# Dasar Keselamatan ICT

# Lembaga Kemajuan kan Malaysia

# (LKIM)

**Mac 2006**

**Versi 2.0**

## PENGENALAN

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

## OBJEKTIF

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

## SKOP

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

## PRINSIP-PRINSIP

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

a. **Akses atas dasar perlu mengetahui**

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar “perlu mengetahui” sahaja. Ini bermakna akses hanya akan diberikan 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;

b. **Hak akses minimum**

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

c. **Akauntabiliti**

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT LKIM;

d. **Pengasingan**

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

e. **Pengauditan**

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

f. **Pematuhan**

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

g. **Pemulihan**

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan pelan pemulihan bencana/kesinambungan perkhidmatan; dan

h. **Saling Bergantungan**

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

## PERKARA 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR DASAR

| Dasar Keselamatan ICT | | |
|---|---|---|
| **010101** | **Pelaksanaan Dasar** | |
| | Pelaksanaan dasar ini akan dijalankan oleh Ketua Pengarah LKIM dibantu oleh Pasukan Pengurusan Keselamatan ICT yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO), dan semua Pengarah Bahagian. | Ketua Pengarah |
| **010102** | **Penyebaran Dasar** | |
| | Dasar ini perlu disebarkan kepada semua pengguna LKIM (termasuk kakitangan, pembekal, pakar runding dll.) | ICTSO |
| **010103** | **Penyelenggaraan Dasar** | |
| | Dasar Keselamatan ICT Kerajaan adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT LKIM:<br>a. kenal pasti dan tentukan perubahan yang diperlukan;<br>b. kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatan Kuasa Pemandu ICT (JPICT);<br>c. perubahan yang telah dipersetujui oleh JPICT dimaklumkan kepada semua pengguna; dan<br>d. dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun. | ICTSO |
| **010104** | **Pengecualian Dasar** | |
| | Dasar Keselamatan ICT LKIM adalah terpakai kepada semua pengguna ICT LKIM dan tiada pengecualian diberikan. | Semua |

## PERKARA 02 ORGANISASI KESELAMATAN

| Infrastruktur Organisasi Keselamatan | | |
|---|---|---|
| Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi. | | |
| **020101** | **Ketua Pengarah** | |
| | Peranan dan tanggungjawab Ketua Pengarah adalah seperti berikut:<br><br>a. memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT LKIM;<br><br>b. memastikan semua pengguna mematuhi Dasar Keselamatan ICT LKIM;<br><br>c. memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; dan<br><br>d. memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT LKIM. | Ketua Pengarah |
| **020102** | **Ketua Pegawai Maklumat (CIO)** | |
| | Timbalan Ketua Pengarah (O) LKIM adalah merupakan Ketua Pegawai Maklumat (CIO). Peranan dan tanggung jawab beliau adalah seperti berikut:<br><br>a. membantu Ketua Pengarah dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT;<br><br>b. menentukan keperluan keselamatan ICT; dan<br><br>c. membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT. | CIO |

| | | |
|---|---|---|
| **020103 Pegawai Keselamatan ICT (ICTSO)** | | |
| | Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut:<br><br>a. mengurus keseluruhan program-program keselamatan ICT LKIM;<br><br>b. menguatkuasakan Dasar Keselamatan ICT LKIM;<br><br>c. memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT LKIM kepada semua pengguna;<br><br>d. mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT LKIM;<br><br>e. menjalankan pengurusan risiko;<br><br>f. menjalankan audit, mengkaji semula, merumus tindak balas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya;<br><br>g. memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;<br><br>h. melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT (GCERT) MAMPU dan memaklumkannya kepada CIO;<br><br>i. bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;<br><br>j. memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT LKIM; dan<br><br>k. menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT. | ICTSO |

