# GARIS PANDUAN
# KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI
# (GPKTMK)
# 2014

# UNIVERSITI PUTRA MALAYSIA

**ISI KANDUNGAN**

## 1.0 PENGENALAN

Garis Panduan Keselamatan Teknologi Maklumat dan Komunikasi (GPKTMK) Universiti Putra Malaysia (UPM) mengandungi peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Garis panduan ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT UPM.

## 2.0 OBJEKTIF

GPKTMK UPM diwujudkan untuk menjamin kesinambungan urusan UPM dengan meminimumkan kesan insiden keselamatan ICT. Garis Panduan ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi UPM. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi. Objektif utama Keselamatan ICT UPM ialah:

a. Memastikan kelancaran operasi UPM yang berasaskan ICT dan meminimumkan kerosakan atau kemusnahan.
b. Melindungi kepentingan pihak yang bergantung kepada sistem maklumat mengenai kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi.
c. Mencegah salah guna atau kecurian aset ICT UPM.

## 3.0 PERNYATAAN

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman atau 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 risiko sentiasa berubah. Keselamatan Teknologi Maklumat dan Komunikasi (KTMK) 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. KTMK berkait rapat dengan perlindungan aset ICT.

Terdapat empat (4) komponen asas keselamatan ICT iaitu:

a. Melindungi maklumat rahsia rasmi dan maklumat rasmi UPM daripada akses tanpa kebenaran yang sah.
b. Menjamin setiap maklumat adalah sah, tepat dan lengkap.
c. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna.
d. Memastikan akses hanya kepada pengguna yang sah atau penerimaan maklumat daripada sumber yang sah.

GPKTMK merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan

kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

a. Kerahsiaan - Maklumat tidak boleh didedahkan sewenang-wenangnya atau diakses tanpa kebenaran;
b. Integriti - Data dan maklumat hendaklah tepat, lengkap dan terkini. Ia hanya boleh diubah dengan cara yang dibenarkan;
c. Tidak Boleh Disangkal - Punca data dan maklumat hendaklah daripada punca yang sah dan tidak boleh disangkal;
d. Kesahihan - Data dan maklumat hendaklah dijamin kesahihannya; dan
e. Ketersediaan - Data dan maklumat hendaklah boleh diakses apabila perlu.

Selain itu, langkah-langkah ke arah menjamin KTMK hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT dan ancaman yang wujud akibat daripada kelemahan tersebut.

Risiko yang mungkin timbul dan langkah-langkah pencegahan yang sesuai perlu diambil untuk menangani masalah berkenaan.

## 4.0 SKOP

Aset ICT UPM terdiri daripada peralatan, perisian, perkhidmatan, data atau maklumat dan manusia. Bagi menentukan keselamatan Aset ICT terjamin sepanjang masa, GPKTMK UPM ini merangkumi perlindungan semua bentuk maklumat UPM 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 berikut:

a. **Peralatan** - Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan UPM. (Contoh: 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 UPM.
c. **Perkhidmatan** - Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsinya. Contoh:
    i. Perkhidmatan infrastruktur rangkaian seperti LAN, WAN dan lain-lain.
    ii. Sistem kawalan akses seperti sistem kad akses.
    iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.
d. **Data atau Maklumat** - Koleksi fakta dalam bentuk kertas atau elektronik, yang mengandungi maklumat untuk digunakan bagi mencapai misi dan objektif UPM. Contohnya, sistem dokumentasi, prosedur operasi, rekod UPM, profil pelanggan, pangkalan data dan fail data, maklumat arkib dan lain-lain.

e. **Manusia** - Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian bagi mencapai misi dan objektif UPM. Individu berkenaan merupakan aset berdasarkan kepada tugasan dan fungsi yang dilaksanakan.

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 pelanggaran langkah-langkah keselamatan.

## 5.0 PEMBANGUNAN DAN PENYELENGGARAAN DOKUMEN GPKTMK

### 5.1 Garis Panduan Keselamatan Teknologi Maklumat dan Komunikasi (GPKTMK)

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

**a) Pelaksanaan**
Pelaksanaan garis panduan ini akan dijalankan oleh Ketua Pegawai Teknikal (CTO) UPM selaku Pengerusi Jawatankuasa Keselamatan ICT (JKKTMK) UPM. JKKTMK ini terdiri daripada Ketua Pegawai Operasi (COO), Pengurus Keselamatan ICT (ICTSM), Pegawai Keselamatan ICT (ICTSO), Pentadbir Sistem ICT, Wakil Pegawai Akademik Fakulti Sains Komputer dan Teknologi Maklumat serta Wakil Pegawai Akademik Fakulti Kejuruteraan.

**b) Penyebaran**
Garis panduan ini perlu disebarkan kepada semua pengguna UPM (termasuk staf, pelajar, pembekal, pakar runding dan lain-lain).

**c) Penyelenggaraan**
GPKTMK UPM adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa dari segi kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, Kaedah-kaedah UPM (Teknologi maklumat dan Komunikasi) dan kepentingan sosial. Prosedur yang berhubung dengan penyelenggaraan GPKTMK UPM adalah seperti berikut:

i. Kenal pasti dan tentukan perubahan yang diperlukan. Perubahan GPKTMK perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko;
ii. Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan JKKTMK;
iii. Membuat hebahan kepada pengguna, perubahan yang telah dipersetujui oleh JKKTMK; dan
iv. Garis Panduan ini hendaklah disemak semula mengikut keperluan semasa (sekurang-kurangnya 1 tahun sekali).

