# Dasar Keselamatan ICT

## Majlis Daerah Kerian
## Perak Darul Ridzuan

## Tarikh kuatkuasa: 2 Jan 2014

## Versi 1.0

| RUJUKAN | VERSI | TARIKH | MUKASURAT |
|---|---|---|---|
| DKICT MDK | 1.0 | 2/1/2014 | |

# PENGENALAN

Dasar Keselamatan ICT (DKICT) MDK mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT).
Dasar ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT bagi MDK.

# OBJEKTIF

Dasar Keselamatan ICT MDK diwujudkan untuk menjamin kesinambungan urusan MDK dengan meminimumkan kesan insiden keselamatan ICT.
Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi bahagian masing-masing.

Ini hanya boleh dicapai dengan mema stikan semua aset ICT dilindungi.

Manakala, objektif utama Keselamatan ICT MDK ialah seperti berikut:

a) Memastikan kelancaran operasi bahagian-bahagian serta meminimumkan kerosakan atau kemusnahan;

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

c) Mencegah salah guna atau kecurian aset ICT Kerajaan.

## PERNYATAAN DASAR

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

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT.

Terdapat empat (4) komponen asas keselamatan ICT iaitu:

- Melindungi maklumat rahsia rasmi dan m aklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;
- Menjamin setiap maklumat adalah tepat dan sempurna;
- Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
- Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

Dasar Keselamatan ICT MDK 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 adalahseperti berikut:

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

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

**(c) Tidak Boleh Disangkal**
Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;

**(d) Kesahihan**

Data dan maklumat hendaklah dijamin kesahihannya; dan

### (e) Ketersediaan

Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

# SKOP

Aset ICT MDK terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan ICT MDK menetapkan keperluan-keperluan asas berikut:

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

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

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

**(a) Perkakasan**

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

**(b) Perisian**

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

**(c) Perkhidmatan**

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

i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
ii. Sistem halangan akses seperti sistem kad akses; dan
iii. Perkhidmatan sokongan sepe rti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

**(d) Data atau Maklumat**

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

**(e) Manusia**

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian bahagian bagi mencapai misi dan objektif agensi. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan; dan

**(f) Premis Komputer Dan Komunikasi**

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara (**a) - (e)** di atas.

Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

# PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT MDK 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 perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas;

**(c) 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. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

1. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
2. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;
3. Menentukan maklumat sedia untuk digunakan;
4. Menjaga kerahsiaan kata laluan;
5. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
6. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
7. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

**(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 ini 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 le ngkap-melengkapi dan bergantung antara satu sama lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

# PENILAIAN RISIKO KESELAMATAN ICT

Majlis Daerah Kerian(MDK) hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan vulnerability yang semakin meningkat hari ini. Justeru itu bahagian yang berkenaan perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahapmrisiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

Jabatan 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 jabatan 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 bilik pelayan, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

Jabatan 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.

Jabatan perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

1. Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

2. Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi;

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

4. 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 bahagian serta perundangan yang berkaitan.

| **010101 Pelaksanaan Dasar** | |
|---|---|
| Pelaksanaan dasar ini akan dijalankan oleh Yang Dipertua MDK selaku Pengerusi Jawatankuasa Keselamatan ICT (JKICT) MDK atau mesyuarat lain yang setara dengannya. Pelaksanaan dasar ini juga boleh dilaksanakan oleh pegawai lain yang dibenarkan oleh Pengerusi JKICT. JKICT ini terdiri daripada Setiausaha MDK, semua Ketua Jabatan dan Pegawai Keselamatan ICT (ICTSO) MDK. | Yang Dipertua MDK |
| **010102 Penyebaran Dasar** | |
| Dasar ini perlu disebarkan dan terpakai oleh semua pengguna di MDK termasuk kakitangan, pembekal, pakar runding dan lain-lain. | ICTSO |
| **010103 Penyelenggaraan Dasar** | |
| Dasar Keselamatan ICT MDK adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial. | ICTSO |

| | |
|---|---|
| Berikut adalah prosedur yang berhubung dengan penyelenggaraan<br>Dasar Keselamatan ICT MDK:<br><br>a) Kenal pasti dan tentukan perubahan yang diperlukan;<br><br>b) Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Jawatankuasa Keselamatan ICT (JKICT), MDK atau Mesyuarat Pengurusan MDK atau mesyuarat yang setara dengannya;<br><br>c) Maklum kepada semua pengguna perubahan yang telah dipersetujui oleh JKICT; dan<br><br>d) Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa. | |
| **010104 Pengecualian Dasar** | |
| Dasar Keselamatan ICT MDK adalah terpakai kepada semua pengguna ICT di bawah Pentadbiran MDK dan tiada pengecualian diberikan. | Semua |

# BIDANG 02: ORGANISASI KESELAMATAN

**0201 Infrastruktur Organisasi Dalaman**

**Objektif:**

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT MDK.

| **020101 Jawatankuasa Keselamatan ICT Pejabat MDK** | |
|---|---|
| Jawatankuasa Keselamatan ICT (JKICT) adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT MDK.<br><br>Mesyuarat Pengurusan MDK juga boleh berperanan untuk menggantikan JKICT MDK.<br><br>Keanggotaan JKICT adalah seperti berikut:<br><br>**Pengerusi** : YDP,MDK<br><br>**Ahli :**<br><br>I. Setiausaha, MDK<br><br>II. Ketua-Ketua Jabatan<br><br>III. Pegawai Keselamatan ICT(ICTSO),MDK<br><br>**Urus Setia:**<br><br>Jabatan Teknologi Maklumat, MDK<br><br>**Bidang kuasa:**<br><br>a) Memperakukan/meluluskan dokumen DKICT MDK:<br><br>b) Memantau tahap pematuhan keselamatan ICT; | JKICT |

| | |
|---|---|
| c) Memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam MDK yang mematuhi keperluan DKICT MDK;<br><br>d) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT;<br><br>e) Memastikan DKICT MDK selaras dengan dasar-dasar ICT kerajaan semasa;<br><br>f) Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa;<br><br>g) Membincang tindakan yang melibatkan pelanggaran DKICT | |
| **020102 YANG DIPERTUA MDK** | |
| Yang Dipertua MDK adalah berperanan dan bertanggungjawab dalam perkara-perkara seperti berikut:<br><br>a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT MDK;<br><br>b) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT MDK;<br><br>c) Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi;<br><br>d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT MDK; dan<br><br>e) Mempengerusikan Mesyuarat Jawatankuasa Keselamatan ICT, MDK. | YDP MDK |
| **020103 Ketua Pegawai Maklumat (CIO)** | |

| | |
|---|---|
| Ketua Pegawai Maklumat (CIO) bagi MDK ialah Setiausaha MDK. | CIO |

| | |
|---|---|
| Peranan dan tanggungjawab CIO adalah seperti berikut:<br><br>a) Membantu Y.D.P MDK dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT;<br><br>b) Menentukan keperluan keselamatan ICT;<br><br>c) Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan DKICT MDK serta pengurusan risiko dan pengauditan; dan<br><br>d) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT MDK. | |
| **020104 Pegawai Keselamatan ICT (ICTSO)** | |
| Pegawai Keselamatan ICT (ICTSO) bagi MDK ialah Pegawai Teknologi Maklumat, Jabatan Teknologi Maklumat,MDK.<br><br>Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut:<br><br>a) Mengurus keseluruhan program-program keselamatan ICT Pejabat MDK;<br><br>b) Menguatkuasakan pelaksanaan Dasar Keselamatan ICT MDK;<br><br>c) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT MDK kepada semua pengguna;<br><br>d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT MDK;<br><br>e) Menjalankan pengurusan risiko; | ICTSO |