| | | |
|---|---|---|
| **020104** | **Pengurus Komputer** | |
| | Pengarah Bahagian Teknologi Maklumat (BTM) adalah merupakan Pengurus Komputer LKIM. Peranan dan tanggungjawab Pengurus Komputer adalah seperti berikut:<br><br>a. membaca, memahami dan mematuhi Dasar Keselamatan ICT LKIM;<br><br>b. mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan LKIM;<br><br>c. menentukan kawalan akses semua pengguna terhadap aset ICT LKIM;<br><br>d. melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan<br><br>e. menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT LKIM. | Pengurus Komputer |
| **020105** | **Pentadbir Sistem ICT** | |
| | Ketua Seksyen Pembangunan Sistem dan Pengkalan Data di Bahagian Teknologi Maklumat adalah merupakan Pentadbir Sistem ICT LKIM. Peranan dan tanggungjawab pentadbir sistem ICT adalah seperti berikut:<br><br>a. mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas;<br><br>b. menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT LKIM;<br><br>c. memantau aktiviti capaian harian pengguna; | Pentadbir Sistem ICT, BTM |

| | | |
|---|---|---|
| | d. memantau aktiviti capaian harian pengguna;<br><br>e. mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta;<br><br>f. menyimpan dan menganalisis rekod jejak audit; dan<br><br>g. menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala. | |
| **020106** | **Pentadbir Rangkaian** | |
| | Ketua Seksyen Sokongan dan Operasi di Bahagian Teknologi Maklumat adalah merupakan Pentadbir Rangkaian. Peranan dan tanggungjawab pentadbir rangkaian adalah seperti berikut:<br><br>a. mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas;<br><br>b. menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT LKIM;<br><br>c. memantau aktiviti capaian rangkaian harian pengguna;<br><br>d. mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta;<br><br>e. menyimpan dan menganalisis rekod jejak audit; dan<br><br>f. menyediakan laporan akses rangkaian secara berkala. | Pentadbir Rangkaian, BTM |

| | | |
|---|---|---|
| **020107 Pengguna** | | |
| | Peranan dan tanggungjawab pengguna adalah seperti berikut:<br><br>a. membaca, memahami dan mematuhi Dasar Keselamatan ICT LKIM;<br><br>b. mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya;<br><br>c. lulus tapisan keselamatan;<br><br>d. melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat LKIM;<br><br>e. melaksanakan langkah-langkah perlindungan seperti berikut :-<br><br>1. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;<br><br>2. memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;<br><br>3. menentukan maklumat sedia untuk digunakan;<br><br>4. menjaga kerahsiaan kata laluan;<br><br>5. mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;<br><br>6. memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan<br><br>7. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.<br><br>f. melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; | Pengguna |

| | | |
|---|---|---|
| | g. melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;<br><br>h. menghadiri program-program kesedaran mengenai keselamatan ICT; dan<br><br>i. menandatangani surat akuan pematuhan Dasar Keselamatan ICT LKIM. | |
| **Pihak Ketiga** | | |
| Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga. | | |
| **020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga** | | |
| | Akses kepada aset ICT LKIM perlu berlandaskan kepada perjanjian kontrak.<br><br>Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeteraikan.<br><br>a. Dasar Keselamatan ICT LKIM;<br><br>b. Tapisan Keselamatan;<br><br>c. Perakuan Akta Rahsia Rasmi 1972;<br><br>d. Hak Harta Intelek;<br><br>Nota 1:<br><br>Surat Pekeliling Perbendaharaan Bilangan 2 Tahun 1995 bertajuk "Tatacara Penyediaan, Penilaian dan Penerimaan Tender" dan Surat Pekeliling Perbendaharaan Bilangan 3 Tahun 1995 bertajuk "Peraturan Perolehan Perkhidmatan Perundingan" yang berkaitan juga boleh dirujuk. | CIO, ICTSO, Pengurus Komputer, Pentadbir Sistem ICT, Pentadbir Rangkaian dan Pihak Ketiga |