**d) Pengecualian**

GPKTMK UPM adalah terpakai kepada semua pengguna perkhidmatan ICT UPM dan tiada pengecualian diberikan.

## 5.2 Prinsip

Prinsip yang menjadi asas kepada GPKTMK UPM dan mesti dipatuhi adalah seperti berikut:

**a) Akses atas Asas Perlu Mengetahui**

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas asas "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**

Hak akses pengguna umum hanya diberi pada tahap 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:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. Memasti dan menentukan maklumat tepat dan lengkap dari semasa ke semasa;
iii. Menentukan maklumat sedia untuk digunakan;
iv. Menjaga kerahsiaan kata laluan;
v. Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
vi. Memberi perhatian kepada maklumat terperingkat terutamanya semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.

**d) Pengasingan**

Tugas mewujud, menghapus, mengemaskini dan mengesahkan data perlu diasingkan bagi mengelakkan daripada akses yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau

dimanipulasi. 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 dipastikan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail* (jejak audit).

**f) Pematuhan**

GPKTMK UPM 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.

**h) Saling Bergantungan**

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

## 5.3 Penilaian Risiko Keselamatan ICT

UPM hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat ancaman dan kerentanan (vulnerability) yang semakin meningkat saban hari. Justeru itu, UPM perlu mengambil langkah-langkah proaktif yang bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

UPM hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya, perlu 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 UPM termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem sokongan lain.

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

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

a. Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
b. Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi;
c. Mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan
d. Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak lain yang berkepentingan.

## 6.0 ORGANISASI KESELAMATAN MAKLUMAT

### 6.1 Struktur Organisasi Dalaman

**Objektif**
Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif GPKTMK UPM.

**a) Ketua Pegawai Teknikal (CTO)**

Ketua Pegawai Teknikal (CTO) bagi UPM ialah Pengarah iDEC. Peranan dan tanggungjawab CTO adalah seperti berikut:

i. Bertanggungjawab ke atas perkara yang berkaitan dengan keselamatan ICT UPM;
ii. Memastikan semua pengguna memahami dan mematuhi peruntukan di bawah GPKTMK UPM;
iii. Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; dan
iv. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam GPKTMK UPM.

**b) Ketua Pegawai Operasi (COO)**

Ketua Pegawai Operasi (COO) bagi UPM ialah Timbalan Pengarah (Pengurusan Strategik dan Sokongan Pengguna) iDEC, UPM. Peranan dan tanggungjawab COO adalah seperti berikut:

i. Membantu CTO dalam melaksanakan tugas yang melibatkan keselamatan ICT;
ii. Menyelaras keperluan keselamatan ICT yang melibatkan keseluruhan operasi ICT UPM;
iii. Menyelaras penyediaan GPKTMK UPM dan pengurusan risiko serta pengauditan; dan
iv. Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT.

**c) Pengurus Keselamatan ICT (ICTSM)**

Pengurus Keselamatan ICT (ICTSM) bagi UPM ialah Timbalan Pengarah (Perkhidmatan Infrastruktur ICT) iDEC, UPM. Peranan dan tanggungjawab ICTSM adalah seperti berikut:

i. Mengurus keseluruhan program keselamatan ICT UPM;
ii. Menguatkuasakan pelaksanaan GPKTMK UPM;
iii. Memberi penerangan dan pendedahan berkenaan GPKTMK UPM kepada semua pengguna;
iv. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan GPKTMK UPM;
v. Melaksanakan pengurusan risiko;
vi. Melaksanakan audit, mengkaji semula, merumus tindak balas pengurusan UPM berdasarkan hasil penemuan dan menyediakan laporan mengenainya;
vii. Melaporkan insiden keselamatan ICT kepada Pasukan Tindak Balas Insiden Keselamatan ICT UPM (UPMCERT), Ketua Pegawai Teknikal (CTO) dan memaklumkannya kepada Pasukan Tindak Balas Keselamatan ICT Kerajaan (GCERT); dan
viii. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera.

**d) Pegawai Keselamatan ICT (ICTSO)**

ICTSO bagi UPM ialah Ketua Unit Keselamatan ICT iDEC, UPM. Peranan dan tanggungjawab ICTSO adalah seperti berikut:

i. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;
ii. Menyedia dan melaksanakan program kesedaran mengenai keselamatan;
iii. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSM; dan
iv. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT UPM.

**e) Pentadbir Sistem ICT**

Pentadbir Sistem ICT bagi UPM ialah semua Ketua Unit iDEC. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut:

i. Mengambil tindakan dengan segera apabila dimaklumkan mengenai staf yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas;
ii. Menentukan ketepatan dan kesempurnaan sesuatu tahap akses berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam GPKTMK UPM;
iii. Memantau aktiviti akses harian sistem aplikasi pengguna;
iv. Mengenal pasti aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatal atau memberhentikannya dengan serta merta;
v. Menganalisis dan menyimpan rekod jejak audit;
vi. Menyediakan laporan mengenai aktiviti akses secara berkala; dan

vii. Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.

**f) Pengguna**

Pengguna ICT UPM ialah mereka yang menggunakan segala peralatan dan perisian ICT di UPM. Pengguna mempunyai peranan dan tanggungjawab seperti berikut:

i. Membaca, memahami dan mematuhi GPKTMK UPM;
ii. Melepasi tapisan keselamatan mengikut keperluan UPM;
iii. Melaksanakan prinsip-prinsip GPKTMK UPM dan menjaga kerahsiaan maklumat UPM;
iv. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;
v. Menghadiri program kesedaran mengenai keselamatan ICT; dan
vi. Menandatangani perjanjian sebagaimana berikut:
    a. Pelajar menandatangani surat akujanji pelajar.
    b. Staf menandatangani surat akujanji staf.
    c. Pihak ketiga menandatangani Surat Akuan Pematuhan GPKTMK UPM.