| | |
|---|---|
| f) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan MDK 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 Kerajaan (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; dan<br><br>j) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.<br><br>k) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT MDK sebagaimana **Lampiran 1**. | |
| **020105 Pengurus ICT** | |
| Pengurus ICT bagi pentadbiran MDK ialah Penolong Pegawai Teknologi Maklumat,Jabatan Teknologi Maklumat.<br><br>Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:<br><br>a. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MDK;<br><br>b. Menentukan kawalan akses pengguna terhadap aset ICT MDK;<br><br>c. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan<br><br>d. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT MDK. | Pengurus ICT |

| | |
|---|---|
| e. Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT MDK sebagaimana **Lampiran 1**. | |
| **020106 Pentadbir Sistem ICT** | |
| Pentadbir Sistem ICT bagi pentadbiran MDK ialah semua pegawai teknikal atau pegawai yang bertanggungjawab bagi sistem yang berkenaan. | Pentadbir Sistem ICT |
| Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut:<br>a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas;<br>b) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT MDK;<br>c) Memantau aktiviti capaian harian sistem aplikasi pengguna;<br>d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta;<br>e) Menganalisis dan menyimpan rekod jejak audit untuk sistem dibawah pantauan masing-masing;<br>f) Menyediakan laporan mengenai aktiviti capaian secara berkala.<br>g) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT MDK sebagaimana Lampiran 1. | |
| **020107 Pengguna** | |

| | |
|---|---|
| Pengguna mempunyai peranan dan tanggungjawab seperti berikut:<br><br>a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT MDK;<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 MDK; dan menjaga kerahsiaan maklumat MDK;<br><br>e) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;<br>f) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan<br><br>g) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT MDK sebagaimana **Lampiran 1.** | Semua |
| **020108 Pasukan Tindak Balas Insiden Keselamatan ICT MDK (CERT MDK)** | |
| Keanggotaan CERT MDK adalah seperti berikut:<br><br>**Pengarah**:Setiausaha MDK<br><br>**Pengurus** : Pegawai Teknologi Maklumat,MDK<br>**Ahli :**<br>1. Pen. Pegawai Teknologi Maklumat F29 Majlis Daerah Kerian.<br><br>Peranan dan tanggungjawab CERT adalah seperti berikut:<br><br>a) Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden;<br><br>b) Merekod dan menjalankan siasatan awal insiden yang diterima;<br><br>c) Menangani tindak balas ( response) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; | CERT MDK |

| | |
|---|---|
| d) Menasihati MDK mengambil tindakan pemulihan dan pengukuhan;<br><br>e) Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada MDK; dan<br><br>f) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan. | |

## 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.<br><br>Perkara yang perlu dipatuhi termasuk yang berikut:<br><br>a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT MDK;<br><br>b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian;<br><br>c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga;<br><br>d) Akses kepada aset ICT MDK perlu berlandaskan kepada perjanjian kontrak;<br><br>e) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai:<br><br>o Dasar Keselamatan ICT MDK;<br>o Tapisan Keselamatan;<br>o Perakuan Akta Rahsia Rasmi 1972; dan<br>o Hak Harta Intelek.<br><br>f) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT MDK sebagaimana **Lampiran 1**<br>. | Pihak Ketiga |

# BIDANG 03: PENGURUSAN ASET

## 0301 Akauntabiliti Aset

### Objektif:

Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT bahagian.

| **030101 Inventori Aset ICT** | |
|---|---|
| Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing.<br><br>Perkara yang perlu dipatuhi adalah seperti berikut:<br>a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa dikemas kini;<br><br>b) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja;<br><br>c) Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di MDK dan juga di jabatan/cawangan;<br><br>d) Peraturan bagi pengendalian aset ICT hendaklah dikenalpasti, di dokumen dan dilaksanakan; dan<br><br>e) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya. | Pentadbir Sistem ICT dan semua |

## 0302 Pengelasan dan Pengendalian Maklumat

## Objektif:

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

| **030201 Pengelasan Maklumat** | |
|---|---|
| Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan.<br>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>b. Rahsia;<br>c. Sulit; atau<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>a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;<br><br>b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;<br><br>c) Menentukan maklumat sedia untuk digunakan;<br><br>d) Menjaga kerahsiaan kata laluan;<br><br>e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;<br><br>f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan<br><br>g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. | Semua |

# BIDANG 04: KESELAMATAN SUMBER MANUSIA

## 0401 Keselamatan Sumber Manusia Dalam Tugas Harian

### Objektif:

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

| | |
|---|---|
| **040101 Sebelum Perkhidmatan** | |
| Perkara-perkara yang mesti dipatuhi termasuk yang berikut:<br><br>a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan bahagian serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan;<br><br>b) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan<br><br>c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan. | Semua |
| **040102 Dalam Perkhidmatan** | |
| Perkara-perkara yang perlu dipatuhi termasuk yang berikut:<br><br>a. Memastikan pegawai dan kakitangan serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT | |

| | |
|---|---|
| berdasarkan perundangan dan peraturan yang ditetapkan;<br><br>b. Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT MDK secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa;<br><br>c. Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan MDK serta pihak ketigayang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan; dan<br><br>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 Bahagian Khidmat Pengurusan,MDK. | Jabatan Khidmat Pengurusan |
| **040103 Bertukar Atau Tamat Perkhidmatan** | |
| Perkara-perkara yang perlu dipatuhi termasuk yang berikut:<br><br>a) Memastikan semua aset ICT dikembalikan kepada bahagian mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan<br><br>b) Membatalkan atau menarik balik semua kebenarancapaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh pentadbiran MDK dan/atau terma perkhidmatan. | Semua |

# BIDANG 05: KESELAMATAN FI ZIKAL 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.<br><br>Perkara-perkara yang perlu dipatuhi termasuk yang berikut:<br><br>a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untukmelindungi aset dan hasil penilaian risiko;<br><br>b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;<br><br>c) Memasang alat penggera atau kamera;<br><br>d) Mengehadkan jalan keluar masuk;<br><br>e) Mengadakan kaunter kawalan;<br><br>f) Menyediakan tempat atau bilik khas untuk pelawat-pelawat;<br><br>g) Mewujudkan perkhidmatan kawalan keselamatan;<br><br>h) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; | Bahagian Khidmat Pengurusan, MDK dan Jabatan masing-masing. |

| | |
|---|---|
| i) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan;<br><br>j) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana;<br>k) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan<br><br>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:<br><br>a) Setiap pengguna MDK atau bahagian masing-masing hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas;<br><br>b) Semua pas keselamatan hendaklah diserahkan balik kepada MDK apabila pengguna berhenti atau bersara dan;<br><br>c) Kehilangan pas mestilah dilaporkan dengan segera. | Bahagian Khidmat Pengurusan, MDK dan Jabatan masing-masing. |
| **050103 Kawasan Larangan** | |
| 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.<br><br>Kawasan larangan di MDK adalah bilik Yang Dipertua MDK , bilik Setiausaha MDK, bilik Ketua Jabatan masing-masing,bilik server di bahagian masing-masing dan Pusat Data (Data Centre) jika ada. | Bahagian Khidmat Pengurusan, MDK dan Jabatan masing- |

| | |
|---|---|
| a) Akses kepada kawasan larangan hanyalah kepada pegawai- pegawai yang dibenarkan sahaja; dan<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, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai. | masing. |