## PERKARA 03 KAWALAN DAN PENGELASAN ASET

| | | |
|---|---|---|
| **Akauntabiliti Aset**<br>Objektif : Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT LKIM | | |
| **030101 Inventori Aset** | | |
| | Semua aset ICT LKIM hendaklah direkodkan.<br><br>Ini termasuklah mengenal pasti aset, mengelas aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik dan sebagainya.<br><br>Setiap pengguna adalah bertanggung jawab ke atas semua aset ICT di bawah kawalannya. | Pentadbir Sistem ICT, Pentadbir Rangkaian<br><br>Semua |
| **Pengelasan dan Pengendalian Maklumat**<br>Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian. | | |
| **030201 Pengelasan Maklumat** | | |
| | Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut:<br><br>a. Rahsia Besar<br><br>b. Rahsia;<br><br>c. Sulit; atau<br><br>d. Terhad. | Semua |
| **030202 Pengendalian Maklumat** | | |
| | Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut :<br><br>menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; | Semua |

| | | |
|---|---|---|
| | a. memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;<br><br>b. menentukan maklumat sedia untuk digunakan;<br><br>c. menjaga kerahsiaan kata laluan;<br><br>d. mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;<br><br>e. memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan<br><br>f. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. | |

## PERKARA 04 KESELAMATAN SUMBER MANUSIA

| | | |
|---|---|---|
| **Keselamatan ICT Dalam Tugas Harian**<br><br>Objektif: Meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT LKIM. | | |
| **040101 Tanggungjawab Keselamatan** | | |
| | Peranan dan tanggungjawab pengguna terhadap keselamatan ICT mestilah lengkap, jelas, di rekod, dipatuhi dan dilaksanakan serta dinyatakan di dalam fail meja atau kontrak.<br><br>Keselamatan ICT merangkumi tanggungjawab pengguna dalam menyediakan dan memastikan perlindungan ke atas semua aset atau sumber ICT yang digunakan di dalam melaksanakan tugas harian. | Semua |
| **040102 Terma dan Syarat Perkhidmatan** | | |
| | Semua warga LKIM yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa. | Semua |
| **040102 Perakuan Akta Rahsia Rasmi** | | |
| | Warga LKIM yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972. | Semua |
| **Menangani Insiden Keselamatan ICT**<br><br>Objektif: Meminimumkan kesan insiden keselamatan ICT. | | |
| **040201 Pelaporan Insiden** | | |
| | Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera:<br><br>a. Maklumat didapati hilang, didedahkan kepada pihak pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;<br><br>b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; | Semua |

| | | |
|---|---|---|
| | c. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;<br><br>d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar;<br><br>e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini.<br><br>Nota 2:<br><br>Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan ICT" mengenainya bolehlah dirujuk. | |
| **Pendidikan**<br><br>Objektif: Meningkatkan pengetahuan dan kesedaran mengenai kepentingan keselamatan ICT. | | |
| **040301 Program Kesedaran Keselamatan ICT** | | |
| | Setiap pengguna di LKIM perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka.<br><br>Program menangani insiden juga dilihat penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT LKIM. | ICTSO |
| **Tindakan Tatatertib**<br><br>Objektif: Meningkat kesedaran dan pematuhan ke atas Dasar Keselamatan ICT LKIM. | | |
| **040401 Pelanggaran Dasar** | | |
| | Pelanggaran Dasar Keselamatan ICT LKIM akan dikenakan tindakan tatatertib. | Semua |

## PERKARA 05 KESELAMATAN FIZIKAL

| | | |
|---|---|---|
| **Keselamatan Kawasan**<br><br>Objektif : Mencegah akses fizikal yang tidak dibenarkan, kerosakan dan gangguan kepada premis dan maklumat. | | |
| **050101** | **Perimeter Keselamatan Fizikal** | |
| | Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Langkah-langkah keselamatan fizikal tidak terhad kepada langkah-langkah berikut :<br><br>a. Kawasan keselamatan fizikal hendaklah di kenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko;<br><br>b. memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan;<br><br>c. Memperkukuhkan dinding dan siling;<br><br>d. Memasang alat penggera atau kamera;<br><br>e. Menghadkan jalan keluar masuk;<br><br>f. Mengadakan kaunter kawalan;<br><br>g. Menyediakan tempat atau bilik khas untuk pelawatpelawat; dan<br><br>h. Mewujudkan perkhidmatan kawalan keselamatan. | Pejabat Ketua Pegawai Keselamatan Kerajaan, CIO dan ICTSO |
| **050102** | **Kawalan Masuk Fizikal** | |
| | a. Setiap pengguna LKIM hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas;<br><br>b. Setiap pelawat boleh mendapat Pas Keselamatan Pelawat di pintu masuk ke kawasan atau tempat berurusan dan hendaklah dikembalikan semula selepas tamat lawatan;<br><br>c. Semua pas keselamatan hendaklah diserahkan balik kepada jabatan apabila pengguna berhenti atau bersara; | Semua dan pelawat |