**g) Pasukan Tindak Balas Insiden Keselamatan ICT UPM (UPMCERT)**

Keanggotaan UPMCERT adalah seperti berikut:

**Pengurus**

Pengurus Keselamatan ICT (ICTSM)

**Ahli**

i. Pegawai Keselamatan ICT (ICTSO) – Setiausaha
ii. Pegawai Teknologi Maklumat (Unit Keselamatan ICT)
iii. Pegawai Teknologi Maklumat (Bidang Kepakaran - Rangkaian)
iv. Pegawai Teknologi Maklumat (Bidang Kepakaran - Pangkalan Data)
v. Pegawai Teknologi Maklumat (Bidang Kepakaran - Aplikasi)
vi. Pegawai Teknologi Maklumat (Bidang Kepakaran - *Server*)

**Bidang Kuasa**

i. Menerima dan mengesah aduan keselamatan ICT serta menilai tahap dan jenis insiden;
ii. Merekod dan menjalankan siasatan awal insiden yang diterima;
iii. Menangani tindak balas (response) insiden keselamatan ICT dan mengambil tindakan baik pulih;
iv. Menasihati pengguna mengambil tindakan pemulihan dan pengukuhan;
v. Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada pengguna; dan
vi. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden dapat dielakkan.

## 6.2 Pengkomputeran Mudah Alih dan *Teleworking*

**Objektif**
Memastikan keselamatan maklumat semasa menggunakan peralatan pengkomputeran mudah alih dan kemudahan *teleworking.*

**a) Panduan Pengkomputeran Mudah Alih**

i. Pendaftaran peralatan pengkomputeran mudah alih;
ii. Keperluan perlindungan secara fizikal;
iii. Mengehadkan instalasi perisian;
iv. Keperluan pengawalan versi perisian pengkomputeran mudah alih dan *patch*; dan
v. Mengehadkan akses kepada perkhidmatan maklumat tertentu.

**b) Teleworking**

Kemudahan *teleworking* hendaklah dilindungi bagi menghalang pendedahan maklumat dan akses tidak sah serta salah guna kemudahan.

## 7.0 KESELAMATAN SUMBER MANUSIA

**Objektif**
Memastikan sumber manusia yang terlibat termasuk staf UPM, pembekal, pakar runding dan pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua staf UPM hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

**a) Sebelum Perkhidmatan**

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab staf UPM serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan
ii. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang ditetapkan.

**b) Dalam Perkhidmatan**

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Memastikan staf UPM serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh UPM;
ii. Memastikan latihan kesedaran dan latihan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT UPM secara berterusan dalam melaksanakan tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa;
iii. Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas staf UPM serta pihak ketiga yang berkepentingan sekiranya berlaku pelanggaran dengan perundangan dan peraturan yang ditetapkan oleh UPM; dan

iv. Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT.

**c) Bertukar atau Tamat Perkhidmatan**

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Memastikan semua aset ICT dikembalikan kepada UPM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan
ii. Membatalkan atau menarik balik semua kebenaran akses ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh UPM dan/atau terma perkhidmatan.

## 8.0 PENGURUSAN ASET

### 8.1 Akauntabiliti Aset

**Objektif**

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

**a) Inventori Aset ICT**

Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang mesti dipatuhi adalah seperti berikut:

i. Memastikan semua aset ICT dikenal pasti, maklumat aset direkod dalam sistem pengurusan aset dan sentiasa dikemas kini;
ii. Memastikan semua aset ICT didaftarkan pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja;
iii. Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di dalam dan luar UPM tetapi perlu mengikut peraturan yang telah ditetapkan;
iv. Peraturan pengendalian aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan; dan
v. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.

### 8.2 Pengelasan dan Pengendalian Maklumat

**Objektif**

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

**a) Pengelasan Maklumat**

Maklumat hendaklah dikelaskan atau dilabel sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Setiap maklumat yang

dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan dalam dokumen Arahan Keselamatan seperti berikut:

i. Rahsia Besar
ii. Rahsia
iii. Sulit
iv. Terhad

**b) Pengendalian Maklumat**

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

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
iii. Menentukan maklumat sedia untuk digunakan;
iv. Menjaga kerahsiaan kata laluan, data dan maklumat;
v. Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pengwujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

**c) Pengendalian Rekod**

Aktiviti pengendalian rekod seperti mengenalpasti, mengindeks, mengesan, menyelenggara dan melupuskan sesuatu rekod merangkumi kawalan rekod dalam bentuk bercetak dan elektronik dengan mengambil kira langkah-langkah keselamatan berikut:

i. Mendaftarkan rekod yang diwujud dan diterima ke dalam fail bagi tujuan kawalan dan jagaan;
ii. Menyediakan bilik khas bagi penyimpanan dan pengendalian yang tidak aktif atau telah ditutup;
iii. Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan yang telah ditetapkan; dan
iv. Memberi perhatian kepada rekod yang penting dan bernilai bagi mencegah pemalsuan dan penipuan.

## 8.3 Pengendalian Media

**Objektif**

Melindungi peralatan media digital daripada sebarang pendedahan, pengubahsuaian, perpindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.

**a) Penghantaran dan Perpindahan**

Penghantaran atau perpindahan media storan dan maklumat ke luar pejabat hendaklah mendapat kebenaran daripada pegawai yang bertanggungjawab.

