DASAR KESELAMATAN ICT

LEMBAGA URUS AIR SELANGOR (LUAS)

13 MAC 2018

VERSI 1.3

SEJARAH DOKUMEN

BIL.	TARIKH PENYEDIAAN/ PINDAAN	VERSI	KELULUSAN	TARIKH KUATKUASA
1	20 MAC 2012	1.0	JPICT BIL. 1/2012	1 OGOS 2012
2	12 OGOS 2014	1.1	JPICT BIL. 2/2014	13 OGOS 2014
3	11 FEBRUARI 2016	1.2	JPICT BIL. 1/2017	29 MAC 2017
4	19 FEBRUARI 2018	1.3	JPICT BIL. 1/2018	13 MAC 2018

JADUAL PINDAAN DASAR KESELAMATAN ICT LUAS

BIL.	VERSI	BUTIRAN PINDAAN
1	1.1	**1. 020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga** i. Meminda g) a. ii. Tapisan Keselamatan dan iii. Akta Kawasan Larangan dan Tempat Larangan 1959 kepada ii. Arahan Keselamatan; dan ii. Menambahbaik borang Akuan Pematuhan DKICT dengan memasukkan klausa, 'Saya bersih daripada sebarang rekod sabitan salah laku jenayah lampau;' **2. 030101 Inventori Aset ICT** i. Meminda peranan Pentadbir Sistem dan Semua kepada Pegawai Aset dan Semua. **3. 030201 Pengelasan Maklumat** i. Meminda peranan Pegawai Aset ICT dan kepada Pengarah. **4. 060802 Pengurusan Mel Elektronik (E-mel)** i. Meminda perkara i) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; kepada i) Pengguna hendaklah memberikan keutamaan kepada e-mel rasmi LUAS untuk digunakan dalam sebarang urusan rasmi; ii. Meminda perkara l) Penghantaran dokumen rasmi hendaklah menggunakan e-mel rasmi LUAS sahaja dan pastikan alamat e-mel penerima adalah betul; kepada l) Pengguna hendaklah memastikan alamat e-mel penerima adalah betul bagi penghantaran dokumen rasmi; iii. Meminda perkara p) Hanya kakitangan LUAS sahaja boleh dipertimbangkan untuk mendapat kemudahan e-mel rasmi LUAS; kepada p) Semua kakitangan LUAS layak diperuntukkan akaun e-mel rasmi LUAS, manakala selain daripada itu akan dipertimbangkan dengan kebenaran Pengarah;

JADUAL PINDAAN DASAR KESELAMATAN ICT LUAS

BIL.	VERSI	BUTIRAN PINDAAN	M.S
1	1.2	**010103 Penyelenggaraan Dasar** Menyemak semula dokumen sekurang-kurangnya **setahun** sekali atau mengikut keperluan bagi memastikan dokumen sentiasa relevan **Dipinda kepada** Menyemak semula dokumen sekurang-kurangnya **dua tahun** sekali atau mengikut keperluan bagi memastikan dokumen sentiasa relevan.	**17**
		020102 Ketua Pegawai Maklumat (CIO) Jawatan Ketua Pegawai Maklumat (CIO) adalah disandang oleh Ketua Penolong Pengarah (**Teknikal**). **Dipinda kepada** Jawatan Ketua Pegawai Maklumat (CIO) adalah disandang oleh Ketua Penolong Pengarah (**Pengurusan Lembangan Sungai dan Pantai**).	**18**
		020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga g) Akses kepada aset ICT LUAS perlu berlandaskan perjanjian kontrak. Perjanjian yang dimeterai perlu mematuhi perkara-perkara berikut: a. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga, perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai. i. DKICT LUAS; ii. Arahan Keselamatan; iii. Arahan Teknologi Maklumat 2007 (*IT Instructions*); iv. Perakuan Akta Rahsia Rasmi 1972; dan v. Hak Harta Intelek. **Ditambahkan dengan** **vi. Akta Kawasan Larangan dan Tempat Larangan 1959.**	**30**

JADUAL PINDAAN DASAR KESELAMATAN ICT LUAS

BIL.	VERSI	BUTIRAN PINDAAN	M.S
1	1.2	**040101 Sebelum Perkhidmatan** b) **Menjalankan tapisan keselamatan** untuk pegawai dan kakitangan LUAS, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan selaras dengan keperluan perkhidmatan; dan **Dipinda kepada** **Memastikan** pegawai dan kakitangan LUAS, pembekal, pakar runding dan pihak-pihak lain **menandatangani surat Akuan Pematuhan DKICT dan Borang Non-Disclosure Agreement** yang berkepentingan selaras dengan keperluan perkhidmatan; dan	34
		040102 Semasa Perkhidmatan 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. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada **Unit Sumber Manusia** atau Unit Teknologi Maklumat. **Dipinda kepada** Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada **Unit Pengurusan Sumber Manusia dan Integriti** atau Unit Teknologi Maklumat.	**35**
		040104 Bertukar atau Tamat Perkhidmatan Ketua Unit PSM dipinda kepada Ketua Unit PSMI;	**36**
		050102 Kawalan Masuk Fizikal c) Setiap pelawat hendaklah mendapatkan **Pas Keselamatan Pelawat di pintu Kawalan Utama Bangunan**. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan **Dipinda kepada** Setiap pelawat hendaklah mendapatkan **Pas Pelawat di Kaunter Tingkat 13**. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan	**38**

JADUAL PINDAAN DASAR KESELAMATAN ICT LUAS

BIL.	VERSI	BUTIRAN PINDAAN	M.S
1	1.2	**050201 Peralatan ICT** m) Peralatan ICT yang hendak dibawa keluar dari premis LUAS, perlulah mendapat kelulusan **Pegawai Aset ICT** atau **Penyelaras IT Bahagian** dan direkodkan bagi tujuan pemantauan; **Dipinda kepada** Peralatan ICT yang hendak dibawa keluar dari premis LUAS, perlulah mendapat kelulusan **Pegawai Aset** atau **Ketua UTM** dan direkodkan bagi tujuan pemantauan;	**42**
		050201 Peralatan ICT n) Peralatan ICT yang hilang hendaklah dilaporkan kepada **ICTSO** dan **Pegawai Aset ICT** dengan segera; **Dipinda kepada** Peralatan ICT yang hilang hendaklah dilaporkan kepada **Ketua UTM** dan **Pegawai Aset** dengan segera;	**42**
		050201 Peralatan ICT q) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran **Pegawai Aset ICT**; **Dipinda kepada** Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran **Pegawai Aset**;	**42**
		050201 Peralatan ICT r) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada **Pegawai Aset ICT** untuk dibaik pulih; **Dipinda kepada** Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada **Pegawai Aset** untuk dibaik pulih;	**42**

JADUAL PINDAAN DASAR KESELAMATAN ICT LUAS

BIL.	VERSI	BUTIRAN PINDAAN	M.S
1	1.2	**050205 Pelupusan** c) **Pegawai Aset ICT** akan mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; **Dipinda kepada** **Pegawai Aset** akan mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;	**45**
		050205 Pelupusan e) **Pegawai Aset ICT** bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem Tatacara Pengurusan Aset (TPA); **Dipinda kepada** **Pegawai Aset** bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem Tatacara Pengurusan Aset (TPA);	**46**
		050206 Penyelenggaraan Perkakasan f) Semua penyelenggaraan mestilah mendapat kebenaran daripada Ketua UTM. **Dipinda kepada** Semua penyelenggaraan mestilah mendapat kebenaran daripada **Pegawai Aset** atau Ketua UTM.	**47**
		050207 Peralatan di luar Premis c) Sebarang kehilangan peralatan adalah di bawah tanggungjawab individu yang membawa keluar peralatan tersebut. **Dipinda kepada** Sebarang kehilangan peralatan adalah di bawah tanggungjawab individu yang membawa keluar peralatan tersebut **dan hendaklah melaporkan kepada pihak Berkuasa dengan segera.**	**48**

JADUAL PINDAAN DASAR KESELAMATAN ICT LUAS

BIL.	VERSI	BUTIRAN PINDAAN	M.S
1	1.2	**050301 Kawalan Persekitaran** Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk perolehan, menyewa, mengubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada **Pejabat Ketua Pegawai Keselamatan Negeri Selangor.** Dipinda kepada Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk perolehan, menyewa, mengubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada **Ketua BKP.**	**48**
		050302 Bekalan Kuasa Peranan Pengurusan Bangunan; Pegawai Keselamatan; Ketua UTM; **Dipinda kepada** Peranan Pengurusan Bangunan ; Ketua BKP; Pegawai Keselamatan; Ketua UTM; Pegawai Aset	**49**
		060102 Kawalan Perubahan e) Setiap perubahan hendaklah dibuat dengan menggunakan Borang Kawalan Perubahan. **Dipinda kepada** Setiap perubahan hendaklah direkodkan dan difailkan secara teratur.	**53**

JADUAL PINDAAN DASAR KESELAMATAN ICT LUAS

BIL.	VERSI	BUTIRAN PINDAAN	M.S
1	1.2	**060104 Prosedur Pengurusan Insiden** a) Mengenalpasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian tanpa kebenaran; b) Menyedia pelan kontigensi dan mengaktifkan pelan kesinambungan Perkhidmatan; c) Menyimpan jejak audit dan memelihara bukti; dan d) Menyediakan tindakan pemulihan segera. Laporan insiden kemudiannya akan dimaklumkan kepada CERT Selangor (*Selangor Computer Emergency Response Team*) jika memerlukan khidmat nasihat dan bantuan. **Dipinda kepada** a) Ketua UTM akan mengenalpasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian tanpa kebenaran; b) Laporan insiden kemudiannya akan dimaklumkan kepada CERT Selangor (*Selangor Computer Emergency Response Team*) jika memerlukan khidmat nasihat dan bantuan. c) Ketua UTM akan menyediakan laporan siasatan dan ICTSO akan mengesahkan sekiranya Pelan Kesinambungan Perkhidmatan (PKP) perlu diaktifkan atau sebaliknya. Pengesahan akan dihantar kepada CIO untuk mengaktifkan PKP d) Laporan insiden yang tidak memerlukan PKP akan diteruskan untuk tindakan pemulihan.	**54**
		060302 Penerimaan Sistem Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. **Dipinda kepada** Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. Kriteria ini hendaklah merangkumi perkara berikut: 1. Memenuhi keperluan dan kehendak pengguna; 2. Menggunakan perisian pembangunan yang sah; 3. Menggunakan teknologi terkini; 4. Memenuhi ciri-ciri keselamatan bagi mengelakkan risiko pencerobohan dan sebagainya; dan 5. Memenuhi keperluan-keperluan teknologi semasa dan akan datang. (Contoh: mampu menggunakan pelbagai platform dan *IPV6 Ready*)	**55**

