projek.
2. Bagi aplikasi yang besar (projek pengkomputeran Bahagian), Jawatankuasa Teknikal dan Jawatankuasa Pemandu di peringkat Bahagian perlu diwujudkan.
3. Bagi sistem aplikasi yang melibatkan pelbagai Bahagian, maka setiap Bahagian perlu mempunyai wakil tetap bagi menganggotai Jawatankuasa Teknikal dan Jawatankuasa Pemandu.
4. Cadangan Sistem (System Proposal) perlu dibentangkan kepada pengguna untuk ulasan dan persetujuan serta ditandatangani oleh pengguna.
5. Bagi sistem yang melibatkan fungsi dan prosedur tertentu, subject matter expert perlu dilibatkan dalam mereka bentuk kawalan yang berkaitan dengan subject matter (contoh: Bagi sistem yang melibatkan fungsi dan prosedur kewangan, Akauntan perlu dilibatkan dalam mereka bentuk kawalan yang berkaitan dengan perakaunan).
6. Pengujian dan prosedur penerimaan sistem di setiap peringkat (unit test, component test dan integration test) perlu dibuat.
7. Pengguna perlu menandatangani Penerimaan Sementara dan Penerimaan Akhir sistem aplikasi.
8. Pelaksanaan kawalan keselamatan ICT dalam aplikasi adalah perlu bagi menghalang capaian yang tidak sah, ubahsuaian, penyebaran maklumat dan kerosakan maklumat.
9. Source code dan hak cipta bagi sesuatu aplikasi yang dibangunkan secara dalaman ataupun secara bersama dengan pembekal perlu dinyatakan dalam kontrak sebagai Hak Kerajaan Malaysia.
10. Bagi aplikasi yang dibangunkan oleh pembekal, klausa mengenai pemindahan teknologi (Transfer of Technology) hendaklah dinyatakan dalam dokumen kontrak.
11. SUB setiap Bahagian yang terlibat akan mempengerusikan mesyuarat kemajuan projek bagi tujuan pemantauan.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	48 DARI 49



LAMPIRAN 3

SURAT AKUAN PEMATUHAN POLISI ICT LEMBAGA PEMBANGUNAN LANGKAWI

Nama (Huruf Besar) : _____
 No. Kad Pengenalan : _____
 Jawatan : _____
 Bahagian : _____

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :

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

Tandatangan : _____
 Tarikh : _____

Pengesahan BTM

()

Tarikh : _____

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT LADA	VERSI 1.0	3 JULAI 2011	49 DARI 49