**b) Kaedah Pengendalian Media**

Kaedah pengendalian media yang perlu dipatuhi adalah seperti berikut:

i. Melabelkan semua media mengikut tahap klasifikasi sesuatu maklumat;
ii. Mengehadkan dan menentukan akses media kepada pengguna yang dibenarkan sahaja;
iii. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;
iv. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan;
v. Menyimpan semua media di tempat yang selamat; dan
vi. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.

**c) Keselamatan Dokumentasi Sistem**

Memastikan penyimpanan dokumentasi sistem adalah terkawal dan mempunyai ciri-ciri keselamatan.

## 9.0 KAWALAN AKSES

### 9.1 Dasar Kawalan Akses

**Objektif**

Mengawal akses ke atas maklumat.

**a) Keperluan Kawalan Akses**

Akses kepada proses dan maklumat perlu dikawal, direkodkan dan dikemas kini mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza.

### 9.2 Pengurusan Capaian Pengguna

**Objektif**

Mengawal akses pengguna ke atas aset ICT UPM.

**a) Akaun Pengguna**

Melaksanakan pendaftaran dan penamatan akaun pengguna untuk memberi dan menarik balik hak akses terhadap aset ICT UPM.

Pentadbir Sistem ICT boleh membeku atau menamatkan akaun pengguna atas sebab berikut:

i. Pengguna yang bercuti panjang dalam tempoh waktu melebihi tiga (3) bulan;
ii. Bertukar bidang tugas serta skop kerja;
iii. Bertukar ke agensi lain;
iv. Bersara; atau
v. Ditamatkan perkhidmatan.

**b) Hak Akses Pengguna**

Peruntukan dan penggunaan hak akses pengguna perlu dikawal dan diselia dengan rapi.

**c) Kata Laluan**

Pemilihan dan penggunaan kata laluan bagi mencapai aset ICT mestilah mematuhi amalan terbaik.

**d) Pengurusan Kata Laluan**

Pengurusan kata laluan perlulah interaktif, mesra pengguna dan disemak secara berkala.

**e) Tanggungjawab Pengguna**

Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.

Pengguna tidak dibenarkan meninggalkan bahan yang sensitif terdedah sama ada di atas meja (Clear Desk Policy) atau di paparan skrin (Clear Screen Policy) apabila pengguna tidak berada di tempatnya.

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer;
ii. Menyimpan bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan
iii. Memastikan semua dokumen diambil segera daripada pencetak, mesin faksimili dan mesin fotostat.

## 9.3 Kawalan Akses Sistem Pengoperasian *Server*

**Objektif**

Menghalang akses tidak sah dan tanpa kebenaran ke atas sistem pengoperasian server.

**a) *Login* Yang Selamat**

*Login* kepada sistem pengoperasian server perlu dikawal mengikut prosedur pemantauan akses.

**b) Pengenalan dan Pengesahan Pengguna**

Setiap pengguna perlu ada pengenalan diri (ID) yang unik.

**c) Penggunaan *System Tools***

Penggunaan *system tools* yang berkeupayaan mengambil alih sistem dan mengawal aplikasi perlulah dihadkan dan dikawal.

**d) Session *Time-out***

Sesi yang tidak aktif perlu ditutup dalam tempoh masa yang ditetapkan.

**e) Had Masa Akses**

Had masa Akses perlu dilaksanakan untuk meningkatkan keselamatan bagi aplikasi yang berisiko tinggi.

## 9.4 Keselamatan Fail Sistem

**Objektif**
Memastikan keselamatan fail sistem terjamin.

**a) Kawalan Fail Sistem**
Perkara yang mesti dipatuhi adalah seperti berikut:
i. Pengemaskinian fail sistem adalah tanggungjawab Pentadbir Sistem ICT dan perlu mematuhi prosedur yang telah ditetapkan;
ii. Kod sumber atau atur cara sistem yang telah dikemas kini hanya boleh digunakan selepas diuji; dan
iii. Akses ke atas kod sumber atau atur cara sistem perlu dikawal.

# 10.0 KAWALAN KRIPTOGRAFI

**Objektif**
Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi berdasarkan kepada Dasar Kriptografi Negara. Antara kawalan yang boleh dilakukan adalah seperti berikut:

**a) Enkripsi**
Maklumat sensitif atau maklumat rahsia rasmi hendaklah dikawal dengan kaedah enkripsi.

**b) Tanda Tangan Digital**
Transaksi maklumat sensitif atau maklumat rahsia rasmi secara elektronik hendaklah menggunakan tanda tangan digital.

**c) Pengurusan *Public Key Infrastructure* (PKI)**
Pengurusan PKI hendaklah dilakukan dengan selamat dan berkesan bagi melindungi kunci berkenaan daripada diubah, dimusnah atau didedahkan sepanjang tempoh sah kunci tersebut.

# 11.0 KESELAMATAN FIZIKAL DAN PERSEKITARAN

## 11.1 Persekitaran Selamat

**Objektif**
Melindungi maklumat dan kemudahan pemprosesan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan, gangguan dan akses yang tidak dibenarkan.

**a) Keselamatan Fizikal Kawasan**
Ini bertujuan untuk mengawal akses, menghalang kerosakan dan gangguan secara fizikal terhadap premis, maklumat dan kemudahan pemprosesan maklumat UPM.

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas;
ii. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko;
iii. Ruang tetamu premis hendaklah dikawal oleh petugas atau kaedah kawalan lain;
iv. Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;
v. Semua pintu di kawasan keselamatan fizikal harus dipasang dengan alat penggera, dipantau dan diuji supaya mematuhi piawaian yang ditetapkan; dan
vi. Sistem pencegahan pencerobohan yang sesuai perlu dipasang dalam kawasan keselamatan fizikal.