JADUAL PINDAAN DASAR KESELAMATAN ICT LUAS

BIL.	VERSI	BUTIRAN PINDAAN	M.S
1	1.2	**060501 Backup** e) LUAS hendaklah menyimpan sekurang-kurangnya tiga (3) generasi *backup*; dan **Perkara e) dikeluarkan dari DKICT.**	**57**
		060802 Pengurusan Mel Elektronik (E-mel) s) Unit Sumber Manusia perlu memaklumkan sebarang status pengguna (bertukar tempat bekerja, bersara, diberhentikan, tidak dapat dikesan bertukar keluar atau masuk ke LUAS di bahagian masing-masing bagi tujuan pengemaskinian e-mel yang terlibat; **Dipinda kepada** Unit Pengurusan Sumber Manusia dan Integriti perlu memaklumkan kepada UTM sebarang status pengguna (bertukar tempat bekerja, bersara, diberhentikan, tidak dapat dikesan bertukar keluar atau masuk ke LUAS di bahagian masing-masing bagi tujuan pengemaskinian e-mel yang terlibat;	**63**
		070203 Pengurusan Kata Laluan j) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan **Dipinda kepada** Kata laluan hendaklah ditukar selepas 365 hari atau selepas tempoh masa yang bersesuaian; dan	**71**
		080402 Pembangunan Perisian secara *Outsource* Peranan UTM; Pentadbir Sistem; **Dipinda kepada** Pemilik Sistem; Ketua UTM;Pentadbir Sistem;	**81**

BIL.	VERSI	BUTIRAN PINDAAN	M.S
1	1.3	**020108 Pentadbir Laman Web** Peranan ; Pentadbir Laman Web **Dipinda kepada** Peranan ; Pentadbir Laman Web a) Unit Korporat (perkara a.) b) Unit Teknologi Maklumat (selain perkara a.)	**34**
		050103 Kawasan Larangan Kawasan larangan di LUAS adalah: a) Bilik server ibu pejabat LUAS dan cawangan; b) Mana-mana kawasan yang telah/akan diisytiharkan sebagai larangan. **Dipinda kepada** Kawasan larangan di LUAS adalah: a) Bilik server ibu pejabat LUAS; **b) Makmal di Pejabat Cawangan Lembaga Urus Air Selangor (LUAS) Seksyen 15;** c) Mana-mana kawasan yang telah/akan diisytiharkan sebagai larangan.	**48**

ISI KANDUNGAN

SEJARAH DOKUMEN 1
JADUAL PINDAAN DASAR 2
PENGENALAN 16
OBJEKTIF 16
PENYATAAN DASAR 17
SKOP 18
PRINSIP-PRINSIP 21
PENILAIAN RISIKO KESELAMATAN ICT 25
BIDANG 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR 25
0101 Dasar Keselamatan ICT 25
010101 Pelaksanaan Dasar 25
010102 Penyebaran Dasar 25
010103 Penyelenggaraan Dasar 25
010104 Pengecualian Dasar 26
BIDANG 02 ORGANISASI KESELAMATAN 27
0201 Infrastruktur Organisasi Dalaman 27
020101 Pengarah 27
020102 Ketua Pegawai Maklumat (CIO) 27
020103 Ketua Unit Teknologi Maklumat 28
020104 Pegawai Keselamatan ICT (ICTSO) 29
020105 Pentadbir Sistem 31
020106 Pentadbir Rangkaian 32
020107 Pentadbir Pangkalan Data 33
020108 Pentadbir Laman Web 34
020109 Pengguna 35
020110 Jawatankuasa Pemandu ICT LUAS (JPICT) 36
0202 Pihak Ketiga 38
020201 Keperluan Keselamatan Kontrak dengan Pihak ketiga 38
BIDANG 03 PENGURUSAN ASET 40
0301 Akauntabiliti Aset 40
030101 Inventori Aset ICT 40
0302 Pengelasan dan Pengendalian Maklumat 41
030201 Pengelasan Maklumat 41
030201 Pengendalian Maklumat 41

BIDANG 04 KESELAMATAN SUMBER MANUSIA..... 43
0401 Keselamatan Sumber Manusia Dalam Tugas Harian..... 43
040101 Sebelum Perkhidmatan..... 43
040102 Semasa Perkhidmatan..... 44
040103 Program Kesedaran Keselamatan ICT..... 45
040104 Bertukar atau Tamat Perkhidmatan..... 45
BIDANG 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN..... 46
0501 Keselamatan Kawasan..... 46
050101 Kawalan Kawasan..... 46
050102 Kawalan Masuk Fizikal..... 47
050103 Kawasan Larangan..... 48
0502 Keselamatan Peralatan..... 50
050201 Peralatan ICT..... 50
050202 Media Storan..... 52
050203 Media Tandatangan Digital..... 53
050204 Media Perisian dan Aplikasi..... 54
050205 Pelupusan..... 54
050206 Penyelenggaraan Perkakasan..... 56
050207 Peralatan di Luar Premis..... 57
0503 Keselamatan Persekitaran..... 57
050301 Kawalan Persekitaran..... 57
050302 Bekalan Kuasa..... 58
050303 Kabel..... 59
050304 Prosedur Kecemasan..... 59
0504 Keselamatan Dokumen..... 60
BIDANG 06 PENGURUSAN OPERASI DAN KOMUNIKASI..... 61
0601 Pengurusan Prosedur Operasi..... 61
060101 Pengendalian Dokumen Prosedur Operasi..... 61
060102 Kawalan Perubahan..... 61
060103 Pengasingan Tugas dan Tanggungjawab..... 62
060104 Prosedur Pengurusan Insiden..... 63
0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga..... 63
060201 Perkhidmatan Penyampaian..... 63
0603 Perancangan dan Penerimaan Sistem..... 64
060301 Perancangan Kapasiti..... 64
060302 Penerimaan Sistem..... 64
0604 Perisian Merbahaya..... 65
060401 Perlindungan dari Perisian Merbahaya..... 65
060402 Perlindungan dari *Mobile Code*..... 66

0605 Housekeeping 66
060501 Backup..... 66
0606 Pengurusan Rangkaian 67
060601 Kawalan Infrastruktur Rangkaian..... 67
0607 Pengurusan Media 68
060701 Media Mudah Alih..... 68
060702 Prosedur Pengendalian Media..... 69
060703 Keselamatan Sistem Dokumentasi..... 69
0608 Pengurusan Pertukaran Maklumat..... 70
060801 Pertukaran Maklumat..... 70
060802 Pengurusan Mel Elektronik (E-mel) 70
0609 Perkhidmatan E-Dagang (*Electronic Commerce Services*) 73
060901 E-Dagang..... 73
060902 Maklumat Umum..... 73
0610 Pengurusan Penyampaian Perkhidmatan Pembekal, Pakar Runding dan Pihak-Pihak Lain Yang Terlibat..... 74
0611 Pemantauan..... 75
061101 Pengauditan dan Forensik ICT..... 75
061102 Jejak Audit..... 76
061103 Sistem Log..... 76
061104 Pemantauan Log..... 77
BIDANG 07 KAWALAN CAPAIAN..... 78
0701 Dasar Kawalan Capaian..... 78
070101 Keperluan Kawalan Capaian..... 78
0702 Pengurusan Capaian Pengguna..... 79
070201 Akaun Pengguna..... 79
070202 Hak Capaian (Privilege)..... 79
070203 Pengurusan Kata Laluan..... 80
070204 *Clear Desk* dan *Clear Screen*..... 81
0703 Kawalan Capaian Rangkaian..... 81
070301 Capaian Rangkaian..... 81
070302 Capaian Internet..... 82
0704 Kawalan Capaian Sistem Pengoperasian 83
070401 Capaian Sistem Pengoperasian..... 83
0705 Kawalan Capaian Aplikasi dan Maklumat..... 85
070501 Capaian Aplikasi dan Maklumat..... 85
0706 Peralatan Mudah Alih dan Jarak Jauh..... 86
070601 Peralatan Mudah Alih 86
070602 Kerja Jarak Jauh 86

BIDANG 08 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM..... 87
0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi..... 87
080101 Keperluan Keselamatan Sistem Maklumat..... 87
080102 Pengesahan Data *Input* dan *Output*..... 88
080103 Kawalan Prosesan..... 88
0802 Kawalan Kriptografi..... 88
080201 Enkripsi..... 88
080202 Tandatangan Digital..... 88
080203 Penggunaan Infrastruktur Kunci Awam (PKI)..... 88
0803 Keselamatan Fail Sistem..... 89
080301 Kawalan Fail Sistem..... 89
0804 Keselamatan Dalam Proses Pembangunan dan Sokongan Sistem..... 90
080401 Prosedur Kawalan Perubahan..... 90
080402 Pembangunan Perisian Secara *Outsource*..... 90
0805 Kawalan Teknikal Keterdedahan (*vulnerability*)..... 91
080501 Kawalan dari Ancaman Teknikal..... 91
BIDANG 09 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN..... 92
0901 Mekanisme Pelaporan Insiden Keselamatan ICT..... 92
090101 Mekanisme Pelaporan..... 92
0902 Pengurusan Maklumat Insiden Keselamatan ICT..... 94
090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT..... 94
BIDANG 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN..... 95
1001 Dasar Kesinambungan Perkhidmatan..... 95
100101 Pelan Pengurusan Kesinambungan Perkhidmatan..... 95
BIDANG 11 PEMATUHAN..... 97
1101 Pematuhan dan Keperluan Perundangan..... 97
110101 Pematuhan Dasar..... 97
110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal..... 97
110103 Pematuhan Keperluan Audit..... 97
110104 Keperluan Perundangan..... 98
110105 Pelanggaran Perundangan..... 98
Glosari..... 99
Lampiran 1..... 106
Lampiran 2..... 107
Lampiran 3..... 109

PENGENALAN

Lembaga Urus Air Selangor (LUAS) berperanan untuk menyediakan perkhidmatan bagi perancangan, pembangunan dan pengurusan sumber manusia sektor awam yang cemerlang berteraskan profesionalisme, integriti dan teknologi. Dokumen ini menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka bagi melindungi aset ICT LUAS. Dokumen ini diguna pakai oleh semua pihak kakitangan, pengguna dan pembekal yang menyediakan perkhidmatan, mencapai dan menggunakan aset dan sistem aplikasi ICT di LUAS.

OBJEKTIF

Dasar Keselamatan ICT (DKICT) LUAS diwujudkan untuk menjamin kesinambungan urusan LUAS dengan meminimumkan kesan insiden keselamatan ICT.

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

Manakala, objektif utama DKICT LUAS adalah seperti berikut:

1) Memastikan kelancaran operasi LUAS yang berlandaskan ICT dengan mencegah serta meminimumkan kerosakan atau kemusnahan aset ICT LUAS;

2) Melindungi kepentingan pihak-pihak yang bergantung kepada aset maklumat daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, tidak boleh disangkal, kebolehsediaan dan kesahihan maklumat dan komunikasi(*CIA*^{3});

3) Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan;

4) Meningkatkan tahap kesedaran keselamatan ICT kepada para kakitangan, pengguna dan pembekal;

5) Memperkemaskan pengurusan risiko;

6) Mencegah penyalahgunaan atau kecurian aset ICT LUAS; dan

7) Melindungi aset ICT daripada penyelewengan oleh kakitangan, pengguna dan pembekal.

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

Keselamatan ICT adalah bermaksud keadaan dimana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Terdapat empat (4) komponen asas keselamatan ICT, iaitu:

1) Melindungi maklumat rahsia rasmi dan maklumat rasmi LUAS dari capaian tanpa kuasa yang sah;

2) Menjamin setiap maklumat adalah tepat dan sempurna;

3) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

4) Memastikan akses hanya kepada pengguna-pengguna yang sah atau penerimaan maklumat dari sumber-sumber yang sah.