| | | |
|---|---|---|
| | d. Setiap pelawat hendaklah mendaftar di pintu utama Jabatan di tingkat 7 terlebih dahulu;<br><br>e. Kehilangan pas mestilah dilaporkan dengan segera;<br><br>f. Hanya pengguna yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT LKIM; | |
| **050103** | **Kawasan Larangan** | |
| | Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di LKIM adalah bilik Ketua Pengarah, bilik-bilik Timbalan Ketua Pengarah, Bilik Pengarah Bahagian dan bilik server di aras 7. Akses kepada bilik-bilik tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja :<br><br>a. Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik, supaya boleh digunakan bila perlu.<br><br>b. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; dan<br><br>c. Semua penggunaan peralatan yang melibatkan penghantaran, kemas kini dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Ketua Jabatan. | Semua |

| | | |
|---|---|---|
| **Keselamatan Peralatan**<br><br>Objektif : Melindung peralatan dan maklumat. | | |
| **050201** | **Perkakasan** | |
| | Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu:<br><br>a. Setiap pengguna hendaklah menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan sempurna;<br><br>b. Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan;<br><br>c. Setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; dan<br><br>d. Sebarang bentuk penyelewengan atau salah guna perkakasan hendaklah dilaporkan kepada ICTSO. | Semua |
| **050202** | **Dokumen** | |
| | Bagi memastikan integriti maklumat, langkah-langkah pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi:<br><br>a. memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin;<br><br>b. menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka kepada dokumen;<br><br>c. menggunakan penyulitan (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik; dan<br><br>d. memastikan dokumen yang mengandungi bahan atau maklumat sensitif diambil segera dari pencetak. | Semua |

| | | |
|---|---|---|
| **050203** | **Media Storan** | |
| | Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar. Langkah-langkah pencegahan seperti berikut hendaklah di ambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang di simpan dalam media storan adalah terjamin dan selamat :<br><br>a. penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;<br><br>b. akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada mereka atau pengguna yang dibenarkan sahaja;<br><br>c. penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; dan<br><br>d. Pergerakan media storan hendaklah direkodkan. | Semua |
| **050204** | **Kabel** | |
| | Kabel komputer hendaklah di lindung kerana boleh menjadi punca maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut :<br><br>a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;<br><br>b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;<br><br>c. Melindung laluan pemasangan kabel sepenuhnya; dan<br><br>d. Hanya kakitangan dari Seksyen Sokongan dan Operasi di Bahagian Teknologi Maklumat dibenarkan membuat sebarang pindaan atau penyenggaraan. | BTM dan ICTSO |

| | | |
|---|---|---|
| **050205** | **Penyelenggaraan** | |
| | Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan dan integriti.<br><br>a. Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan;<br><br>b. Perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja;<br><br>c. Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; dan<br><br>d. Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengarah Bahagian berkenaan. | Semua |
| **050206** | **Peminjaman Perkakasan Untuk Kegunaan Di Luar Pejabat** | |
| | Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan perkakasan :<br><br>a. Peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai atasan dan tertakluk kepada tujuan yang dibenarkan; dan<br><br>b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan. | Semua |
| **050207** | **Peralatan di Luar Premis** | |
| | Bagi perkakasan yang dibawa keluar dari premis LKIM, langkah-langkah keselamatan hendaklah diadakan dengan mengambil kira risiko yang wujud di luar kawalan LKIM:<br><br>a. Peralatan perlu dilindungi dan dikawal sepanjang masa; dan<br><br>b. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian. | Semua |