## 0502 Keselamatan Peralatan

## Objektif:

Melindungi peralatan ICT MDK dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.

| **050201 Peralatan ICT** | |
|---|---|
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna;<br><br>b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;<br><br>c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan;<br><br>d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT;<br><br>e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;<br><br>f) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (activated) dan dikemaskini | Semua |

disamping melakukan imbasan ke atas media storan yang digunakan;

g) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;

h) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;

i) Peralatan-peralatan kritikal perlu disokong oleh Uninterruptable Power Supply (UPS);

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

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

l) Peralatan ICT yang hendak dibawa keluar dari premis bahagian, perlulah mendapat kelulusan Pentadbir Sistem ICT atau Ketua Jabatan dan direkodkan bagi tujuan pemantauan;

m) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset di jabatan masing-masing dengan segera;

n) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT;

p) Pengguna dilarang menggunakan perkakasan rangkaian tanpa wayar tanpa kebenaran Pentadbir Sistem ICT.

q) Pengguna dilarang menggunakan perisian antivirus selain yang ditetapkan oleh Jabatan Teknologi Maklumat.

| | |
|---|---|
| r) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaikpulih;<br><br>s) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;<br><br>t) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;<br><br>u) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (administrator password) yang telah ditetapkan oleh Pentadbir Sistem ICT;<br><br>v) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;<br><br>w) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan “OFF ” apabila meninggalkan pejabat;<br><br>x) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan<br><br>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 magnetik, optical disk, flash disk , CDROM, thumb drive dan media storan lain.<br><br>Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut: | Semua |

| | |
|---|---|
| a) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;<br><br>b) Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja;<br><br>c) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan;<br><br>d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet;<br><br>e) Akses dan pergerakan media storan hendaklah direkodkan;<br><br>f) Perkakasan backup hendaklah diletakkan di tempat yang terkawal;<br><br>g) Mengadakan salinan atau penduaan ( backup) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data;<br><br>h) Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan<br><br>i) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu. | |
| **050203 Media Tandatangan Digital** | |
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br>a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan;<br><br>b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan<br><br>c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan | Semua |

| | |
|---|---|
| seterusnya. | |
| **050204 Media Perisian dan Aplikasi** | |
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan MDK;<br><br>b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran;<br><br>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<br><br>d) Source code sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan. | Semua |
| **050205 Penyelenggaraan Perkakasan** | |
| Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar;<br><br>b) Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;<br><br>c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan;<br><br>d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; | Pegawai Aset, MDK |

| | |
|---|---|
| e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan<br><br>f) Semua penyelenggaraan mestilah mendapat kebenaran Pengurus ICT. | |
| **050206 Peralatan di Luar Premis** | |
| Perkakasan yang dibawa keluar dari premis MDK adalah terdedah kepada pelbagai risiko.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<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. | |
| **050207 Pelupusan Perkakasan** | |
| Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh MDK dan ditempatkan di MDK dan Cawangan.<br><br>Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa.<br><br>Pelupusan perlu dilakukan secara terkawal mengikut Pekeliling Perbendaharaan Bil. 5 Tahun 2007 dan lengkap supaya maklumat tidak terlepas dari kawalan MDK dan bahagian.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<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; | Semua,<br>Pegawai Aset |

| | |
|---|---|
| c) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;<br><br>d) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;<br><br>e) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;<br><br>f) Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori;<br><br>g) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan<br><br>h) Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut:<br><br>i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, hardisk, motherboard dan sebagainya;<br><br>ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di MDK;<br><br>iii. Memindah keluar dari MDK mana-mana peralatan ICT yang hendak dilupuskan;<br><br>iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab jabatan; dan<br><br>v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam computer disalin pada media storan kedua seperti disket atau thumb drive sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan. | |

## 0503 Keselamatan Persekitaran

### Objektif:

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

<table>
<tr><td colspan="2">050301 Kawalan Persekitaran</td></tr>
<tr><td>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 Bahagian Khidmat Pengurusan, MDK (bagi bangunan dan premis di bawah pentadbiran MDK) dan jabatan masing-masing (bagi premis atau aset di bawah tanggungjawab bahagian sendiri).<br><br>Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi:<br><br>a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetak an, peralatan computer 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 pintumkecemasan;<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;</td><td>Bahagian Khidmat Pengurusan, dan bahagian masing-masing</td></tr>
</table>

| | |
|---|---|
| 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<br><br>h. Akses kepada saluran riser hendaklah sentiasa dikunci. | |
| **050302 Bekalan Kuasa** | |
| Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>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 Uninterruptable Power Supply (UPS) 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. | Bahagian Khidmat Pengurusan, Jabatan Teknologi Maklumat |
| **050303 Kabel** | |
| Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah.<br><br>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) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan wire tapping; dan | Bahagian Khidmat Pengurusan, Jabatan Teknologi Maklumat |

| | |
|---|---|
| d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui trunking bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat. | |
| **050304 Prosedur Kecemasan** | |
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>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. | Semua |

**0504 Keselamatan Dokumen**

**Objektif:**

Melindungi maklumat MDK masing-masing dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.

| | |
|---|---|
| **050401 Dokumen** | |
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>a. Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar;<br><br>b. Pergerakan fail dan dokumen hendaklahmdirekodkan dan perlulah mengikutmprosedur keselamatan;<br><br>c. Kehilangan dan kerosakan ke atas semua jenismdokumen perlu dimaklumkan | Semua |

| | |
|---|---|
| mengikutmprosedur Arahan Keselamatan;<br><br>d. Pelupusan dokumen hendaklah mengikutmprosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan<br><br>e. Menggunakan enkripsi (encryption ) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik. | |

# BIDANG 06: PENGURUSAN OPERASI DAN KOMUNIKASI

## 0601 Pengurusan Prosedur Operasi

**Objektif:**

Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.

| | |
|---|---|
| **060101 Pengendalian Prosedur** | |
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>a. Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan digunapakai hendaklah didokumen, 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** | |
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>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 | Semua |

| | |
|---|---|
| set ICT berkenaan;<br><br>c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan<br><br>d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak. | |
| **060103 Pengasingan Tugas dan Tanggungjawab** | |
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT;<br><br>b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; dan<br><br>c) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai production . Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian. | Pengurus ICT bahagian dan ICTSO |

## 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:<br><br>a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga;<br><br>b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan<br><br>c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal istem dan proses yang terlibat serta penilaian semula risiko. | Semua |

## 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.<br><br>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 dan ICTSO |

| **060302 Penerimaan Sistem** | |
|---|---|
| Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. | Pentadbir Sistem ICT dan 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 dipatuhi adalah seperti berikut:<br>a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) serta mengikut prosedur penggunaan yang betul dan selamat;<br>b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa;<br>c) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya;<br>d) Mengemas kini anti virus dengan pattern antivirus yang terkini;<br>e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;<br>f) Menghadiri sesi kesedaran mengenai ancaman perisianberbahaya dan cara mengendalikannya;<br>g) Memasukkan klausa tanggungan di dalam kontrak yangtelah ditawarkan kepada pembekal perisian. Klausa inibertujuan untuk tuntutan baik pulih sekiranya perisiantersebut mengandungi | Semua |

| | |
|---|---|
| program berbahaya;<br><br>h) Mengadakan program dan prosedur jaminan kualiti ke atassemua perisian yang dibangunkan; dan<br><br>i) Memberi amaran mengenai ancaman keselamatan ICTseperti serangan virus. | |
| **060402 Perlindungan dari Mobile Code** | |
| Penggunaan mobile code yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan. | Semua |