DKICT LUAS 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:

1) **Kerahsiaan -** maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan akses tanpa kebenaran;

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

3) **Tidak boleh disangkal** - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;

4) **Kesahihan** - Data dan maklumat hendaklah dijamin kesahihannya; dan

5) **Ketersediaan** - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

SKOP

Aset ICT LUAS terdiri daripada organisasi, manusia, perisian, perkakasan, telekomunikasi, kemudahan ICT dan data. DKICT LUAS telah menetapkan keperluan-keperluan asas keselamatan seperti berikut:

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

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

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, DKICT LUAS ini merangkumi perlindungan ke atas semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui penubuhan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

1) Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan LUAS. Contoh peralatan dan periferal seperti komputer, pelayan, *firewall,* pencetak, peralatan media, peralatan komunikasi dan alat-alat prasarana seperti *Uninterruptible Power Supply (UPS)* dan sebagainya;

2) Perisian

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

3) Perkhidmatan

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

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

ii. Sistem halangan akses seperti sistem kad akses; dan

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

4) Data dan maklumat

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

5) Manusia

Semua pengguna infrastruktur ICT LUAS yang dibenarkan, termasuk kakitangan, pengguna dan pembekal. Individu yang mempunyai pengetahuan untuk melaksanakan skop kerja harian LUAS bagi mencapai misi dan objektif LUAS. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan;

6) Media storan

Semua media storan dan peralatan yang berkaitan seperti disket, storan mudah alih, kartrij, CD-ROM, pita, cakera, pemacu cakera, pemacu pita dan lain-lain;

7) Media komunikasi

Semua peralatan berkaitan komunikasi seperti pelayan rangkaian, *gateway, bridge, router*, peralatan PABX, *wireless* LAN, talian ISDN, peralatan *video conferencing, modem*, PCMCIA, kabel rangkaian, NIC, *switches, hub* dan lain-lain;

8) Dokumentasi

Semua dokumen (prosedur dan manual pengguna) yang berkaitan dengan aset ICT, pemasangan dan pengoperasian peralatan dan perisian, sama ada dalam bentuk elektronik atau bukan elektronik;

9) Premis Komputer dan Komunikasi

Semua kemudahan serta premis yang diguna untuk menempatkan perkara 1 hingga 8 di atas. Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada DKICT LUAS dan perlu dipatuhi adalah seperti berikut:

1) Akses Atas Dasar Perlu Mengetahui

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

2) Hak Akses Minimum

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

3) Kebertanggungjawaban/Akauntabiliti

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

Akauntabiliti atau tanggungjawab pengguna termasuklah:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

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

iii. Menentukan maklumat sedia untuk digunakan;

iv. enjaga 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.

4) Pengasingan

Tugas mewujud, menghapus, mengemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan (*unauthorized access*) serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasikan. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian;

5) Pengauditan

Tujuan aktiviti ini ialah untuk mengenalpasti insiden berkaitan keselamatan aset ICT atau keadaan yang mengancam keselamatan aset ICT. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan.

Dengan itu, aset ICT seperti komputer, pelayan, *router, firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau jejak audit (*audit trail)*. Semua log yang berkaitan dengan aset ICT perlu disimpan bagi tujuan jejak audit;

6) Pematuhan

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

7) Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian bagi meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan dan ketidakbolehcapaian. Pemulihan boleh dilakukan melalui proses penduaan (*backup*) dan mewujudkan pelan pemulihan bencana/kesinambungan perkhidmatan (BRP); dan

8) Saling Bergantungan

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

PENILAIAN RISIKO KESELAMATAN ICT

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

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

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat LUAS 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 yang lain.

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

LUAS perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko yang berlaku dan memilih tindakan berikut: -

a) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

b) Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan LUAS;

c) Mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan

d) Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

BIDANG 01
PEMBANGUNAN DAN PENYELENGGARAAN DASAR

0101 Dasar Keselamatan ICT

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

010101 Pelaksanaan Dasar

Pelaksanaan dasar ini akan dijalankan oleh Pengarah dibantu oleh Jawatankuasa Pemandu ICT LUAS (JPICT) yang terdiri daripada: - i. Ketua Pegawai Maklumat (CIO); ii. Ketua Unit Teknologi Maklumat; iii. Pegawai Keselamatan ICT (ICTSO); dan iv. Semua Ketua Bahagian/Seksyen/Unit.	Pengarah; CIO

010102 Penyebaran Dasar

Dasar ini perlu disebarkan kepada semua pengguna yang terlibat dengan infrastruktur ICT LUAS meliputi kakitangan, pengguna dan pembekal.	

010103 Penyelenggaraan Dasar

Dasar Keselamatan ICT LUAS adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur perundangan dan kepentingan sosial.	JPICT; ICTSO

Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT LUAS: a) Mengenal pasti dan menentukan perubahan yang diperlukan; b) Mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan, pertimbangan dan persetujuan Mesyuarat Jawatankuasa Pemandu ICT (JPICT); c) Memaklumkan perubahan yang telah dipersetujui oleh JPICT kepada semua pihak iaitu kakitangan, pengguna dan pembekal; dan d) Menyemak semula dokumen sekurang-kurangnya dua tahun sekali atau mengikut keperluan bagi memastikan dokumen sentiasa relevan.	
010104 Pengecualian Dasar	
Dasar Keselamatan ICT LUAS adalah terpakai dan mestilah dipatuhi oleh semua kakitangan, pengguna serta pembekal ICT LUAS dan tiada pengecualian diberikan.	Semua

BIDANG 02
ORGANISASI KESELAMATAN

0201 Infrastruktur Organisasi Dalaman

Objektif :

Menerangkan peranan dan tanggungjawab semua pihak yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT LUAS.

020102 Pengarah

Peranan dan tanggungjawab Pengarah adalah seperti berikut: a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT LUAS; b) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT LUAS; c) Memastikan semua keperluan LUAS seperti 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 LUAS.	Pengarah

020102 Ketua Pegawai Maklumat (CIO)

Jawatan Ketua Pegawai Maklumat (CIO) adalah disandang oleh Ketua Penolong Pengarah (Pengurusan Lembangan Sungai dan Pantai). Peranan dan tanggungjawab CIO adalah seperti berikut: a) Membantu Pengarah dalam melaksanakan tugas-tugas yang berkaitan Keselamatan ICT; b) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT LUAS;	CIO

c) Bertanggungjawab menyelaras dan mengurus pelan tindakan dan program keselamatan seperti penyediaan DKICT LUAS, pelan latihan dan kesedaran pengguna, pengurusan risiko dan pengauditan; d) Menentukan keperluan keselamatan ICT; dan e) Menguatkuasakan pelaksanaan Dasar Keselamatan LUAS di semua bahagian dan cawangan LUAS.	
020103 Ketua Unit Teknologi Maklumat	
Peranan dan tanggungjawab Ketua Unit Teknologi Maklumat (UTM) adalah seperti berikut: a) Memastikan DKICT LUAS dilaksanakan di peringkat bahagian; b) Memastikan semua kakitangan, perunding, kontraktor dan pembekal yang terlibat dengan bahagian mematuhi dasar, piawaian dan garis panduan keselamatan ICT dan seterusnya melaporkan sebarang insiden berkaitan keselamatan ICT; c) Mengkaji semula aspek-aspek keselamatan fizikal seperti kemudahan *backup* dan persekitaran pejabat yang perlu; d) Melaksanakan keperluan DKICT dalam operasi semasa seperti berikut: i. Pelaksanaan sistem atau aplikasi baru sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baru; ii. Pembelian atau peningkatan perisian dan sistem komputer; iii. Perolehan teknologi dan perkhidmatan komunikasi baru; dan iv. Pelantikan pembekal, perunding atau rakan usaha sama. e) Menyimpan rekod atau laporan terkini tentang ancaman keselamatan. Sebarang perkara atau penemuan ancaman terhadap keselamatan ICT hendaklah dilaporkan kepada ICTSO;	Ketua UTM

f) Membangunkan garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam LUAS yang mematuhi keperluan DKICT LUAS;

g) Membangun, mengkaji semula dan mengemas kini pelan kontingensi keselamatan ICT di bahagian;

h) Melaksanakan sistem kawalan capaian pengguna ke atas aset-aset ICT LUAS;

i) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan LUAS;

j) Menentukan kawalan akses pengguna terhadap aset ICT LUAS;

k) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO;

l) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT LUAS.

020104 Pegawai Keselamatan ICT (ICTSO)

Jawatan Pegawai Keselamatan ICT (ICTSO) adalah disandang oleh Pegawai Teknologi Maklumat.

Peranan dan tanggungjawab ICTSO adalah seperti berikut:

a) Mengurus keseluruhan program keselamatan ICT LUAS;

b) Memberi penerangan dan pendedahan berkenaan DKICT LUAS kepada semua pengguna;

c) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT LUAS;

d) Menjalankan pengurusan risiko;

e) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan LUAS berdasarkan hasil penemuan dan menyediakan laporan mengenainya;

f) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;

g) Mencadangkan langkah-langkah pengukuhan bagi mematuhi dasar-dasar berkaitan keselamatan ICT LUAS;

h) Melaporkan insiden keselamatan ICT kepada Pasukan Tindak Balas Insiden Keselamatan ICT (CERT) Selangor bagi membantu dalam penyiasatan atau pemulihan;

i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;

j) Menjalankan program-program kesedaran mengenai keselamatan ICT;

k) Menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlaku ancaman kepada keselamatan ICT dan menyediakan khidmat nasihat serta langkah pemulihan yang bersesuaian;

l) Memastikan pematuhan DKICT LUAS oleh pihak luaran seperti perunding, kontraktor dan pembekal yang mencapai dan menggunakan aset ICT LUAS untuk tujuan penyelenggaraan, pemasangan, naik taraf dan sebagainya;

m) Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan ICT;

n) Memastikan DKICT LUAS dikemas kini sesuai dengan perubahan teknologi, arahan LUAS dan ancaman-ancaman dari semasa ke semasa; dan

o) Memastikan Pelan Strategik ICT LUAS mengandungi aspek keselamatan ICT.