| | | |
|---|---|---|
| **050208** | **Pelupusan** | |
| | Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan LKIM:<br><br>a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding degauzing* atau pembakaran;<br><br>b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; dan<br><br>c. Maklumat lanjut pelupusan bolehlah merujuk kepada Surat Pekeliling Perbendaharaan Bilangan 7 Tahun 1995 bertajuk "Garis Panduan Pelupusan Peralatan Komputer". | Semua |
| **050209** | ***Clear Desk* dan *Clear Screen*** | |
| | Semua maklumat dalam apa jua bentuk media hendaklah di simpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja warga atau di paparan skrin apabila warga tidak berada di tempatnya :<br><br>a. Gunakan kemudahan *password screen saver* atau log keluar apabila meninggalkan komputer;<br><br>b. Bahan-bahan sensitif hendaklah disimpan dalam laci atau kabinet fail yang berkunci. | Semua |

| | | |
|---|---|---|
| **Keselamatan Persekitaran**<br><br>Objektif: Melindungi aset ICT LKIM dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan. | | |
| **050301** | **Kawalan Persekitaran** | |
| | Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah di ambil :<br><br>a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti;<br><br>b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;<br><br>c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan;<br><br>d. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT;<br><br>e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT;<br><br>f. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; dan | Semua |

| | | |
|---|---|---|
| | 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 | |
| **050302** | **Bekalan Kuasa** | |
| | a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT<br><br>b. Peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan<br><br>c. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual. | BTM, ICTSO |
| **050303** | **Prosedur Kecemasan** | |
| | a. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan MAMPU 2004; dan<br><br>b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik mengikut aras; | Semua |

## PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI

| | | |
|---|---|---|
| **Pengurusan Prosedur Operasi**<br><br>Objektif: Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat | | |
| **060101 Pengendalian Prosedur** | | |
| | a. Semua prosedur keselamatan ICT yang di wujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal;<br><br>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<br><br>c. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan. | Semua |
| **060102 Kawalan Perubahan** | | |
| | a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;<br><br>b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;<br><br>c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan | Semua |

| | | |
|---|---|---|
| | d. Semua aktiviti perubahan atau pengubahsuaian hendaklah di rekod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak | |
| **060103** | **Prosedur Pengurusan Insiden** | |
| | Bagi memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan; prosedur pengurusan insiden mestilah mengambil kira kawalan-kawalan berikut:<br><br>a. mengenal pasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran;<br><br>b. menyedia pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan;<br><br>c. menyimpan jejak audit dan memelihara bahan bukti; dan<br><br>d. menyediakan tindakan pemulihan segera. | JPICT LKIM , ICTSO |
| | **Perancangan dan Penerimaan Sistem**<br><br>Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem. | |
| **060201** | **Perancangan Kapasiti** | |
| | a. 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; dan<br><br>b. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang. | Pentadbir Sistem ICT, ICTSO |

| | | |
|---|---|---|
| **060202** | **Penerimaan Sistem** | |
| | Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. | Pentadbir Sistem ICT, ICTSO |
| | **Perisian Berbahaya**<br>Objektif : Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus dan trojan. | |
| **060301** | **Perlindungan dari Perisian Berbahaya** | |
| | a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus dan *Intrusion Detection System* (IDS) dan mengikut prosedur penggunaan yang betul dan selamat;<br><br>b. Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah Akta Hakcipta (Pindaan) Tahun 1997;<br><br>c. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya;<br><br>d. Mengemas kini *pattern* anti virus setiap minggu;<br><br>e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;<br><br>f. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;<br><br>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;<br><br>h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan | Semua |

| | | |
|---|---|---|
| | i. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus. | |
| ***Housekeeping***<br><br>Objektif: Melindungi integriti maklumat dan perkhidmatan komunikasi agar boleh diakses pada bila-bila masa. | | |
| **060401** | **Penduaan** | |
| | Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. Salinan penduaan hendaklah direkodkan dan di simpan di *off site*.<br><br>a. Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;<br><br>b. Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi; dan<br><br>c. Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan. | Semua |
| **060402** | **Sistem Log** | |
| | a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;<br><br>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. | BTM |