**b) Kawalan Masuk Fizikal**

Ini bertujuan untuk mengawal akses secara fizikal terhadap premis agensi. Kawalan akses merupakan aktiviti utama dalam aspek keselamatan maklumat. Kawalan masuk fizikal hendaklah dikenal pasti dan mekanisma akses fizikal hendaklah mematuhi peraturan dan garis panduan yang ditetapkan. Mekanisma kawalan akses adalah seperti berikut:

i. Fizikal (contoh: Pintu Keselamatan)
ii. Teknologi (contoh: Biometrik, Kad Pintar)
iii. Pentadbiran (contoh: Pas Pelawat, Buku Log)

**c) Kawasan Larangan**

Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada staf yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawalan akses yang dimaksudkan adalah seperti berikut:

i. Akses ke kawasan larangan hanyalah kepada staf yang dibenarkan sahaja;
ii. Pihak Ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; dan
iii. Hak akses ke kawasan larangan hendaklah disemak semula secara berterusan dan maklumat hak akses dikemaskini.

**d) Keselamatan Pejabat, Bilik dan Kemudahan**

Ini bertujuan untuk memastikan keselamatan fizikal pejabat, bilik dan kemudahan sentiasa terjamin. Perkara yang mesti dipatuhi adalah seperti berikut:

i. Kemudahan utama perlu diasingkan daripada akses umum;
ii. Papan tanda dan maklumat mengenai fungsi bangunan tidak didedahkan pada umum;
iii. Kemudahan perlu dikonfigurasi supaya aktiviti atau maklumat sulit tidak dilihat atau didengar dari luar. Perlindungan elektromagnetik juga perlu dititik beratkan; dan

iv. Buku panduan dan buku telefon dalaman yang mengandungi kemudahan pemprosesan maklumat yang sulit perlu dikawal akses daripada pihak yang tidak dibenarkan.

**e) Kawalan Persekitaran**

Bagi menghindarkan kerosakan dan gangguan terhadap premis ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, mengubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada pihak yang menguruskan keselamatan dan kesihatan pekerjaan; dan pihak yang menguruskan pembangunan serta pengurusan aset di UPM. Bagi menjamin keselamatan persekitaran, perkara yang mesti dipatuhi adalah seperti berikut:

i. Merancang dan menyediakan pelan keseluruhan susun atur Pusat Data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti;
ii. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan, seperti alat sistem pasif dan aktif pengesan pencegah kebakaran;
iii. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan;
iv. Bahan kimia mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT;
v. Semua sumber cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan daripada aset ICT;
vi. Tidak menggunakan peralatan elektrik yang tidak berkaitan;
vii. Semua peralatan perlindungan hendaklah disemak dan diuji mengikut peraturan dan keperluan semasa; dan
viii. Akses kepada saluran *riser* hendaklah sentiasa dikunci.

**f) Bekerja dalam Kawasan Keselamatan**

Tatacara kerja semasa berada dalam kawasan keselamatan hendaklah diwujudkan dan dilaksanakan bagi memastikan perkara berikut dipatuhi:

i. Semua staf perlu tahu tentang kewujudan kawasan keselamatan dan aktivitinya;
ii. Pelaksanaan aktiviti tanpa penyeliaan hendaklah dielak bagi tujuan keselamatan dan bagi mencegah sebarang peluang pencerobohan;
iii. Kawasan keselamatan yang tidak digunakan perlu dikunci dan dipantau secara berkala; dan
iv. Peralatan pengambaran, video, audio dan peralatan rakaman lain hendaklah dilarang dalam kawasan keselamatan kecuali diberi kebenaran.

**g) Kawasan Penghantaran dan Pemunggahan**

Kawasan masuk fizikal untuk penghantaran dan pemunggahan hendaklah diasingkan daripada kemudahan pemprosesan maklumat supaya ianya dikawal daripada pencerobohan oleh pihak yang tidak dibenarkan. Perkara yang mesti dipatuhi adalah seperti berikut:

i. Kebenaran masuk ke kawasan penghantaran dan pemunggahan mestilah terhad kepada staf yang telah dikenalpasti dan dibenarkan sahaja;
ii. Kawasan penghantaran dan pemunggahan hendaklah ditempatkan dalam kawasan di mana pihak yang menghantar tidak perlu melalui bangunan lain;

iii. Pintu luar kawasan penghantaran dan pemunggahan hendaklah dikunci apabila pintu dalam dibuka;
iv. Bahan yang diterima hendaklah diperiksa bagi memastikan ianya tidak mengandungi bahan letupan, bahan kimia dan lain-lain bahan berbahaya sebelum dialih ke kawasan penghantaran dan pemunggahan;
v. Bahan yang diterima hendaklah didaftarkan mengikut prosedur pengurusan aset;
vi. Penghantaran masuk dan penghantaran keluar hendaklah diasingkan jika boleh; dan
vii. Bahan yang diterima hendaklah diperiksa untuk sebarang *tampering* sewaktu proses penghantaran dan jika didapati ada unsur *tampering*, laporan kepada pihak keselamatan perlu dibuat.