020105 Pentadbir Sistem

Peranan dan tanggungjawab Pentadbir Sistem adalah seperti berikut: a) Memastikan ketepatan dan menyekat kebenaran capaian serta-merta apabila tidak lagi diperlukan atau melanggar DKICT LUAS; b) Melaksanakan prinsip-prinsip DKICT dan menjaga kerahsiaan maklumat LUAS; c) Menentukan ketepatan dan kesempurnaan kawalan capaian pengguna berdasarkan kepada garis panduan keselamatan ICT LUAS; d) Mengambil tindakan segera dan bersesuaian apabila dimaklumkan oleh bahagian sekiranya terdapat pegawai yang telah tamat perkhidmatan, bertukar, berkursus panjang atau berlaku perubahan dalam bidang tugas; e) Memantau aktiviti pengguna yang diberi keutamaan capaian yang tinggi dan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam DKICT LUAS; f) Memantau aktiviti capaian harian sistem aplikasi pengguna; g) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; h) Menganalisa dan menyimpan rekod jejak audit; i) Menyediakan laporan mengenai aktiviti capaian secara berkala; j) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.	Pentabir Sistem

020106 Pentadbir Rangkaian

Peranan dan tanggungjawab Pentadbir Rangkaian adalah seperti berikut: a) Memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di LUAS beroperasi sepanjang masa; b) Memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna; c) Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada; d) Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil; e) Memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian; f) Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian LUAS secara tidak sah seperti melalui peralatan *modem* dan *dial-up*; dan g) Menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian.	Pentabir Sistem

020107 Pentadbir Pangkalan Data

Peranan dan tanggungjawab Pentadbir Pangkalan Data adalah seperti berikut: a) Melaksanakan pemasangan *(installation)* dan penambahbaikan pangkalan data serta perisian lain yang berkaitan dengan pangkalan data; b) Memastikan pangkalan data boleh digunakan pada setiap masa; c) Melaksanakan pemantauan dan penyelenggaraan yang berterusan ke atas pangkalan data; d) Melaksanakan proses *backup* dan *restoration* ke atas pangkalan data; e) Memastikan aktiviti pentadbiran pangkalan data seperti prestasi capaian, penyelesaian masalah pangkalan data dan proses pengemaskinian data dilaksanakan dengan teratur; f) Melaksanakan polisi pengguna pangkalan data berdasarkan kepada prinsip-prinsip DKICT; g) Melaksanakan proses pembersihan data (*housekeeping*) di dalam pangkalan data; dan h) Melaporkan sebarang insiden pelanggaran dasar keselamatan pangkalan data kepada ICTSO.	Pentadbir Pangkalan Data

020108 Pentadbir Laman Web

Peranan dan tanggungjawab Pentadbir Laman Web adalah seperti berikut: a) Memastikan kandungan laman web sentiasa sahih dan terkini; b) Memantau prestasi capaian dan menjalankan penilaian prestasi untuk memastikan akses yang lancar; c) Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai muka laman; Menghadkan capaian Pentadbir Laman Web bahagian ke *web server;* d) Mengasingkan kandungan dan aplikasi atas talian untuk capaian secara Intranet dan Internet portal LUAS; e) Memastikan data-data SULIT tidak boleh disalin atau dicetak oleh orang yang tidak berhak; f) Memastikan reka bentuk web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; g) Melaksanakan *housekeeping* keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di *web server*; h) Melaksanakan proses *backup* dan *restoration* secara berkala; dan i) Melaporkan sebarang pelanggaran keselamatan laman portal kepada ICTSO.	Pentadbir Laman Web Unit Korporat (perkara a.) ; Unit Teknologi Maklumat (selain perkara a.)

020109 Pengguna	
Peranan dan tanggungjawab pengguna adalah seperti berikut: a) Pengguna warga LUAS dan pihak ketiga perlu membaca, memahami dan mematuhi DKICT LUAS; b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; d) Melaksanakan prinsip-prinsip DKICT dan menjaga kerahsiaan maklumat LUAS; e) Melaksanakan langkah-langkah perlindungan seperti berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; Menentukan maklumat sedia untuk digunakan; iii. Menjaga kerahsiaan kata laluan; iv. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan ICT yang ditetapkan; v. Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vi. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. f) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; g) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan h) Menandatangani Surat Akuan Pematuhan DKICT Lembaga Urus Air Selangor (LUAS) sebagaimana **Lampiran 1**.	Pengguna Pengarah

020110 Jawatankuasa Pemandu ICT (LUAS)

Pengarah

Keanggotaan JPICT adalah seperti berikut:

Pengerusi : Pengarah

Ahli :
i. CIO
ii. Ketua Bahagian
iii. ICTSO

Urusetia : Unit Teknologi Maklumat

Bidangkuasa:

i. Menentukan arah tuju keselamatan ICT LUAS;

ii. Menilai, melulu dan menguatkuasakan pelaksanaan DKICT LUAS;

iii. Memastikan pengauditan sistem ICT LUAS dilaksanakan;

iv. Meluluskan program dan aktiviti berkaitan keselamatan ICT LUAS;

v. Memastikan DKICT LUAS selaras dengan Pelan Strategik Teknologi Maklumat (PSTM);

vi. Memantau ancaman-ancaman utama keselamatan ICT;

vii. Melaporkan insiden keselamatan yang telah berlaku dan tindakan yang telah diambil kepada pihak pengurusan LUAS;

viii. Menyelenggara dokumen DKICT LUAS;

ix. Memantau tahap pematuhan DKICT LUAS;

x. Menilai aspek teknikal keselamatan projek-projek ICT;

xi. Membangunkan garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam LUAS yang mematuhi keperluan DKICT;

xii. Menyemak semula sistem ICT supaya sentiasa mematuhi keperluan keselamatan dari semasa ke semasa;

xiii. Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT;

xiv. Memastikan DKICT LUAS selaras dengan dasar-dasar ICT Kerajaan semasa; dan

xv. Bekerjasama dengan Pasukan Tindak Balas Insiden Keselamatan ICT (CERT) SELANGOR untuk mendapatkan maklum balas ke atas insiden untuk tindakan penyelenggaraan DKICT LUAS.

0202 Pihak Ketiga

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

020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga

Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi: a) Membaca, memahami dan mematuhi DKICT LUAS; b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; d) Akses kepada aset ICT LUAS perlu berlandaskan kepada perjanjian kontrak; e) Mengenal pasti risiko ke atas keselamatan maklumat dan memastikan pelaksanaan kawalan yang sesuai ke atas maklumat tersebut; f) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga, dan	CIO; Ketua UTM; ICTSO; Pihak Ketiga

g) Akses kepada aset ICT LUAS perlu berlandaskan perjanjian kontrak. Perjanjian yang dimeterai perlu mematuhi perkara-perkara berikut:

a. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga, perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai.

i. DKICT LUAS;

ii. Arahan Keselamatan;

iii. Arahan Teknologi Maklumat 2007 (*IT Instructions*);

iv. Perakuan Akta Rahsia Rasmi 1972;

v. Hak Harta Intelek; dan

vi. Akta Kawasan Larangan dan Tempat Larangan 1959

h) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT LUAS dan *Non-Disclosure Agreement (NDA)* sebagaimana **Lampiran 1** dan **Lampiran 2**.

BIDANG 03
PENGURUSAN ASET

0301 Akauntabiliti Aset

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

030101 Inventori Aset ICT

Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Tanggungjawab yang perlu dipatuhi untuk memastikan semua aset ICT dikawal dan dilindungi adalah seperti berikut: a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa di kemas kini; b) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; c) Memastikan semua pengguna mengesahkan aset ICT yang ditempatkan di LUAS; d) Semua peraturan pengendalian aset hendaklah dikenal pasti, didokumen dan dilaksanakan; dan e) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Pegawai Aset dan Semua

0302 Pengelasan dan Pengendalian Maklumat	
Objektif : Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
030201 Pengelasan Maklumat	
Sesuatu maklumat hendaklah dikelaskan berdasarkan kepada nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal kepada LUAS. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: a) Rahsia Besar b) Rahsia; c) Sulit; atau d) Terhad.	Pengarah
030202 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnahkan hendaklah mengambil kira langkah-langkah keselamatan berikut: a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c) Menentukan maklumat sedia untuk digunakan; d) Menjaga kerahsiaan kata laluan;	Semua

e) Menjaga kerahsiaan kata laluan; Mematuhi *standard*, prosedur, langkah dan garis panduan keselamatan ICT yang ditetapkan;

f) Melaksanakan peraturan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan;

g) Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum;

h) 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;

i) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan

j) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.

BIDANG 04
KESELAMATAN SUMBER MANUSIA

0401 Keselamatan Sumber Manusia dalam Tugas Harian

Objektif :

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

040101 Sebelum Perkhidmatan

Memastikan pegawai dan kakitangan LUAS, pembekal, pakar perunding dan pihak-pihak lain yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT bagi meminimumkan risiko seperti kesilapan, kecuaian, penipuan dan penyalahgunaan aset ICT. Perkara yang mesti dipatuhi termasuk yang berikut: a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan LUAS, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan ke atas keselamatan ICT sebelum, semasa dan selepas perkhidmatan; b) Memastikan pegawai dan kakitangan LUAS, pembekal, pakar runding dan pihak-pihak lain menandatangani surat Akuan Pematuhan DKICT dan Borang Non-Disclosure Agreement (yang berkepentingan selaras dengan keperluan perkhidmatan; dan c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Pegawai Aset dan Semua

040102 Semasa Perkhidmatan	
Memastikan pegawai dan kakitangan LUAS, pembekal, pakar perunding dan pihak-pihak lain yang berkepentingan sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong DKICT LUAS dan meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara yang perlu dipatuhi termasuk yang berikut: a) Memastikan pegawai dan kakitangan LUAS, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan ditetapkan LUAS; b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pegawai dan kakitangan LUAS secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dari semasa ke semasa; c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan LUAS, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan sekiranya berlaku pelanggaran dengan perundangan dan peraturan yang ditetapkan LUAS; dan 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. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Unit Pengurusan Sumber Manusia dan Integriti atau Unit Teknologi Maklumat.	Semua

040103 Program Kesedaran Keselamatan ICT	
Setiap pengguna di LUAS perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Program menangani insiden juga adalah penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT LUAS.	Ketua UTM
040104 Bertukar atau Tamat Perkhidmatan	
Memastikan pertukaran atau tamat perkhidmatan pegawai dan kakitangan LUAS, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan diuruskan dengan teratur. Perkara yang perlu dipatuhi termasuk: a) Memastikan semua aset ICT dikembalikan kepada LUAS mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan b) Membatalkan atau meminda semua kebenaran capaian maklumat, kemudahan proses maklumat dan semua akses berkaitan mengikut peraturan yang ditetapkan LUAS dan/atau terma perkhidmatan.	Ketua Unit PSMI; Ketua UTM

BIDANG 05
KESELAMATAN FIZIKAL DAN PERSEKITARAN

0501 Keselamatan Kawasan

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

050101 Kawalan Kawasan

Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko. b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; c) Memasang alat penggera atau kamera; d) Menghadkan jalan keluar masuk; e) Mengadakan kaunter kawalan; f) Menyediakan tempat atau bilik khas untuk pelawat-pelawat; g) Mewujudkan perkhidmatan kawalan keselamatan; h) Melindungi kawasan larangan melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;	CIO; Pengurusan Bangunan; Pegawai Keselamatan; ICTSO

i) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; j) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; k) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan l) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	
050102 Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: - a) Setiap pengguna LUAS hendaklah memakai atau mengenakan pas sepanjang waktu bertugas; b) Semua pas keselamatan hendaklah diserahkan balik kepada LUAS apabila pengguna berhenti atau bersara; c) Setiap pelawat hendaklah mendapatkan Pas Pelawat di Kaunter Tingkat 13. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan d) Kehilangan pas mestilah dilaporkan dengan segera.	Semua

050103 Kawasan Larangan

Pengarah;
CIO;
Ketua UTM;
Pegawai Keselamatan;

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 LUAS adalah:

a) Bilik server ibu pejabat LUAS dan cawangan;

b) Makmal di Pejabat Cawangan Lembaga Urus Air Selangor (LUAS) Seksyen 15;

c) Mana-mana kawasan yang telah/akan diisytiharkan sebagai larangan.

Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas premis tersebut adalah seperti berikut:

a) Sumber data atau server, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik server atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegah kebakaran;

b) Akses adalah terhad kepada pegawai yang telah diberi kuasa sahaja dan dipantau setiap masa;

c) Pemantauan dibuat menggunakan kamera CCTV atau lain-lain peralatan yang sesuai;

d) Peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual;

e) Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan;

f) Pelawat yang dibawa masuk mesti diiringi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan;

g) Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan dan laluan awam;

h) Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan;

i) Memperkukuhkan dinding dan siling;

j) Menghadkan jalan keluar masuk;

k) Mengadakan kaunter kawalan;

l) Menyediakan tempat atau bilik khas untuk pelawat; dan

m) Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.

0502 Keselamatan Peralatan	
Objektif: Melindungi peralatan ICT LUAS dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
050201 Peralatan ICT	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: - a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; c) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; d) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; e) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; f) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; g) Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubahsuai tanpa kebenaran dan salah guna; h) Setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; i) Peralatan-peralatan kritikal perlu disokong oleh UPS;	Semua

j) UPS yang berkuasa tinggi perlu diletakkan di bilik yang berasingan bersuhu rendah yang dilengkapi dengan pengudaraan yang sesuai;

k) Semua peralatan 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 bilik atau rak berkunci;

l) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai;

m) Peralatan ICT yang hendak dibawa keluar dari premis LUAS, perlulah mendapat kelulusan Pegawai Aset atau Ketua UTM dan direkodkan bagi tujuan pemantauan;

n) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera;

o) Aset ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden;

p) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa;

q) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pegawai Aset;

r) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pegawai Aset untuk dibaik pulih;

s) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;

t) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;

u) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*Administrator Password*) yang telah ditetapkan oleh Pentadbir Sistem; v) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; w) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan *"OFF"* apabila meninggalkan pejabat; x) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan y) Memastikan plag dicabut daripada suis utama (*Main Switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
050202 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetic, Semua *optical disk*, *flash disk*, CDROM, *thumb drive* dan media-media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Bagi menjamin keselamatan, langkah-langkah berikut perlu diambil: a) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; b) Bagi media yang hendak dilupuskan, semua maklumat dalam media tersebut perlu dihapuskan terlebih dahulu;	Semua

c) Semua media storan data yang hendak dilupuskan mesti dihapuskan dengan teratur dan selamat; d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan (*data safe*) yang mempunyai termasuk tahan dari dipecahkan, api, air dan medan magnet; e) Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; f) Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; g) Storan dan peralatan *backup* hendaklah disimpan di lokasi yang berasingan yang lebih privasi dan tidak terbuka kepada umum. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja; h) Akses dan pergerakan kepada media storan yang mempunyai data kritikal perlu direkodkan; i) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; dan j) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	
050203 Media Tandatangan Digital	
Sebarang media yang digunakan untuk tandatangan digital hendaklah mematuhi langkah-langkah berikut: a) Pengguna hendaklah bertanggungjawab sepenuhnya bagi perlindungan daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan;	Semua

b) Tidak boleh dipindah milik atau dipinjamkan; dan c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan selanjutnya mengikut Prosedur Pelaporan Insiden.	
050204 Media Perisian dan Aplikasi	
Sebarang media yang digunakan sebagai media perisian dan aplikasi hendaklah mematuhi langkah-langkah berikut: a) Hanya perisian yang rasmi sahaja dibenarkan bagi kegunaan LUAS; b) Sistem aplikasi dalaman tidak dibenarkan diagih/didemontrasikan kepada pihak lain kecuali dengan kebenaran Ketua UTM; 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.	Semua
050205 Pelupusan	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh LUAS termasuk di pejabat-pejabat cawangan. Langkah-langkah berikut perlu diambil dalam memastikan peralatan ICT dilupuskan dengan teratur: a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui shredding, grinding, degauzing atau pembakaran;	Semua; Pegawai Aset; UTM

b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan;

c) Pegawai Aset akan mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;

d) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;

e) Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem Tatacara Pengurusan Aset (TPA);

f) Pelupusan peralatan ICT boleh dilakukan secara berpusat/tidak berpusat mengikut tatacara pelupusan semasa yang berkuat kuasa;

g) Peralatan-peralatan ICT yang akan dilupuskan hendaklah dipastikan bahawa data-data dalam storan telah dihapuskan dengan cara yang selamat;

h) Pengguna ICT adalah **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*, *mother board* dan sebagainya;

ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian LUAS; dan

iii. Memindah keluar dari LUAS mana-mana peralatan ICT yang hendak dilupuskan;

iv. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan. v. Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Lembaga Arkib Negara	
050206 Penyelenggaraan Perkakasan	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut: a) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara; b) Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; e) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pegawai Aset atau Ketua UTM.	Pegawai Aset; UTM

050207 Peralatan di luar Premis	
Perkakasan yang dibawa keluar dari premis LUAS adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: - a) Peralatan perlu dilindungi dan dikawal sepanjang masa; b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri - ciri keselamatan yang bersesuaian; dan c) Sebarang kehilangan peralatan adalah di bawah tanggungjawab individu yang membawa keluar peralatan tersebut dan hendaklah melaporkan kepada pihak Berkuasa dengan segera.	Semua
0503 Keselamatan Persekitaran	
Objektif: Melindungi aset ICT LUAS dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
050301 Kawalan Persekitaran	
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk perolehan, menyewa, mengubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Ketua BKP. Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil: a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b) Semua ruang pejabat khususnya yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;	Semua

c) Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f) Pengguna 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 dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan h) Akses kepada saluran *riser* hendaklah sentiasa dikunci.	Semua
050302 Bekalan Kuasa	
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan 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 dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan c) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	Ketua BKP; Pegawai Keselamatan; Ketua UTM; Pegawai Aset

050303 Kabel	
Kabel komputer/rangkaian hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: - a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan; dan *wire tapping*; d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	ICTSO; Pentadbir Rangkaian
050304 Prosedur Kecemasan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: - a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan MAMPU 2004; dan b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan yang dilantik oleh LUAS.	Semua

0504 Keselamatan Dokumen	
Objektif: Melindungi maklumat LUAS dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	
Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan sistem dokumentasi: a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada; c) Setiap dokumen hendaklah difailkan dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; d) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; e) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan keselamatan; f) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Lembaga Arkib Negara; dan g) Menggunakan penyulitan (*encryption*) ke atas dokumen rahsia rasmi yang disediakan, disimpan dan dihantar secara elektronik.	Semua

BIDANG 06
PENGURUSAN OPERASI DAN KOMUNIKASI

0601 Pengurusan Prosedur Operasi

Objektif:
Memastikan pengurusan operasi dan kemudahan pemprosesan maklumat berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.

060101 Pengendalian Dokumen Prosedur Operasi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: - a) Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian *output*, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa mengikut keperluan.	Semua

0601 Pengurusan Prosedur Operasi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: - a) Pengubahsuaian melibatkan perkakasan, sistem pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran Ketua UTM, pegawai atasan atau pemilik aset ICT terlebih dahulu; b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemaskini 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;	Semua

c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau sebaliknya; dan e) Setiap perubahan hendaklah direkodkan dan difailkan secara teratur.	
060103 Pengasingan Tugas dan Tanggungjawab	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut; a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b) Tugas mewujud, memadam, 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 di manipulasi; dan c) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	Pentadbir Sistem

060104 Prosedur Pengurusan Insiden	
Sebarang insiden keselamatan ICT yang dikenalpasti hendaklah dilaporkan kepada ICTSO untuk pendaftaran dan siasatan awal. Tindakan menangani insiden keselamatan ICT perlu diambil dengan cepat, teratur dan berkesan. Prosedur pengurusan insiden mestilah mengambil kira kawalan-kawalan berikut: a) Ketua UTM akan mengenalpasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian tanpa kebenaran; b) Laporan insiden kemudiannya akan dimaklumkan kepada CERT Selangor (*Selangor Computer Emergency Response Team*) jika memerlukan khidmat nasihat dan bantuan. c) Ketua UTM akan menyediakan laporan siasatan dan ICTSO akan mengesahkan sekiranya Pelan Kesinambungan Perkhidmatan (PKP) perlu diaktifkan atau sebaliknya. Pengesahan akan dihantar kepada CIO untuk mengaktifkan PKP d) Laporan insiden yang tidak memerlukan PKP akan diteruskan untuk tindakan pemulihan. Carta lengkap mengenai perjalanan laporan insiden adalah seperti di **Lampiran 2.**	Semua
0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	
Objektif: Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.	
060201 Perkhidmatan Penyampaian	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: - a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga; b) Perkhidmatan laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan	Semua

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.

0603 Perancangan dan Penerimaan Sistem

Objektif:
Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

060301 Perancangan Kapasiti

Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem; ICTSO

060302 Penerimaan Sistem

Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. Kriteria ini hendaklah merangkumi perkara berikut: a. Memenuhi keperluan dan kehendak pengguna; b. Menggunakan perisian pembangunan yang sah; c. Menggunakan teknologi terkini; d. Memenuhi ciri-ciri keselamatan bagi mengelakkan risiko pencerobohan dan sebagainya; dan e. Memenuhi keperluan-keperluan teknologi semasa dan akan datang. (Contoh: mampu menggunakan pelbagai platform dan *IPV6 Ready*)	Ketua UTM; Pentadbir Sistem; ICTSO

0604 Perisian Berbahaya

Objektif:

Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, Trojan dan sebagainya.

060401 Perlindungan dari Perisian Berbahaya

Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT dari perisian berbahaya: a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, IDS (*Intrusion Detection System*) dan IPS (*Intrusion Prevention System)* mengikut prosedur penggunaan yang betul dan selamat; b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan lindungi di bawah mana-mana undang-undang bertulis yang berkuatkuasa; c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; d) Mengemas kini paten antivirus dengan 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 mengendalikannya; g) 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; h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	Ketua UTM; Semua

060402 Perlindungan dari *Mobile Code*	
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Pentadbir Sistem
0605 Housekeeping	
Objektif: Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.	
060501 Backup	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. *Backup* hendaklah direkodkan dan disimpan di *off site*, di antaranya adalah: a) Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat; c) Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; d) *Backup* hendaklah dilaksanakan secara harian, mingguan, bulanan dan tahunan. Kekerapan *backup* bergantung pada tahap kritikal maklumat; dan e) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	Pentadbir Sistem; Pentadbir Pangkalan Data

0606 Pengurusan Rangkaian

Objektif:
Melindungi maklumat rangkaian dan infrastruktur sokongan.