| | | |
|---|---|---|
| **Pengurusan Rangkaian**<br><br>Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan. | | |
| **060501** | **Kawalan Infrastruktur Rangkaian** | |
| | Infrastruktur Rangkaian mestilah di kawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah-langkah yang perlu dipertimbangkan :<br><br>a. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;<br><br>b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk;<br><br>c. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja iaitu kakitangan dari seksyen sokongan dan operasi;<br><br>d. Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi;<br><br>e. *Firewall* hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta dikonfigurasi oleh pentadbir sistem;<br><br>f. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan LKIM;<br><br>g. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;<br><br>h. Memasang perisian *Intrusion Detection System* (IDS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat LKIM; | Pentadbir Rangkaian dan Pentadbir Sistem ICT |

| | | |
|---|---|---|
| | i. Memasang *Web Content Filter* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan";<br><br>j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan LKIM hendaklah mendapat kebenaran ICTSO;<br><br>k. Semua pengguna hanya dibenarkan menggunakan rangkaian LKIM sahaja. Penggunaan modem atau melakukan penyambungan ke rangkaian lain atau yang seumpamanya, adalah dilarang sama sekali; dan<br><br>l. Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum. | |
| **Pengurusan Media**<br><br>Objektif: Melindungi aset ICT dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal. | | |
| **060601** | **Penghantaran dan Pemindahan** | |
| | Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu. | Semua |
| **060602** | **Prosedur Pengendalian Media** | |
| | a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;<br><br>b. Menghadkan dan menentukan capaian media kepada pengguna yang sah sahaja;<br><br>c. Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan; | Semua |

| | | |
|---|---|---|
| | d. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan;<br><br>e. Menyimpan semua media di tempat yang selamat; dan<br><br>f. Media yang mengandungi maklumat rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat. | |
| **060603** | **Keselamatan Sistem Dokumentasi** | |
| | a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan;<br><br>b. Menyediakan dan memantapkan keselamatan sistem dokumentasi; dan<br><br>c. Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada. | Pentadbir Sistem ICT, ICTSO |
| **Keselamatan Komunikasi**<br><br>Objektif: Melindungi aset ICT melalui sistem komunikasi yang selamat | | |
| **060701** | **Internet** | |
| | a. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan;<br><br>b. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendaklah dinyatakan;<br><br>c. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik ke Internet;<br><br>d. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; | Semua |

| | | |
|---|---|---|
| | e. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh LKIM;<br><br>f. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimana pun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada Ketua Jabatan terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; dan<br><br>g. Maklumat lanjut mengenai keselamatan Internet bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan". | |
| **060702** | **Mel Elektronik** | |
| | a. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh LKIM sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;<br><br>b. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh LKIM;<br><br>c. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;<br><br>d. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul;<br><br>e. Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi dua (2) megabait semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; | Semua |

| | | |
|---|---|---|
| | f. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;<br><br>g. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;<br><br>h. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan;<br><br>i. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;<br><br>j. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; dan<br><br>k. Maklumat lanjut mengenai keselamatan e-mel bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan". | |

## PERKARA 07 KAWALAN CAPAIAN

| | | |
|---|---|---|
| **Dasar Kawalan Capaian**<br>Objektif : Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset LKIM. | | |
| **07101** | **Keperluan Dasar** | |
| | 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 | BTM, ICTSO |
| **Pengurusan Capaian Pengguna**<br>Objektif : Mengawal capaian pengguna ke atas aset ICT LKIM. | | |
| **070201** | **Akaun Pengguna** | |
| | Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi:<br>a. akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan;<br>b. akaun pengguna mestilah unik;<br>c. akaun pengguna yang di wujud pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu;<br>d. pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;<br>e. penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan<br>f. pentadbir sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut; | Semua |

| | | |
|---|---|---|
| | i. pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi dua (2) minggu<br>ii. Bertukar bidang tugas kerja;<br>iii. ke agensi lain;<br>iv. Bertukar<br>v. Bersara; atau<br>vi. Ditamatkan perkhidmatan | |
| **070202 Jejak Audit** | | |
| | Jejak audit akan merekodkan semua aktiviti sistem. Jejak audit juga adalah penting dan digunakan untuk tujuan penyiasatan sekiranya berlaku kerosakan atau penyalahgunaan sistem. Aktiviti jejak audit mengandungi:<br>a. maklumat identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan program yang digunakan;<br>b. aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan<br>c. maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan<br>Pentadbir sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubah suaian yang tidak dibenarkan. | Pentadbir Sistem ICT |