## 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 hendaklah dilakukan setiap kali konfigurasi berubah.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>a) Membuat backup keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;<br><br>b) Membuat backup ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan backup bergantung pada tahap kritikal maklumat;<br><br>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; | Semua |

| | |
|---|---|
| d) Menyimpan sekurang-kurangnya tiga (3) generasi backup; dan<br><br>e) Merekod dan menyimpan salinan backup di lokasi yang berlainan dan selamat. | |

## 0606 Pengurusan Rangkaian

## Objektif:

Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

| **060601 Kawalan Infrastruktur Rangkaian** | |
|---|---|
| Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<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;<br><br>d) Semua peralatan mestilah melalui proses Factory Acceptance Check (FAC) semasa pemasangan dan konfigurasi;<br><br>e) Firewall hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Sistem ICT;<br><br>f) Semua trafik keluar dan masuk hendaklah melalui firewall di bawah kawalan MDK dan jabatan; | Pengurus ICT, Pentadbir ICT dan Jabatan |

| | |
|---|---|
| g) Semua perisian sniffer atau network analyser adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;<br><br>h) Memasang perisian Intrusion Prevention System (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat MDK dan jabatan;<br><br>i) Memasang Web Content Filtering pada Internet Gateway untuk menyekat aktiviti yang dilarang;<br><br>j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan MDK dan jabatan adalah tidak dibenarkan;<br><br>k) Pengguna dilarang mewujudkan rangkaian tanpa wayar selain daripada yang diperakukan oleh Jabatan Teknologi Maklumat;<br><br>l) 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 Penghantaran dan Pemindahan** | |
| Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu. | Semua |
| **060702 Prosedur Pengendalian Media** | |
| Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut:<br><br>a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; | |

| | |
|---|---|
| b) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja;<br><br>c) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;<br><br>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 terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat. | Semua |
| **060703 Keselamatan Sistem Dokumentasi** | |
| Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut:<br><br>a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan;<br><br>b) Menyedia dan memantapkan keselamatan sistem dokumentasi; dan<br><br>c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada. | Semua |

## 0608 Pengurusan Pertukaran Maklumat

## Objektif:

Memastikan keselamatan pertukaran maklumat dan perisian antara MDK dengan agensi luar yang lain terjamin.

| **060801 Pertukaran Maklumat** | |
|---|---|
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi;<br><br>b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara MDK dengan agensi luar;<br><br>c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari MDK; dan<br><br>d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya. | Semua |
| **060802 Pengurusan Mel Elektronik (E-mel)** | |
| Penggunaan e-mel di MDK hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling<br>Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan” dan mana-mana undang-undang bertulis yang berkuat kuasa.<br><br>Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut:<br><br>a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh MDK 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 MDK;<br><br>c) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; | |

| | |
|---|---|
| d) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul;<br><br>e) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh megabait (10Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;<br><br>f) Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;<br><br>g) Pengguna hendaklah mengenal pasti dan mengesahkan identity 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 sitem komputer adalah tepat;<br><br>k) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera;<br><br>l) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan<br><br>m) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan mailbox masing-masing. | |

## 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 penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan Internet.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan;<br><br>b) Maklumat yang terlibat dalam transaksi dalam talian ( on-line ) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan<br><br>c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan. | Semua |
| **060902 Maklumat Umum** | |
| Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut:<br><br>a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian;<br><br>b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan<br><br>c) Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web. | Semua |

## 0610 Pemantauan

**Objektif**:

Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

<table>
<tr><td colspan="2">061001 Pengauditan dan Forensik ICT</td></tr>
<tr><td>ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut:<br><br>a) Sebarang percubaan pencerobohan kepada sistem ICT;<br><br>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 );<br><br>c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak;<br><br>d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan;<br><br>e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan;<br><br>f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar ( bandwidth ) rangkaian;<br><br>g) Aktiviti penyalahgunaan akaun e-mel; dan<br><br>h) Aktiviti penukaran alamat IP ( IP address ) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.</td><td>ICTSO</td></tr>
<tr><td colspan="2">061002 Jejak Audit</td></tr>
<tr><td>Jejak audit hendaklah mengandungi maklumat-maklumat berikut:<br><br>a) Rekod setiap aktiviti transaksi;<br><br>b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti,</td><td></td></tr>
</table>

| | |
|---|---|
| rangkaian dan aplikasi yang digunakan;<br><br>c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan<br><br>d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.<br><br>Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta ArkibNegara.<br><br>Pentadbir Sistem ICT hendaklah menyemak catatan jejak auditdari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal denganlebih awal. Jejak audit juga perlu dilindungi dari kerosakan,kehilangan, penghapusan, pemalsuan dan pengubahsuaian yangtidak dibenarkan. | Pentadbir Sistem ICT |
| **061003 Sistem Log** | |
| Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut:<br><br>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 tindakanmembaik pulih dengan segera; dan<br><br>c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO. | Pentadbir Sistem ICT |
| **061004 Pemantauan Log** | |

| | |
|---|---|
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;<br><br>b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala;<br><br>c) Kemudahan merekod dan ma klumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan;<br><br>d) Aktiviti pentadbiran dan operator sistem perlu direkodkan;<br><br>e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya;dan<br><br>f) Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam MDK atau domain keselamatanperlu diselaraskan dengan satu sumber waktu yang dipersetujui. | Pentadbir Sistem ICT |

# BIDANG 07: KAWALAN CAPAIAN

## 0701 Dasar Kawalan Capaian

**Objektif:**

Mengawal capaian ke atas maklumat.

| **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 an dikaji semula berasaskan keperluan perkhidmatan dan keselamatan.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna;<br><br>b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;<br><br>c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan<br><br>d) Kawalan ke atas kemudahan pemprosesan maklumat. | ICTSO |

## 0702 Pengurusan Capaian Pengguna

### Objektif:

Mengawal capaian pengguna ke atas aset ICT MDK.

<table>
<tr><th colspan="2">070201 Akaun Pengguna</th></tr>
<tr><td>Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan.<br><br>Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi:<br><br>a. Akaun yang diperuntukkan oleh MDK boleh digunakan;<br><br>b. Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna;<br><br>c. Akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat ke lulusan daripada pemilik sistem ICT terlebih dahulu;<br><br>d. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;<br><br>e. Penggunaan akaun milik ora ng lain atau akaun yang dikongsi bersama adalah dilarang; dan<br><br>f. Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut:<br><br>• Pengguna yang bercuti panjang dalam tempoh<br>• waktu melebihi dua (2) minggu;<br>• Bertukar bidang tugas kerja;<br>• Bertukar ke agensi lain;<br>• Digantung kerja;<br>• Bersara; atau<br>• Ditamatkan perkhidmatan.</td><td>Pentadbir Sistem ICT</td></tr>
<tr><td colspan="2"></td></tr>
</table>

| | |
|---|---|
| **070202 Hak Capaian** | |
| Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas. | Pentadbir Sistem ICT |
| **070203 Pengurusan Kata Laluan** | |
| Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi prosedur yang ditetapkan seperti berikut:<br><br>a. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;<br><br>b. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;<br><br>c. Panjang kata laluan mestilah sekurang-kurangnya dua belas (12) dengan gabungan aksara, angka dan aksara khusus;<br><br>d. Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun;<br><br>e. Kata laluan windows dan screen saver hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;<br><br>f. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;<br><br>g. Kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas login kali pertama atau selepas kata laluan diset semula;<br><br>h. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;<br><br>i. Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan;<br><br>j. Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan | Semua |