060601 Kawalan Infrastruktur Rangkaian

Infrastruktur rangkaian perlu dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Langkah-langkah bagi menangani ancaman ke atas rangkaian adalah seperti berikut: a) Semua 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, gegar dan habuk; c) Semua peralatan mestilah melalui proses Pengujian Penerimaa Pengguna (UAT) semasa pemasangan dan konfigurasi; d) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; e) Semua capaian kepada Internet dan sistem aplikasi mestilah melalui *firewall* dan diselia oleh Pentadbir Rangkaian; f) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan LUAS; g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;	Ketua UTM; Pentadbir Rangkaian;

a) Memasang perisian IPS bagi mengesan dan menghalang sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat LUAS; b) Memasang *Web Content Filter* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; c) Semua pengguna hanya dibenarkan menggunakan rangkaian LUAS kecuali mendapat kebenaran dari Ketua UTM dan penggunaan modem adalah dilarang sama sekali; d) Sebarang penyambungan rangkaian yang bukan di bawah kawalan LUAS adalah tidak dibenarkan; dan e) Kemudahan bagi *Wireless* LAN perlu dipastikan kawalan keselamatan.	
0607 Pengurusan Media	
Objektif: Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
060701 Media Mudah Alih	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua UTM / pemilik sistem terlebih dahulu.	Semua

060702 Prosedur Pengendalian Media	
Di antara prosedur-prosedur pengendalian media yang perlu dipatuhi termasuk: a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e) Menyimpan semua media di tempat yang selamat; dan f) Media yang mengandungi maklumat terperingkat hendaklah dihapus atau dimusnahkan mengikut peraturan dan prosedur yang betul dan selamat.	Pentadbir Sistem; Pengguna
060703 Keselamatan Sistem Dokumentasi	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b) Menyedia dan memantapkan keselamatan sistem dokumentasi; dan c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada;	Semua

0608 Pengurusan Pertukaran Maklumat	
Objektif: Memastikan keselamatan pertukaran maklumat dan perisian antara LUAS dan mana-mana entiti luar terjamin.	
060801 Pertukaran Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Polisi prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara LUAS dengan pihak luar; c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari LUAS; dan d) Maklumat yang terdapat dalam e-mel perlu dilindungi sebaik-baiknya.	KETUA UTM; ICTSO; Pentadbir Sistem
060802 Pengurusan Mel Elektronik (E-mel)	
Penggunaan e-mel di LUAS hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”; “Garis Panduan Penggunaan Mel Elektronik LUAS” dan mana-mana undang-undang bertulis yang berkuatkuasa. Di antara prosedur-prosedur pengurusan e-mel termasuk: a) Akaun atau alamat e-mel yang diperuntukkan oleh LUAS sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;	Pentadbir E-mel; Semua

b) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;

c) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh megabait (10Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;

d) Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;

e) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;

f) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;

g) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat;

h) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera;

i) Pengguna hendaklah memberikan keutamaan kepada e-mel rasmi LUAS untuk digunakan dalam sebarang urusan rasmi;

j) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing;

k) Menghadkan jenis dan saiz fail lampiran bagi tujuan mengelakkan jangkitan virus dan serangan *email bombing*;

l) Pengguna hendaklah memastikan alamat e-mel penerima adalah betul bagi penghantaran dokumen rasmi;

m) Penggunaan e-mel LUAS bagi tujuan peribadi adalah tidak dibenarkan; Pentadbir e-mel perlu menetapkan had minimum kuota *mailbox*;

n) Pembersihan e-mel hendaklah dibuat sekiranya *mailbox* didapati tidak aktif selama dua (2) bulan atau melebihi kuota dan had masa yang ditetapkan;

o) Penghantaran lampiran dalam *format/extension* "*.exe, *.bat" dan ".com "tidak dibenarkan dan pengguna yang menerima fail berkenaan juga adalah dilarang untuk membuka e-mel tersebut kerana boleh mengakibatkan penyebaran virus;

p) Semua kakitangan LUAS layak diperuntukkan akaun e-mel rasmi LUAS, manakala selain daripada itu akan dipertimbangkan dengan kebenaran Pengarah;

q) Fungsi *Auto-Reply* adalah tidak dibenarkan kecuali pengguna yang bercuti atau bertugas di luar pejabat iaitu dengan menggunakan mesej *Out-Of-Office*;

r) Pengguna adalah dilarang sama sekali menggunakan alamat e-mel rasmi LUAS bagi pendaftaran dalam mana-mana web/kumpulan/forum yang tidak berkaitan dengan urusan kerja rasmi; dan

s) Unit Pengurusan Sumber Manusia dan Integriti perlu memaklumkan kepada UTM sebarang status pengguna (bertukar tempat bekerja, bersara, diberhentikan, tidak dapat dikesan bertukar keluar atau masuk ke LUAS di bahagian masing-masing bagi tujuan pengemaskinian e-mel yang terlibat;

t) Perlanggaran kepada mana-mana peraturan boleh menyebabkan penggantungan akaun pengguna atau mana-mana tindakan tatatertib yang bersesuaian. Pengguna hendaklah memastikan alamat e-mel penerima adalah betul bagi penghantaran dokumen rasmi;

Perlanggaran kepada mana-mana peraturan boleh menyebabkan penggantungan akaun pengguna atau mana-mana tindakan tatatertib yang bersesuaian.

0609 Perkhidmatan E-Dagang (*Electronic Commerce Services*)	
Objektif: Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.	
060901 E-Dagang	
Bagi menggalakkan pertumbuhan e-dagang serta sebagai menyokong hasrat kerajaan mempopularkan perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan internet. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; b) Maklumat yang terlibat dalam transaksi dalam talian*(online)* dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	Pentadbir Sistem; Pengguna
060902 Maklumat Umum	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: - a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu: dan c) Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	Semua

0610 Pengurusan Penyampaian Perkhidmatan Pembekal, Pakar Runding dan Pihak-Pihak Lain yang terlibat

Objektif:

Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pembekal, pakar runding dan pihak-pihak lain yang terlibat.

Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a) Memasukkan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat; b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa. Pengurusan ke atas perubahan penyediaan perkhidmatan termasuk menyelenggara dan menambah baik polisi keselamatan, prosedur dan kawalan maklumat sedia ada, perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	KETUA UTM; Pentadbir Sistem

0611 Pemantauan

Objektif:
Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

061101 Pengauditan dan Forensik ICT

ICTSO mestilah bertanggungjawab merekod dan menganalisa perkara-perkara berikut:- a) Sebarang percubaan pencerobohan kepada sistem ICT LUAS; 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 komputer 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 bandwith rangkaian; g) Aktiviti penyalahgunaan akaun e-mel; h) Aktiviti penukaran alamat IP (*IP address*) selain daripada yang diperuntukkan tanpa kebenaran Pentadbir Rangkaian; dan i) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian.	ICTSO

061102 Jejak Audit	
Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi 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; 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 akitiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Pentadbir Sistem yang berkaitan hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	Pentadbir Sistem
061103 Sistem Log	
Fungsi-fungsi sistem log adalah seperti 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 tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	Pentadbir Sistem

061104 Pemantauan Log	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: - a) Log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu 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; e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan, maklumat log dianalisa dan diambil tindakan sewajarnya; dan f) Masa yang berkaitan dengan sistem pemprosesan maklumat dalam LUAS atau domain keselamatan perlu diselaraskan dengan satu sumber masa yang dipersetujui.	Pentadbir Sistem

BIDANG 07
KAWALAN CAPAIAN

0701 Dasar Kawalan Capaian

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

070101 Keperluan Kawalan Capaian

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan d) Kawalan ke atas kemudahan pemprosesan maklumat.	Ketua UTM; Pentadbir Sistem; ICTSO

0702 Pengurusan Capaian Pengguna	
Objektif: Mengawal capaian pengguna ke atas aset ICT LUAS.	
070201 Akaun Pengguna	
Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, Pentadbir Sistem perlu mengambil langkah-langkah berikut; a) Akaun yang diperuntukkan oleh LUAS sahaja boleh digunakan; b) Akaun pengguna (*user id*) hendaklah unik dan mencerminkan identiti pengguna; c) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan LUAS. Akaun boleh ditarik balik jika kaedah penggunaannya melanggar peraturan; d) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan e) Pentadbir Sistem boleh menggantung dan menamatkan akaun pengguna atas sebab-sebab berikut; i. Pengguna bercuti panjang atau menghadiri kursus diluar pejabat dalam tempoh melebihi 3 bulan; ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain; iv. Bersara; atau v. Ditamatkan Perkhidmatan.	Pentadbir Sistem; Semua
070202 Hak Capaian (Privilege)	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem

070203 Pengurusan Kata Laluan

Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh LUAS 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 dengan (8) aksara gabungan antara huruf dan nombor (alphanumerik); 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 gunasama; f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g) Disarankan membuat pertukaran kata laluan semasa login kali pertama atau selepas login kali pertama atau selepas kata laluan diset semula; h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; i) Disarankan had masa pengesahan adalah selama dua (2) minit dan selepas had itu, sesi ditamatkan; j) Kata laluan hendaklah ditukar selepas 365 hari atau selepas tempoh masa yang bersesuaian; dan k) Mengelakkan penggunaan semula kata laluan yang baru digunakan.	Pentadbir Sistem; Pengguna

070204 *Clear Desk* dan *Clear Screen*	
Prosedur *Clear Desk* dan *Clear Screen* perlu dipatuhi supaya maklumat dalam apa jua bentuk media disimpan dengan teratur dan selamat bagi mengelakkan apa jua bentuk media disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* and *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a) Menggunakan kemudahan *password screen saver* atau *log out* apabila meninggalkan komputer; b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.	Semua
0703 Kawalan Capaian Rangkaian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	
070301 Capaian Rangkaian	
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian LUAS, rangkaian agensi lain dan rangkaian awam; b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaiannya; dan c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	ICTSO; Pentadbir Rangkaian

070302 Capaian Internet	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Penggunaan internet di LUAS hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaanya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian LUAS; b) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; c) Penggunaan proksi yang telah ditetapkan oleh LUAS bagi mengawal akses Internet mengikut fungsi kerja dan mematuhi pekeliling semasa yang dikeluarkan; d) Penggunaan teknologi *packet shaper* untuk mengawal aktiviti *video conferencing, video streaming, chat, downloading* adalah perlu bagi menguruskan penggunaan jalur lebar (*broadband*) yang maksimum dan lebih berkesan; e) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengarah berhak menentukan pengguna yang dibenarkan menggunakan internet atau sebaliknya; f) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh pegawai yang diberi kuasa; g) Bahan yang diperolehi dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; h) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Bahagian sebelum dimuat naik ke Internet; 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 LUAS;	Semua

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

Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut:

a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan LUAS;

b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf super user;

c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem; dan

d) Menyediakan tempoh penggunaan mengikut kesesuaian.

Perkara-perkara yang perlu dipatuhi termasuk berikut:

a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin;

b) Mewujudkan satu pengenalan diri (*ID*) yang unik dan hanya digunakan oleh pengguna berkenaan sahaja dan satu teknik pengesahan yang bersesuaian hendaklah diwujudkan bagi mengesahkan pengenalan diri pengguna;

c) Menghadkan dan mengawal penggunaan program utiliti yang berkemampuan bagi satu tempoh yang ditetapkan; dan

d) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.