**h) Perkhidmatan Sokongan**

Bagi memastikan peralatan ICT berfungsi dengan baik semua perkhidmatan sokongan (bekalan kuasa, telekomunikasi, bekalan air, gas, kumbahan, pengedaran udara dan penghawa dingin) hendaklah dikawal daripada gangguan atau kerosakan. Perkara yang mesti dipatuhi adalah seperti berikut:

i. Semua peralatan ICT hendaklah dibekalkan dengan bekalan elektrik yang sesuai;
ii. Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana (generator) hendaklah digunakan bagi perkhidmatan kritikal seperti di Pusat Data supaya mendapat bekalan kuasa berterusan;
iii. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual dan jika perlu dipasang alat penggera untuk mengesan kerosakan; dan
iv. Pencahayaan dan komunikasi semasa kecemasan hendaklah disediakan dan suis kecemasan untuk mematikan bekalan perlu disediakan.

**i) Keselamatan Kabel**

Kabel letrik dan rangkaian hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah atau mengalami kerosakan. Langkah-langkah keselamatan yang mesti diambil adalah seperti berikut:

i. Menggunakan kabel letrik dan kabel rangkaian yang menepati Sistem Pengkabelan Berstruktur (Structured Cabling System) dan spesifikasi yang telah ditetapkan;
ii. Melindungi kabel letrik dan rangkaian daripada kerosakan yang disengajakan atau tidak disengajakan;
iii. Kabel letrik dan kabel rangkaian perlu diasingkan untuk mengelakkan gangguan;
iv. Semua kabel rangkaian hendaklah dilabelkan dengan jelas dan mestilah melalui *trunking* yang dilindungi bagi memastikan keselamatan kabel rangkaian daripada kerosakan dan pintasan maklumat;
v. Sebarang kerosakan yang berlaku ke atas kabel rangkaian hendaklah diambil tindakan segera; dan
vi. Bagi sistem yang sensitif atau kritikal pemasangan sistem kawalan yang lebih ketat hendaklah dilaksanakan.

## 11.2 Keselamatan Dokumen

**Objektif**
Melindungi maklumat UPM daripada sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian dan perubahan teknologi.

**a) Dokumen**

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Setiap dokumen hendaklah difailkan dan dilabel mengikut klasifikasi keselamatan;
ii. Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan;
iii. Kehilangan dan kerosakan ke atas semua jenis dokumen hendaklah dimaklumkan mengikut prosedur Arahan Keselamatan; dan
iv. Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara.

## 11.3 Keselamatan Peralatan

**Objektif**
Melindungi peralatan ICT UPM daripada kehilangan, kerosakan, kecurian, penyalahgunaan serta gangguan kepada peralatan tersebut.

**a) Peralatan ICT**

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Pengguna bertanggungjawab sepenuhnya ke atas peralatan ICT masing-masing dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;
ii. Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna;
iii. Pengguna tidak dibenarkan membuat sebarang pengubahsuaian ke atas perkakasan dan perisian yang telah ditetapkan;
iv. Sebarang aktiviti pengurusan aset ICT seperti pergerakan dan kehilangan hendaklah mematuhi peraturan kewangan UPM;
v. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;
vi. Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (administrator password) yang telah ditetapkan oleh Pentadbir Sistem ICT; dan
vii. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO.

**b) Media Storan Mudah Alih**

Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, pita magnetik, *optical disk*, *flash disk*, dan media storan lain. Media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan dan kebolehsediaan untuk digunakan. Perkara yang mesti dipatuhi adalah seperti berikut:

i. Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;
ii. Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja;
iii. Semua media storan perlu dikawal bagi mencegah daripada akses yang tidak dibenarkan, kecurian dan kemusnahan;
iv. Semua media storan yang mengandungi data kritikal hendaklah disimpan di tempat yang sesuai dan mempunyai ciri-ciri keselamatan;
v. Akses dan pergerakan media storan hendaklah direkodkan;
vi. Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan
vii. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.

**c) Media Tandatangan Digital**

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan;
ii. Media ini tidak boleh dipindah milik atau dipinjamkan; dan
iii. Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.

**d) Media Perisian dan Aplikasi**

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Hanya perisian yang diperakui bagi kegunaan UPM;
ii. Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurusan UPM;
iii. Lesen perisian (Kod Pendaftaran, nombor siri, *CD-keys*) perlu dilindungi bagi mengelakkan daripada berlakunya kecurian atau cetak rompak; dan
iv. Kod Sumber dan dokumentasi sesuatu sistem aplikasi UPM hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.

**e) Penyelenggaraan Peralatan**

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Semua peralatan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar;
ii. Peralatan hanya boleh diselenggara oleh staf UPM atau pihak ketiga yang dibenarkan sahaja;
iii. Bertanggungjawab terhadap setiap peralatan bagi penyelenggaraan peralatan sama ada dalam tempoh jaminan atau telah tamat tempoh jaminan;
iv. Menyemak dan menguji semua peralatan sebelum dan selepas proses penyelenggaraan;
v. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan
vi. Rekod penyelenggaraan hendaklah disimpan.

**f) Peralatan di Luar Premis**

Peralatan yang dibawa keluar dari premis UPM adalah terdedah kepada pelbagai risiko. Perkara yang mesti dipatuhi adalah seperti berikut:

i. Pengunaan peralatan di luar premis hendaklah mendapat kelulusan pihak Pengurusan UPM;
ii. Staf atau pihak luar yang diberi kuasa untuk membenarkan peralatan dibawa keluar dari premis hendaklah dikenalpasti;
iii. Tempoh masa peralatan boleh berada di luar premis hendaklah ditetapkan dan verifikasi terhadapan peralatan perlu dibuat bila peralatan dibawa masuk ke dalam premis;
iv. Rekod peralatan keluar masuk perlu disimpan;
v. Peralatan perlu sentiasa dilindungi dan dikawal;
vi. Penyimpanan atau penempatan peralatan di luar premis mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian dan menilai risko yang berkaitan; dan
vii. Log perpindahan peralatan di luar premis antara individu hendaklah direkodkan dan tanggungjawab individu terhadap peralatan hendaklah dinyatakan.