| | | |
|---|---|---|
| **Kawalan Capaian Sistem dan Aplikasi**<br><br>Objektif: Melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan | | |
| **070301** | **Sistem Maklumat dan Aplikasi** | |
| | Capaian sistem dan aplikasi di LKIM adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkahlangkah berikut hendaklah dipatuhi:<br><br>a. pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan;<br><br>b. setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini;<br><br>c. memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalah gunaan;<br><br>d. menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;<br><br>e. memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan<br><br>f. capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimana pun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja. | Pentadbir Sistem ICT, ICTSO |

| | | |
|---|---|---|
| **Peralatan Komputer Mudah Alih**<br><br>Objektif : Memastikan keselamatan maklumat apabila menggunakan kemudahan atau peralatan komputer mudah alih. | | |
| **070401** | **Penggunaan Peralatan Komputer Mudah Alih** | |
| | a. Merekodkan aktiviti keluar masuk penggunaan peralatan komputer mudah alih bagi mengesan kehilangan atau pun kerosakan; dan<br><br>b. Komputer mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan. | |

## PERKARA 08 PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

| | | |
|---|---|---|
| **Keselamatan Dalam Membangunkan Sistem dan Aplikasi**<br>Objektif : Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian. | | |
| **080101 Keperluan Keselamatan** | | |
| | a. Pembangunan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat;<br><br>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; dan<br><br>c. Sebaiknya-baiknya, semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan. | Pemilik sistem, Pentadbir Sistem ICT, ICTSO |
| **Kriptografi**<br>Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat. | | |
| **080201 Penyulitan** | | |
| | Pengguna hendaklah membuat penyulitan ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa. | Semua |
| **080202 Tandatangan Digital** | | |
| | Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik | Semua |

| | | |
|---|---|---|
| **080203** | **Pengurusan Kunci** | |
| | Pengurusan kunci hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, di musnah dan didedahkan sepanjang tempoh sah kunci tersebut. | Semua |
| | **Fail Sistem**<br>Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat | |
| **080301** | **Kawalan Fail Sistem** | |
| | a. Proses pengemas kini fail sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan;<br>b. Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji;<br>c. Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubah suaian tanpa kebenaran, penghapusan dan kecurian; dan<br>d. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemas kinian untuk tujuan statistik, pemulihan dan keselamatan. | Pentadbir Sistem ICT |
| | **Pembangunan dan Proses Sokongan**<br>Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi. | |
| **080401** | **Kawalan Perubahan** | |
| | Perubahan atau pengubah suaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai. | Pentadbir Sistem ICT |

## PERKARA 09 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

| | | |
|---|---|---|
| **Dasar Kesinambungan Perkhidmatan**<br><br>Objektif : Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan. | | |
| **090101** | **Pelan Kesinambungan Perkhidmatan** | |
| | Pelan kesinambungan perkhidmatan hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT dan perkara-perkara berikut perlu diberi perhatian:<br><br>a. mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;<br><br>b. melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;<br><br>c. mendokumentasikan proses dan prosedur yang telah dipersetujui;<br><br>d. mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;<br><br>e. membuat penduaan; dan<br><br>f. menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali | ICTSO |

## PERKARA 10 PEMATUHAN

| Pematuhan dan Keperluan Perundangan | | |
|---|---|---|
| Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT LKIM. | | |
| **100101 Pematuhan Dasar** | | |
| | Setiap pengguna di LKIM hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT LKIM dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa.<br><br>Semua aset ICT di LKIM termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua Jabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan | Semua |
| **100102 Keperluan Perundangan** | | |
| | Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di LKIM:<br><br>a. Arahan Keselamatan;<br><br>b. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan";<br><br>c. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS);<br><br>d. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);<br><br>e. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan";<br><br>f. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam; | Semua |

| | | |
|---|---|---|
| | g. Akta Tandatangan Digital 1997;<br>h. Akta Jenayah Komputer 1997;<br>i. Akta Hak cipta (Pindaan) Tahun 1997; dan<br>j. Akta Komunikasi dan Multimedia 1998 | |