0705 Kawalan Capaian Aplikasi dan Maklumat

Objektif:

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

070501 Capaian Aplikasi dan Maklumat

Bertujuan melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Capaian sistem dan aplikasi di LUAS adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut perlu dipatuhi; a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian, keselamatan 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; c) Memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan; d) Menghadkan 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.	Pentadbir Sistem; Semua

0706 Peralatan Mudah Alih dan Jarak Jauh	
Objektif: Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan jarak jauh.	
070601 Peralatan Mudah Alih	
Perkara yang perlu dipatuhi adalah seperti berikut: - a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Semua
070602 Kerja Jarak Jauh	
Perkara yang perlu dipatuhi adalah seperti berikut: - a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua

BIDANG 08
PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

0801 Keselamatan dalam Pembangunan Sistem dan Aplikasi

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

080101 Keperluan Keselamatan Sistem Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: - a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketetapan maklumat; 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 dan sempurna dan sistem *output* untuk memastikan data yang telah diproses adalah tepat; 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 sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	ICTSO; Pemilik Sistem; Pentadbir Sistem

080102 Pengesahan data *input* dan *output*	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: - a) Data *input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan adalah betul dan bersesuaian; dan b) Data *Output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pentadbir Sistem
080103 Kawalan Prosesan	
Kawalan proses perlu ada dalam aplikasi bagi tujuan mengesan sebarang pengubahsuaian ke atas maklumat yang berkemungkinan terhasil daripada masalah semasa prosesan.	Pentadbir Sistem
0802 Kawalan Kriptografi	
Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
080201 Enkripsi	
Pengguna hendaklah membuat penyulitan (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Pentadbir Sistem; Pentadbir Rangkaian;
080202 Tandatangan Digital	
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Pentadbir Sistem; Pentadbir Rangkaian
080203 Penggunaan Infranstruktur Kunci Awam (PKI)	
Pengurusan ke atas Infrastruktur Kunci Awam (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Pentadbir Sistem; Pentadbir Rangkaian

0803 Keselamatan Fail Sistem

Objektif:

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

080301 Kawalan Fail Sistem

Fail sistem perlu dikawal dan dikendalikan dengan baik dan selamat. a) Proses pengemas kini fail sistem hanya boleh dilakukan oleh Pentadbir Sistem atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b) Kod atau aturcara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; c) Mengawal capaian ke atas kod atau aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pentadbir Sistem

0804 Keselamatan dalam Proses Pembangunan dan Sokongan Sistem	
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
080401 Prosedur Kawalan Perubahan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: - a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkod dan disahkan sebelum diguna pakai; b) Aplikasi kritikal perlu dikaji semula dan diuji sekiranya terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk berlaku terhadap sistem tersebut dan suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pembekal; c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; d) Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan e) Menghalang sebarang peluang untuk membocorkan maklumat.	Pentadbir Sistem
080402 Pembangunan Perisian secara *Outsource*	
Pembangunan perisian aplikasi secara *outsource* perlu dipantau oleh pemilik sistem. *Source code* adalah menjadi hak milik LUAS.	Pemilik Sistem; Ketua UTM; Pentadbir Sistem;

0805 Kawalan Teknikal Keterdedahan (*vulnerability*)

Objektif:

Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.

080501 Kawalan dari Ancaman Teknikal

Maklumat mengenai ancaman teknikal sistem maklumat yang digunakan perlu diperolehi. Pendedahan organisasi kepada ancaman teknikal perlu dinilai bagi mengenalpasti tahap risiko yang bakal dihadapi. Perkara-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.	ICTSO; Pentadbir sistem

BIDANG 09
PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

0901 Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif :

Untuk memastikan semua insiden dikendalikan dengan cepat, tepat dan berkesan dan memastikan sistem ICT LUAS dapat segera beroperasi semula dengan baik supaya tidak menjejaskan imej LUAS dan sistem penyampaian perkhidmatan.

090101 Mekanisme Pelaporan

ICTSO;

Pengguna

Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar DKICT sama ada yang ditetapkan secara tersurat atau tersirat.

Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO kadar segera dan semua maklumat adalah dianggap SULIT:

a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau 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, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;

d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan

e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.

Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di LUAS sepertimana di **Lampiran 2**.

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.

i) **Pelaporan**

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

ii) **Tanggungjawab ICTSO**

ICTSO akan bertindak menghubungi dan melaporkan insiden yang berlaku kepada CERT SELANGOR sama ada sebagai input atau untuk tindakan seterusnya.

iii) **Tanggungjawab Pengguna**

Semua kakitangan, pembekal, pakar runding dan pihak-pihak lain yang terlibat diingatkan supaya tidak melaksanakan sebarang tindakan secara sendiri, tapi sebaliknya perlu terus melaporkan dengan segera sebarang kejadian insiden-insiden keselamatan ICT, kerentanan yang diperhatikan atau disyaki terdapat dalam sistem maklumat menerusi mekanisme pelaporan ini. Ini adalah bagi mengelakkan kerosakan atau kehilangan bahan bukti pencerobohan dan cubaan menceroboh.

iv) **Tindakan Dalam Keadaan Berisiko Tinggi**

Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan serta-merta supaya satu keputusan segera dapat diambil. Tindakan ini perlu bagi mengelakkan kesan atau merebak.

0902 Pengurusan Maklumat Insiden Keselamatan ICT

Objektif:
Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat Insiden Keselamatan ICT.

090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT

Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisa bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada LUAS. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan diselenggarakan dengan baik. 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.	ICTSO

BIDANG 10
PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1001 Dasar Kesinambungan Perkhidmatan

Objektif :

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

100101 Pelan Pengurusan Kesinambungan Perkhidmatan

Pelan Pengurusan Kesinambungan Perkhidmatan (*Business Continuity Management - BCM*) 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 dan perkara-perkara berikut perlu diberi perhatian: a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan dan pemulihan; b) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT; 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.	Pegawai keselamatan; CIO; Ketua UTM

Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: -

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

b) Senarai personel LUAS dan pembekal beserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel 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 di mana boleh.

Salinan pelan BCM perlu disimpan dilokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan BCM hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan.

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

LUAS hendaklah memastikan salinan pelan BCM sentiasa dikemas kini dan dilindungi seperti di lokasi utama.

BIDANG 11
PEMATUHAN

1101 Pematuhan dan keperluan Perundangan

Objektif :

Meningkatkan tahap keselamatan ICT bagi mengelak daripada perlanggaran kepada DKICT LUAS.

110101 Pematuhan Dasar

Setiap pengguna di LUAS hendaklah membaca, memahami dan mematuhi DKICT LUAS dan undang-undang atau peraturan-peraturan lain yang berkaitan. Semua aset ICT di LUAS termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Pengarah berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.	Semua

110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal

ICTSO perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu melalui pemeriksaan secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO

110103 Pematuhan Keperluan Audit

Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem di mana sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Semua

110104 Keperluan Perundangan	
Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di LUAS adalah seperti di **Lampiran 3.**	Pengguna
110105 Pelanggaran Perundangan	
Mengambil tindakan undang-undang dan tatatertib ke atas sesiapa yang terlibat di dalam semua perbuatan kecuaian, kelalaian dan perlanggaran keselamatan yang membahayakan perkara-perkara terperingkat di bawah Akta Rahsia Rasmi 1972 dan akta lain yang berkaitan.	Pengguna

GLOSARI	
Antivirus	Perisian yang mengimbas virus pada peralatan ICT seperti komputer, *server* serta media storan, seperti cakera keras (*hard disk*) dan disket (*diskette*) untuk sebarang kemungkinan adanya virus.
Aset ICT	Terdiri daripada organisasi, manusia, perisian, perkakasan, telekomunikasi, kemudahan ICT dan data.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi. (Cth: di antara cakera keras dan komputer utama) dalam jangka masa yang ditetapkan.
BRP	*Business Resumption Planning* Pelan Kesinambungan Perkhidmatan
UTM	Unit Teknologi Maklumat (*Information Technology Unit*).
CCTV	*Closed-circuit television system* Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang di dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
CIA^3	*Confidentiality, Integrity, Authenticity, Accessibility, Accountability.*
CERT SELANGOR	Selangor *Computer Emergency Response Team* Organisasi yang ditubuhkan untuk Membantu agensi mengurus pengendalian insiden keselamatan ICT di SUK Selangor dan agensi di bawah kawalannya.
CIO	*Chief Information Office* Ketua Pegawai Maklumat yang bertanggungjawabkan terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Data center	Pusat simpanan data.

GLOSARI	
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi atau penyulitan. Proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
E-mel	Mel Elektronik (*Electronic Mail*).
Firewall	Sistem yang direkabentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Juga pemisah di antara rangkaian luar dan dalam. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft*/*espionage*), penipuan (*hoaxes*).
Hard Disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	*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.
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan ICT di sesebuah Organisasi.
ICT	*Information and Communication Technology.*
Insiden Keselamatan	Musibah (*adverse event*) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.

GLOSARI	
ISDN	*Integrated Services Digital Networks* Menggunakan isyarat digital pada talian telefon analog yang sedia ada.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna pada mana-mana komputer boleh membuat capaian maklumat daripada pelayan (*server*) atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian tersebut agar sentiasa berasingan.
Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau LUAS dan hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.
IDS	*Intrusion Detection System* (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.
IPS	*Intrusion Prevension System* (Sistem Pencegah Pencerobohan) Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindakbalas menyekat atau menghalang aktiviti serangan atau malicious *code*. E.g. *Network-based* IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan
Keadaan Berisiko Tinggi	Dalam situasi yang mudah mendapat ancaman dari pihak luar atau apa-apa kemungkinan yang boleh menjejaskan kelancaran sistem.
PTM	Pegawai Teknologi Maklumat
PPTM	Penolong Pegawai Teknologi Maklumat

GLOSARI	
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Ligthning arrestor	Alat yang digunakan untuk mencegah daripada ancaman kilat.
Lock	Mengunci komputer.
Log out	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse*, *worm, spyware* dan sebagainya.
MODEM	*MOdulator DEModulator* Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya.la biasanya disambung ke talian telefon bagi membolehkan capaian Internet ibuat dari komputer.
NOMC	*Network Operation and Monitoring Centre.*
Outsource	Maklumat yang diproses dan diperolehi di luar daripada sesuatu organisasi atau struktur kerja.
Pegawai Aset	Pegawai yang telah dilantik untuk menguruskan Aset LUAS.
LUAS	Singkatan bagi Lembaga Urus Air Selangor (LUAS) iaitu agensi yang akan mengguna pakai dan tertakluk kepada DKICT termasuk pejabat-pejabat cawangan.
Pengguna	Semua individu yang menggunakan perkhidmatan/ aplikasi/kemudahan ICT yang disediakan oleh LUAS.
PSMI	Unit Pengurusan Sumber Manusia dan Integriti
Pegawai Keselamatan	Pegawai yang dilantik yang bertanggungjawab mengenai pentadbiran LUAS untuk melaksanakan arahan-arahan keselamatan Kerajaan dengan berhubung rapat dan mendapat nasihat dari Pegawai Keselamatan Kerajaan.

GLOSARI	
Pentadbir Pangkalan Data	Pegawai yang telah diberi kuasa mentadbir pangkalan data LUAS yang terdiri daripada PTM/PPTM.
Pentadbir Rangkaian	Pegawai yang telah diberi kuasa mentadbir rangkaian yang terdiri daripada PTM/PPTM.
Pentadbir Sistem	Pegawai yang telah diberi kuasa mentadbir sesuatu sistem LUAS yang terdiri daripada PTM/PPTM.
Pentadbir Laman Web	Pegawai yang telah diberi kuasa mentadbir semua Web rasmi LUAS yang terdiri daripada PTM/PPTM.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau agensi.
Pihak Ketiga	Pihak pembekal, perunding atau mana-mana pihak luar yang berurusan dengan LUAS.
PKI	*Public-Key Infrastructure* Infrastruktur Kunci Awam.
Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan negara, menyebabkan kerosakan besar kepada kepentingan dan martabat Malaysia atau member keuntungan besar kepada sesebuah kuasa asing.
Rahsia Besar	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Malaysia.