| | |
|---|---|
| k. Mengelakkan penggunaan semula kata laluan yang baru digunakan. | |
| **070204 Clear Desk dan Clear Screen** | |
| Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.<br><br>Clear Desk dan 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.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>a. Menggunakan kemudahan password screen saver atau logout apabila meninggalkan komputer;<br><br>b. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan<br><br>c. Memastikan semua dokumen diambil segera dari pencetak,pengimbas, mesin faksimile 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:<br><br>a) Menempatkan atau memasang antara muka yang bersesuaian | |

| | |
|---|---|
| di antara rangkaian MDK, rangkaian agensi lain dan rangkaian awam;<br><br>b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan<br><br>c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT. | Pentadbir Sistem ICT dan ICTSO |
| **070302 Capaian Internet** | |
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>a. Penggunaan Internet di MDK hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan malicious code, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian;<br><br>b. Kaedah Content Filtering mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan;<br><br>c. Penggunaan teknologi ( packet shaper ) untuk mengawal aktiviti (video conferencing, video streaming, chat, downloading ) adalah perlu bagi menguruskan penggunaan jalur lebar (bandwidth ) yang maksimum dan lebih berkesan;<br><br>d. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja.Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya;<br><br>e. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan;<br><br>f. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Bahagian atau pegawai atasan yang diberi kuasa sebelum dimuat naik ke Internet;<br><br>g. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; | Pentadbir Sistem ICT,ICTSO |

| | |
|---|---|
| h. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh bahagian/jabatan/agensi;<br><br>i. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti newsgroup dan bulletin board . Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan;<br><br>j. Penggunaan modem (sendiri) untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; dan<br><br>k. Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut:<br><br>i. Melayari, memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan<br><br>ii. Melayari, menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur unsur lucah, perjudian, fitnah, pelaburan yang diharamkan atau tidak sah, dan lain-lain perkara yang melanggar undang-undang. | |

**0704 Kawalan Capaian Sistem Pengoperasian**

**Objektif:**

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

| **070401 Capaian Sistem Pengoperasian** | |
|---|---|
| Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. | |

| | |
|---|---|
| Kemudahan ini juga perlu bagi:<br><br>a. Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan<br><br>b. Merekodkan capaian yang berjaya dan gagal.<br><br>Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut:<br><br>a. Mengesahkan pengguna yang dibenarkan;<br><br>b. Mewujudkan jejak audit ke atas semua capaian system pengoperasian terutama pengguna bertaraf super user; dan<br><br>c. Menjana amaran ( alert ) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br>a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur log on yang terjamin;<br><br>b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja;<br><br>c) Mengehadkan dan mengawal penggunaan program; dan<br><br>d) Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi. | Pentadbir Sistem ICT dan ICTSO |
| **070402 Kad Pintar** | |
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>a) Penggunaan kad pintar Kerajaan Elektronik (Kad EG) hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan;<br><br>b) Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; | Semua |

| | |
|---|---|
| c) Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; dan<br><br>d) Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada pegawai yang bertanggungjawab di MDK. | |

## 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 aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.<br><br>Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi:<br><br>a. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan;<br><br>b. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log);<br><br>c. Mengehadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;<br><br>d. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan | Pentadbir Sistem ICT dan ICTSO |

| | |
|---|---|
| e. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja. | |

## 0706 Peralatan Mudah Alih dan Kerja Jarak Jauh

### Objektif:

Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh

| | |
|---|---|
| **070601 Peralatan Mudah Alih** | |
| Perkara yang perlu dipat uhi adalah seperti berikut:<br><br>a. Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan. | Semua |
| **070602 Kerja Jarak Jauh** | |
| Perkara yang perlu dipat uhi adalah seperti berikut:<br><br>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 Membangunkan 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:<br><br>a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan 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;<br><br>c) Aplikasi perlu mengandungi semakan pengesahan (validation) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan<br><br>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. | Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO |
| **080102 Pengesahan Data Input dan Output** | |
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>a) Data input bagi aplikasi perlu disahkan bagi memastikan data | Pemilik Sistem |

| | |
|---|---|
| yang dimasukkan betul dan bersesuaian; dan<br><br>b) Data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat. | dan Pentadbir Sistem. |

## 0802 Kawalan Kriptografi

### Objektif:

Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.

| | |
|---|---|
| **080201 Enkripsi** | |
| Pengguna hendaklah membuat enkripsi (encryption ) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa. | Semua |
| **080202 Tandatangan Digital** | |
| Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna (jika ada); khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik. | Semua |
| **080203 Pengurusan Infrastru ktur Kunci Awam ( PKI )** | |
| Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut. | Semua |

## 0803 Keselamatan Fail Sistem

## Objektif:

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

<table>
<tr><td colspan="2">080401 Prosedur Kawalan Perubahan</td></tr>
<tr><td>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai;<br><br>b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor;<br><br>c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja;<br><br>d) Akses kepada kod sumber (source code) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan<br><br>e) Menghalang sebarang peluang untuk membocorkan maklumat.</td><td>Pemilik Sistem dan Pentadbir Sistem ICT</td></tr>
<tr><td colspan="2">080402 Pembangunan Perisian Secara Outsource</td></tr>
<tr><td>Pembangunan perisian secara outsource perlu diselia dan dipantau oleh pemilik sistem.<br><br>Pengujian dan pengiktirafan bagi kualiti dan ketepatan bagi perisian yang dibangunkan hendaklah dilaksanakan dan disahkan oleh pemilik sistem.<br><br>Kod sumber (source code) bagi semua aplikasi dan perisian adalah menjadi hak milik MDK dan jabatan yang berkenaan.</td><td>Jabatan Teknologi Maklumat, Pentadbir Sistem ICT</td></tr>
</table>

| | |
|---|---|

## 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** | |
|---|---|
| Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan.<br><br>Perkara yang perlu dipatuhi adalah seperti berikut:<br><br>a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan;<br><br>b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan<br><br>c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan. | Pentadbir Sistem ICT |

# BIDANG 09: PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

## 0901 Mekanisme Pelaporan Insiden Keselamatan ICT

### Objektif:

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

| **090101 Mekanisme Pelaporan** | |
|---|---|
| Insiden keselamatan ICT bermaksud musibah ( adverse event ) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat.<br><br>Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO Pejabat MDK dan GCERT MAMPU 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;<br><br>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; dan<br><br>e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.<br><br>Prosedur pelaporan insiden keselamatan ICT berdasarkan:<br><br>▪ Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan | Semua |

| | |
|---|---|
| ▪ Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam. | |

## 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 dianalisis 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 MDK.<br><br>Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut:<br><br>a) Menyimpan jejak audit, backup secara berkala dan melindungi integriti semua bahan bukti;<br><br>b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;<br><br>c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan;<br><br>d) Menyediakan tindakan pemulihan segera; dan<br><br>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 Kesinambungan Perkhidmatan** | |
|---|---|
| Pelan Kesinambungan Perkhidmatan (Business Continuity Management - BCM) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan.<br><br>Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JKICT MDK.<br><br>Perkara-perkara berikut perlu diberi perhatian:<br><br>a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;<br><br>b) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT;<br><br>c) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;<br><br>d) Mendokumentasikan proses dan prosedur yang telah dipersetujui;<br><br>e) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;<br><br>f) Membuat backup; dan | Pengurus ICT |

| | |
|---|---|
| g) Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.<br><br>Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut:<br><br>Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;<br><br>Senarai personel MDK dan pembekal berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani insiden;<br><br>Senarai lengkap maklumat yang memerlukan backup dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;<br><br>Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan<br><br>Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh.<br><br>Salinan pelan BCM perlu disimpan di lokasi 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.<br><br>Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan.<br><br>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.<br><br>MDK dan jabatan yang berkenaan yang mempunyai pelan BCM hendaklah memastikan salinan pelan BCM masing-masing sentiasa dikemas kini dan dilindungi seperti di lokasi utama. | |