**g) Pelupusan Peralatan**

Pelupusan melibatkan semua peralatan ICT, sama ada harta modal atau inventori yang telah rosak, usang dan tidak boleh dibaiki, yang disediakan oleh UPM dan ditempatkan di UPM. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan UPM. Perkara yang mesti dipatuhi adalah seperti berikut:

i. Data di dalam storan hendaklah dipastikan telah dihapus dengan cara yang selamat sebelum sesuatu peralatan ICT dilupuskan atau sebelum dipindah milik;
ii. Sekiranya maklumat perlu disimpan, pengguna bolehlah membuat penduaan mengikut kaedah yang ditetapkan;
iii. Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan; dan
iv. Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara seperti berikut:
    a. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi;
    b. Menyimpan dan memindahkan perkakasan luaran komputer seperti *AVR, speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di UPM;
    c. Memindah keluar dari UPM mana-mana peralatan ICT yang hendak dilupuskan; dan
    d. Melupuskan sendiri peralatan ICT.

**h) Peralatan Ditinggalkan Pengguna**

Semua peralatan yang ditinggalkan dalam apa jua bentuk media hendaklah dikawal / dipastikan keselamatannya.

Pengguna hendaklah tidak meninggalkan bahan yang sensitif terdedah sama ada di atas meja (Clear Desk Policy) atau di paparan skrin (Clear Screen Policy) apabila tidak berada di tempatnya.

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan peralatan komputer;
ii. Menyimpan bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan
iii. Memastikan semua dokumen diambil segera daripada pencetak, mesin faksimili dan mesin fotostat.

**i) Panduan *Clear Desk* dan *Clear Screen***

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Maklumat sensitif atau kritikal perlu disimpan dengan selamat bila tidak digunakan;
ii. Komputer dan terminal perlu di *logoff* atau dipasang *screen saver* atau menggunakan mekanisme mengunci papan kekunci; dan
iii. Penggunaan tanpa kebenaran peralatan pencetak, mesin fotostat atau alat penyalin tidak dibenarkan.

## 12.0 PENGURUSAN OPERASI KESELAMATAN

### 12.1 Prosedur Operasi

**Objektif**

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

**a) Pengendalian Prosedur**

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Semua prosedur pengurusan operasi yang diwujudkan, dikenal pasti dan diguna pakai hendaklah didokumenkan, disimpan dan dikawal;
ii. Setiap prosedur mestilah mengandungi arahan yang jelas, teratur dan lengkap; dan
iii. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.

**b) Kawalan Perubahan**

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai yang bertanggungjawab atau pemilik aset ICT terlebih dahulu;
ii. Aktiviti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;
iii. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan

iv. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat.

**c) Pengasingan Tugas dan Tanggungjawab**

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Skop tugas dan peranan setiap pegawai perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT;
ii. Tugas mewujud, menghapus, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada akses yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; dan
iii. Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan semasa *production*.

**d) Pengurusan Kapasiti**

Pengurusan Kapasiti mesti dilaksanakan dalam pengurusan ICT Universiti dengan melaksanakan perancangan kapasiti bagi sesuatu pembangunan atau penaiktarafan infrastruktur dan infostruktur.

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Perancangan kapasiti perlu dibuat sebelum sesuatu pembangunan ICT dilaksanakan bagi mengoptimumkan keupayaan sesuatu infrastruktur ICT; dan
ii. Pengawalan penggunaan sumber perlu dilaksanakan dalam memastikan pembangunan sistem ICT sentiasa berada di tahap keupayaan optimum.

## 12.2 Perisian Berbahaya

**Objektif**

Melindungi integriti perisian dan maklumat daripada pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya (malicious software).

**a) Perlindungan daripada Perisian Berbahaya**

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Memasang sistem keselamatan seperti *Anti Virus, Intrusion Detection System (IDS)* dan *Intrusion Prevention System (IPS)* untuk mengesan perisian atau fail berbahaya;
ii. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa;
iii. Mengimbas perisian atau sistem yang ditetapkan dengan anti virus sebelum menggunakannya;
iv. Memastikan paten antivirus dikemaskini dengan versi terkini;
v. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;

vi. Mempunyai kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;
vii. Memasukkan klausa liabiliti di dalam kontrak yang akan ditawarkan kepada pihak ketiga. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;
viii. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus; dan
ix. Larangan membuat akses kepada laman web yang disenarai hitamkan atau dikenal pasti merbahaya.

**b) Perlindungan daripada *Mobile Code***

Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.

Perkara yang mesti dipatuhi adalah seperti berikut:
i. Memastikan perisian *antivirus* sentiasa dikemaskini;
ii. Mengubah tetapan pelayar untuk menyekat aplikasi interaktif seperti JavaScript daripada beroperasi secara automatik; dan
iii. Sentiasa mengemaskini *patches* pelayar.

## 12.3 Penyelenggaraan Maklumat

**Objektif**

Melindungi integriti maklumat agar boleh diakses apabila diperlukan.