GLOSARI	
Restoration	Pemulihan ke atas data.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan
UTM	Unit Teknologi Maklumat
PKI	*Public-Key Infrastructure* Infrastruktur Kunci Awam.
Sulit	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat Malaysia atau kegiatan Kerajaan atau orang perseorangan atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing.
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian CSMA/CD secara mengurangkan perlanggaran yang berlaku.
Terhad	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakkan juga diberi satu tahap perlindungan keselamatan.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
UAT	*User Acceptance Test*

GLOSARI	
UPS	*Uninterruptible Power Supply.* Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Videoconference	Sidang Video. 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	Aturcara yang bertujuan merosakkan data atau sistem aplikasi.
WAN	*Wide Area Network.* Rangkaian yang merangkumi kawasan yang luas.
Worms	Sejenis virus yang boleh mereplikasi dan membiak dengan sendiri. Ia biasanya menjangkiti sistem operasi yang lemah atau tidak dikemas kini.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.
Email bombing	Kegiatan pengiriman sejumlah besar e-mel bagi memenuhkan mailbox sasaran sehingga mampu menghabiskan ruang storan server.
BCM	Pelan Pengurusan Kesinambungan Perkhidmatan (*Business Continuity Management* - BCM)
BKP	Bahagian Khidmat Pengurusan
Pentadbir E-mel	Pegawai yang bertanggungjawab mengendalikan pentadbiran sistem emel LUAS yang terdiri daripada PTM/PPTM.

Lampiran 1

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT

Nama (Huruf Besar) :

No. Kad Pengenalan :

Jawatan :

Bahagian :

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:-

1. Saya bersih daripada sebarang rekod sabitan salah laku jenayah lampau;
2. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT LUAS; dan
3. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT (ICTSO), Unit Teknologi Maklumat

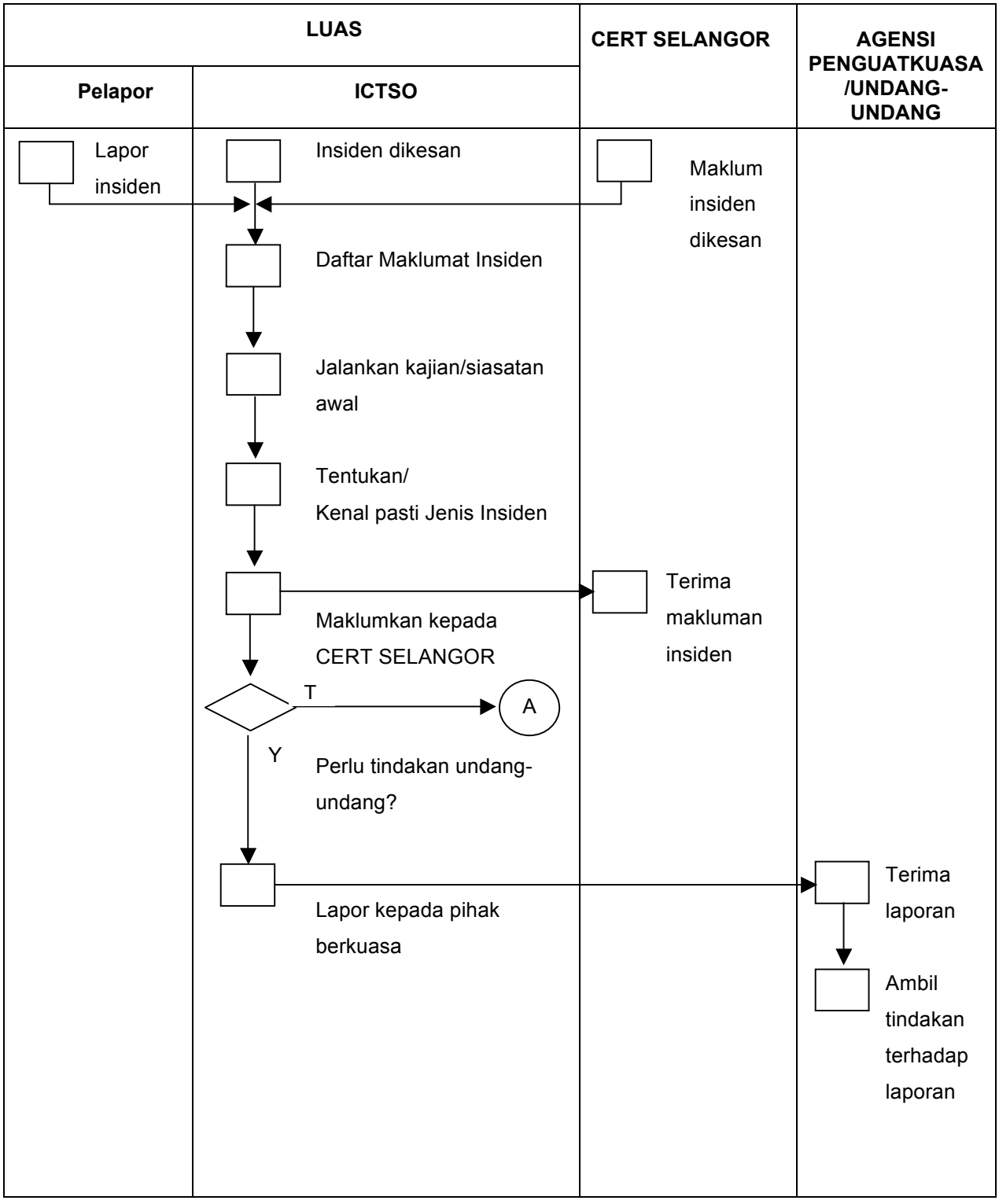
.....

(Nama Pegawai Keselamatan ICT)
b.p. Pengarah Lembaga Urus Air Selangor

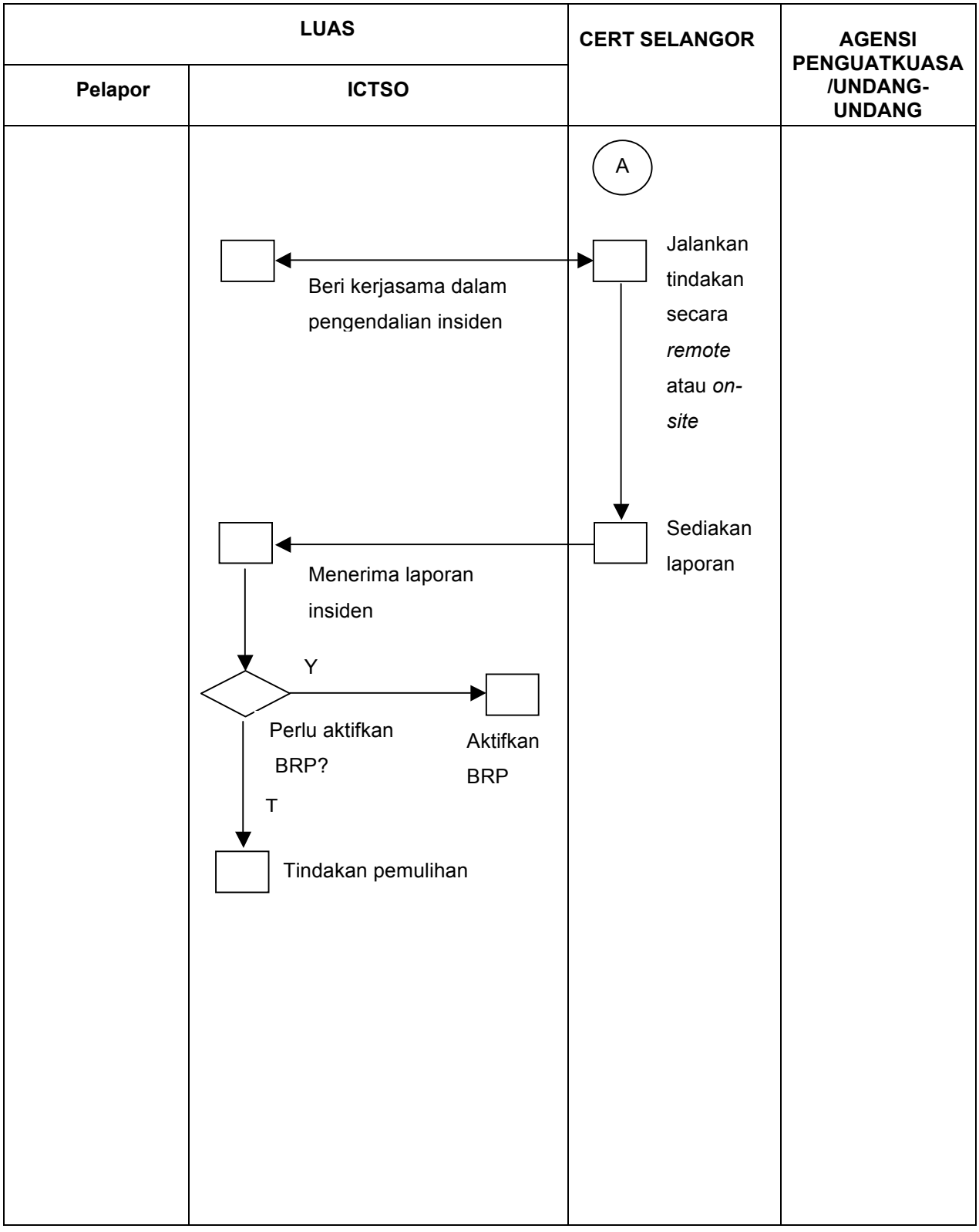
Tarikh: .....

Lampiran 2

Rajah 1: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT Lembaga Urus Air Selangor (LUAS)



Rajah 1: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT Lembaga Urus Air Selangor (LUAS)



Lampiran 3

SENARAI PERUNDANGAN DAN PERATURAN

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 bertajuk “Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam”,

g) Akta Tandatangan Digital 1997,

h) Akta Rahsia Rasmi 1972,

i) Akta Jenayah Komputer 1997,

j) Akta Hak Cipta 1987,

k) Akta Komunikasi dan Multimedia 1998,

l) Surat Pekeliling Perbendaharaan Bil.2 Tahun 1995 (Tambahan pertama) bertajuk “Tatacara Penyediaan, Penilaian dan PenerimaanTender”,

m) Surat Pekeliling Perbendaharaan Bil. 3 Tahun 1995 bertajuk “Peraturan Perolehan Perkhidmatan Perundingan”,

n) Surat Pekeliling Am Bil. 4 Tahun 2006 bertajuk “Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam”,

o) Perintah-Perintah Am,

p) Arahan Perbendaharaan,

q) Arahan Teknologi Maklumat 2007,

r) Surat Akujanji,

s) MPK Lembaga, dan

t) Fail Meja Kakitangan.