# BIDANG 11: PEMATUHAN

## 1101 Pematuhan dan Keperluan Perundangan

### Objektif:

Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT MDK.

| | |
|---|---|
| **110101 Pematuhan Dasar** | |
| Setiap pengguna di MDK hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT ini dan undang-undang atau peraturan- peraturan lain yang berkaitan yang berkuat kuasa.<br><br>Semua aset ICT di MDK termasuk maklumat yang disimpan di dalamnya adalah hak milik Kera jaan. Yang Dipertua MDK/ Ketua Jabatan yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.<br><br>Sebarang penggunaan aset ICT MDK dan Jabatan masing-masing selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber. | Semua |
| **110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal** | |
| ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal.<br><br>Sistem maklumat perlu diperiksa 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 maklumat.<br><br>Keperluan audit dan 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** | |
| Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di MDK dan bahagian masing-masing adalah seperti di Lampiran 3. | Semua |
| **110105 Pelanggaran Dasar** | |
| Pelanggaran Dasar Keselamatan ICT ini boleh dikenakan tindakan tatatertib. | Semua |

# GLOSARI

| | |
|---|---|
| **Antivirus** | Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, optical disk, flash disk , CDROM, thumb drive untuk sebarang kemungkinan adanya virus. |
| **Aset ICT** | Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. |
| **Backup** | Proses penduaan sesuatu dokumen atau maklumat. |
| **Bandwidth** | Lebar Jalur<br>Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan. |
| **CIO** | Chief Information Officer<br>Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi. |
| **Denial of service** | Halangan pemberian perkhidmatan. |
| **Downloading** | Aktiviti muat-turun sesuatu perisian. |
| **Encryption** | Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah. |
| **Firewall** | Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya. |
| **Forgery** | Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan |

| | |
|---|---|
| | pencurian identiti, pencurian maklumat ( information theft/espionage ), penipuan ( hoaxes). |
| **GCERT** | Government Computer Emergency Response Team atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya. |
| **Hard disk** | Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas. |
| **Hub** | Hab ( hub ) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan ( broadcast) data yang diterima daripada sesuatu port kepada semua port yang lain. |
| **ICT** | Information and Communication Technology (Teknologi Maklumat dan Komunikasi). |
| **ICTSO** | ICT Security Officer - Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer. |
| **Internet** | Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain. |
| **Internet Gateway** | Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan. |
| **Intrusion Detection System (IDS)** | Sistem Pengesan Pencerobohan<br>Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian. |

| | |
|---|---|
| **Intrusion Prevention System (IPS)** | Sistem Pencegah Pencerobohan<br>Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya.Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau malicious code.<br>Contohnya: Network-based IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan. |
| **LAN** | Local Area Network<br>Rangkaian Kawasan Setempat yang menghubungkan computer |
| **Logout** | Log-out komputer<br>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<br>Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer. |
| **Outsource** | Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui. |
| **Perisian Aplikasi** | Ia merujuk pada perisian atau pakej yang selalu digunakan seperti spreadsheet dan word processing ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan. |
| **Public-Key Infrastructure (PKI)** | Infrastruktur Kunci Awam mer upakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet. |
| **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 komputer. |
| **Switches** | Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian Carrier Sense Multiple Access/Collision Detection (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku. |
| **Uninterruptible Power Supply (UPS)** | Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung. |
| **Video Conference** | Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar. |
| **Video Conference** | Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak |
| **Virus** | Atur cara yang bertujuan merosakkan data atau sistem aplikasi. |
| **Wireless LAN** | Jaringan komputer yang terhubung tanpa melalui kabel. |

# LAMPIRAN 1: SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT MAJLIS DAERAH KERIAN

Nama (Huruf Besar) : ……………………………………………………
No. Kad Pengenalan : ……………………………………………………
Jawatan : ……………………………………………………
Jabatan : ……………………………………………………

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT ini; dan

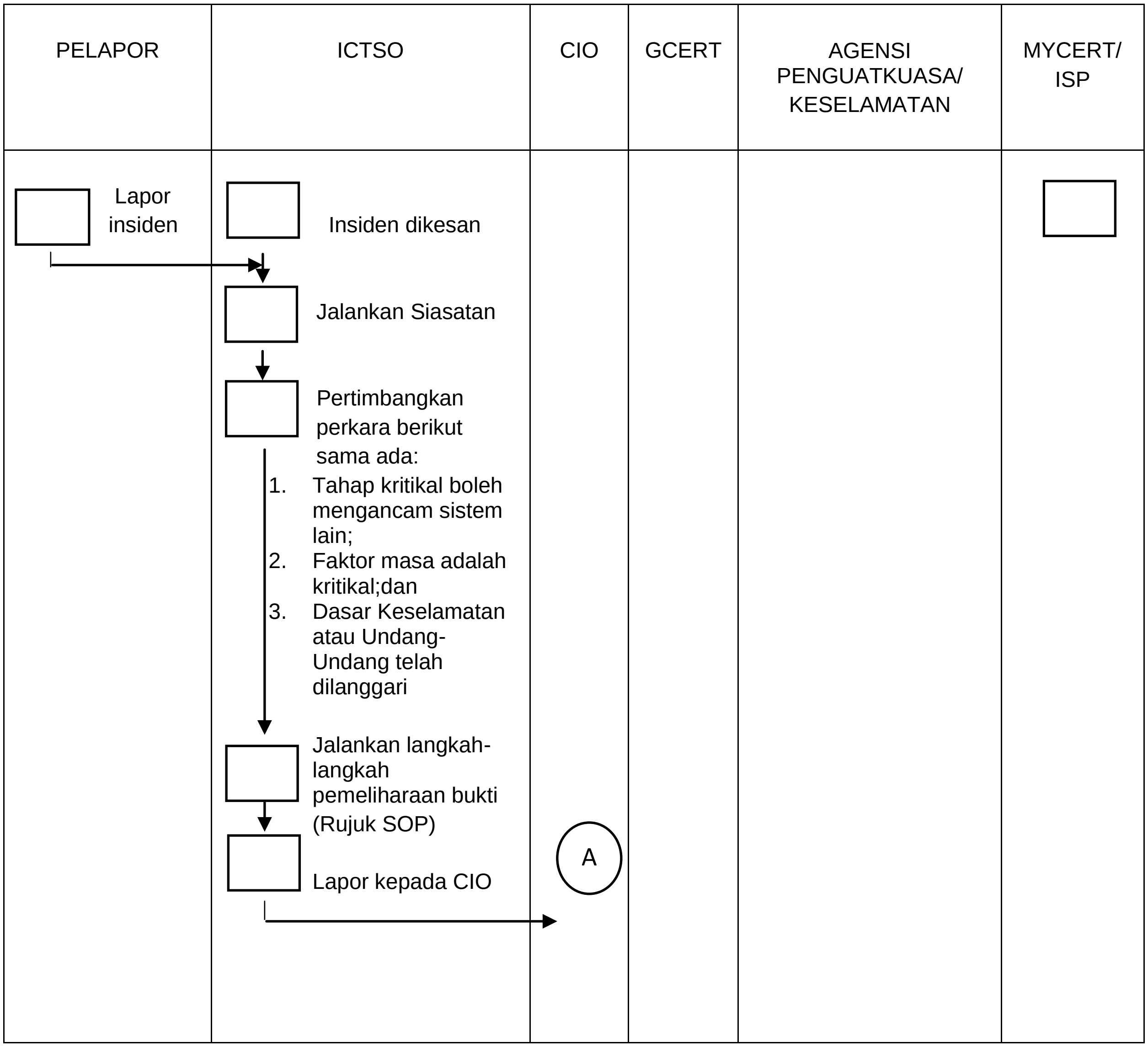
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

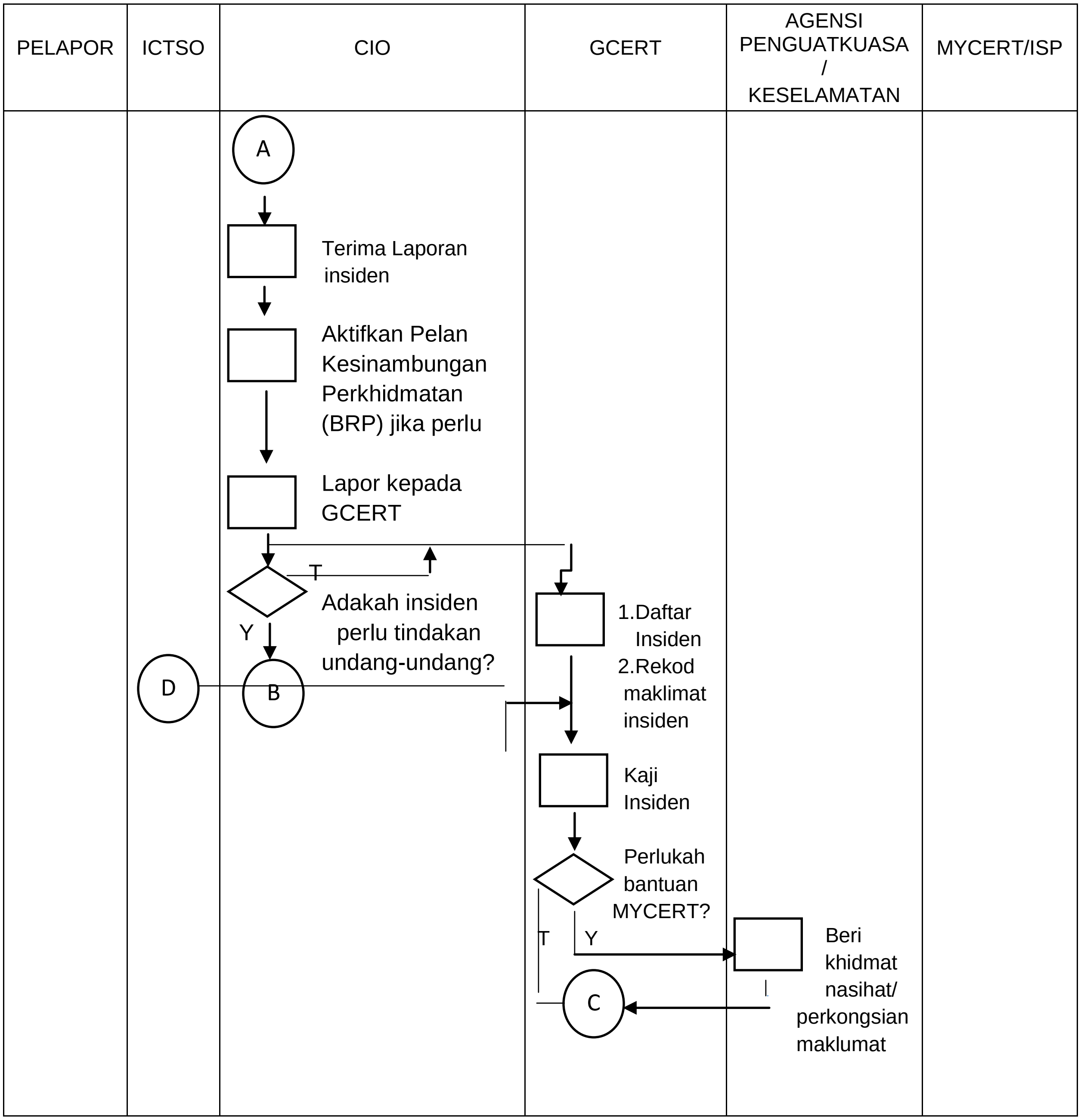
Tanda tangan : .................................................
Tarikh : .................................................

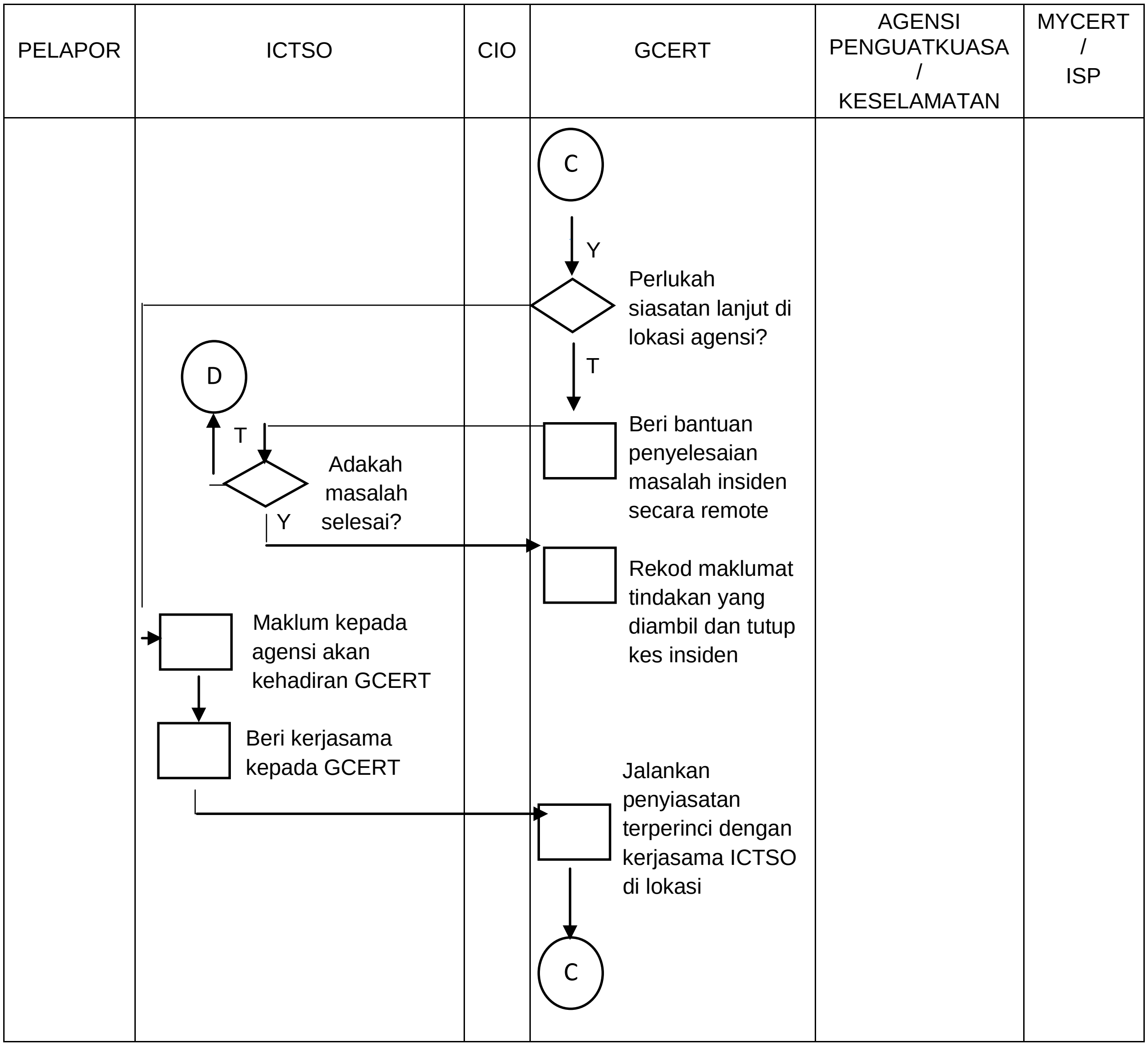
**Pengesahan Pegawai Keselamatan ICT**
.......................................
( )
b.p. Yang Dipertua
Majlis Daerah Kerian

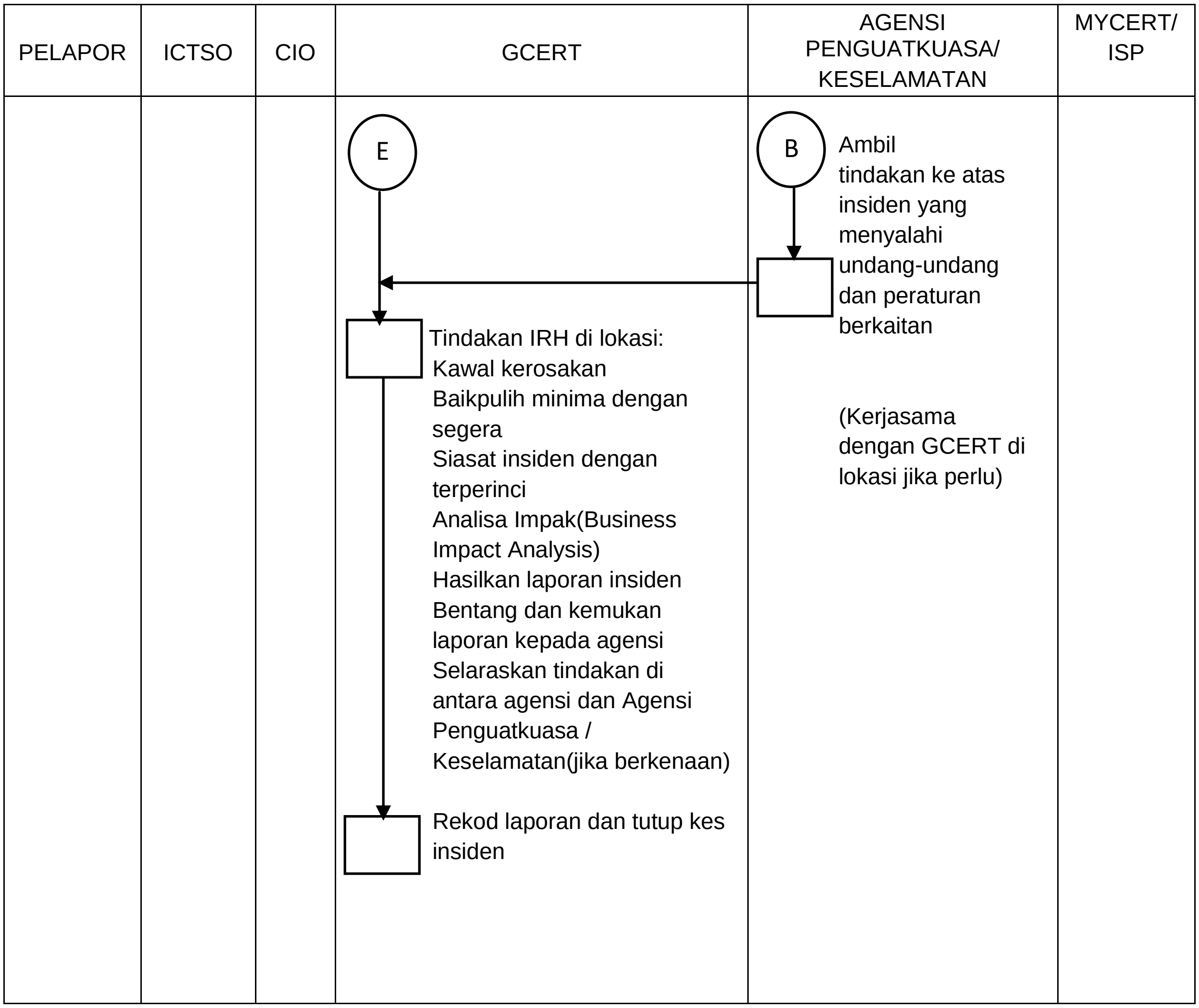
Tarikh: .........................

# LAMPIRAN 2: RINGKASAN PROSES KERJA PELAPORAN INSIDEN KESELAMATAN ICT




PELAPOR
ICTSO
CIO
GCERT
AGENSI PENGUATKUASA / KESELAMATAN
MYCERT/ISP
A
Terima Laporan insiden
Aktifkan Pelan Kesinambungan Perkhidmatan (BRP) jika perlu
Lapor kepada GCERT
T
Adakah insiden perlu tindakan undang-undang?
Y
D
B
1.Daftar Insiden
2.Rekod maklimat insiden
Kaji Insiden
Perlukah bantuan MYCERT?
T
Y
Beri khidmat nasihat/ perkongsian maklumat
C


PELAPOR
ICTSO
CIO
GCERT
AGENSI PENGUATKUASA / KESELAMATAN
MYCERT / ISP
C
Y
Perlukah siasatan lanjut di lokasi agensi?
T
D
T
Beri bantuan penyelesaian masalah insiden secara remote
Adakah masalah selesai?
Y
Rekod maklumat tindakan yang diambil dan tutup kes insiden
Maklum kepada agensi akan kehadiran GCERT
Beri kerjasama kepada GCERT
Jalankan penyiasatan terperinci dengan kerjasama ICTSO di lokasi
C




**Penunjuk:**

SOP-Standard Operating Procedure

## LAMPIRAN 3: SENARAI PERUNDANGAN DAN PERATURAN

1. Arahan Keselamatan;

2. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;

3. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002;

4. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);

5. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;

6. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;

7. Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;

8. Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006;

9. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;

10. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;

11. Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);

12. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender;

13. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;

14. Akta Tandatangan Digital 1997;

15. Akta Rahsia Rasmi 1972;

16. Akta Jenayah Komputer 1997;

17. Akta Hak Cipta (Pindaan) Tahun 1997;
18. Akta Komunikasi dan Multimedia 1998;
19. Perintah-Perintah Am;
20. Arahan Perbendaharaan;
21. Arahan Teknologi Maklumat 2007;
22. Garis Panduan Keselamatan MAMPU 2004;
23. Standard Operating Procedure (SOP) ICT MAMPU;
24. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;
25. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.