**a) *Backup***

*Backup* hendaklah dilakukan bagi memastikan sistem dapat digunakan semula sekiranya berlaku bencana. Perkara yang perlu dipatuhi adalah seperti berikut:
i. Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi secara berkala atau apabila terdapat perubahan versi;
ii. Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat;
iii. Menguji sistem *backup* dan *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan;
iv. Menyimpan backup sekurang-kurangnya setahun ataupun mengikut keperluan sistem;
v. Merekod dan menyimpan salinan *backup* di lokasi yang berlainan, selamat dan bergantung kepada keperluan sistem;
vi. Melaksanakan *backup* selepas waktu pejabat untuk mengurangkan beban pada waktu puncak kepada infrastruktur ICT; dan
vii. *Backup Tools* hendaklah hanya disimpan oleh staf ICT yang ditugaskan sahaja dan digunakan dengan kawalan dan kebenaran penyelia staf ICT tersebut.

**b) *Housekeeping***

*Housekeeping* perlu dilakukan bagi memastikan sistem dapat berfungsi dengan baik. Perkara yang mesti dipatuhi adalah seperti berikut:

i. Pengemaskinian perisian dan sistem aplikasi; dan
ii. Pengurusan fail sistem dan storan seperti pembersihan log dan fail sementara (*temporary file*).

## 12.4 *Logging* dan Pemantauan

**Objektif**
Memastikan aktiviti pemprosesan maklumat direkodkan dan bukti aktiviti dapat diterbitkan jika diperlukan.

**a) *Event Logging***

i. Perlu mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna pengecualian ralat dan maklumat keselamatan aktiviti; dan
ii. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera.

Log aktiviti mesti mengandungi maklumat berikut:

i. Rekod setiap aktiviti transaksi;
ii. Maklumat log mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan;
iii. Aktiviti akses pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan
iv. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.

**b) Perlindungan Maklumat Log**

Kemudahan merekod log dan maklumat log perlu dilindungi daripada sebarang akses atau pengubahsuaian yang tidak dibenarkan.

**c) Pentadbir dan Operator Log**

Semua aktiviti pentadbir sistem dan operator sistem perlu direkodkan, dikawal serta disemak secara berkala**.**

**d) Pelarasan Masa**

Masa sistem pengoperasian perlu diselaraskan dengan satu sumber rujukan yang telah ditetapkan.

## 12.5 Kawalan Ke atas Perisian Pengoperasian

**Objektif**
Memastikan integriti bagi sistem pengoperasian.

**a) Instalasi Perisian Sistem Pengoperasian.**

Prosedur perlu dilaksanakan bagi mengawal pemasangan perisian ke atas sistem pengoperasian. Perkara yang mesti dipatuhi adalah seperti berikut:

i. Pengemaskinian perisian sistem operasi dan aplikasi mestilah dilaksanakan oleh pegawai yang telah diberi kuasa;
ii. Perisian sistem operasi dan aplikasi yang digunakan mestilah sentiasa dikemaskini dengan ***patches*** yang terkini;
iii. Sesi pengujian secara berasingan mestilah meliputi kebolehgunaan, keselamatan, impak kepada sistem lain dan juga mesra pengguna sebelum perisian sistem operasi dan aplikasi digunapakai;
iv. Strategi ***rollback*** mestilah diwujudkan sebelum sebarang perubahan dilaksanakan;
v. Sistem kawalan konfigurasi mestilah digunakan untuk menyimpan kawalan bagi semua implimentasi perisian dan boleh digunakan sebagai dokumentasi sistem; dan
vi. Log mestilah dikemaskini bagi semua proses sistem operasi dan aplikasi.

## 12.6 Pengurusan Kerentanan Teknikal

**Objektif**
Memastikan pengurusan kerentanan teknikal adalah sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.

**a) Kawalan daripada Ancaman Teknikal**

Pengurusan kerentanan teknikal perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang mesti dipatuhi adalah seperti berikut:

i. Memperolehi maklumat kerentanan teknikal yang tepat pada masanya terhadap sistem maklumat yang digunakan;
ii. Menilai tahap pendedahan bagi mengenal pasti risiko yang bakal dihadapi; dan
iii. Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.

**b) Mengehadkan Instalasi Perisian**

Peraturan instalasi perisian oleh pengguna hendaklah diwujudkan dan dilaksanakan.

Organisasi mestilah menakrif dan menguatkuasa polisi yang ketat ke atas setiap perisian yang mungkin diinstalasi oleh pengguna melalui prinsip kelayakan minima (*least privilege).*

## 12.7 Pertimbangan Audit Sistem Maklumat

**Objektif**
Untuk meminimumkan kesan aktiviti pengauditan ke atas sistem pengoperasian.

**a) Kawalan Audit Sistem Maklumat**

Aktiviti dan keperluan audit yang melibatkan verifikasi sistem pengoperasian hendaklah dirancang dengan teliti dan dipersetujui untuk meminimumkan gangguan(disruptions) pada proses sesebuah organisasi.

## 13.0 KESELAMATAN KOMUNIKASI

### 13.1 Pengurusan Keselamatan Rangkaian

**Objektif**
Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

**a) Kawalan Infrastruktur Rangkaian**
Infrastruktur rangkaian hendaklah dikawal dan diuruskan sebaik mungkin bagi melindungi daripada ancaman kepada maklumat. Perkara yang mesti dipatuhi adalah seperti berikut:

i. Tanggungjawab dan kerja operasi hendaklah diasingkan untuk menghalang akses dan pengubahsuaian yang tidak dibenarkan;
ii. Perkakasan *firewall* hendaklah dipasang, dikonfigurasi dan ditadbir di mana semua trafik keluar dan masuk hendaklah melalui *firewall*;
iii. Pengguna dilarang menggunakan perisian *sniffer* atau *network analyzer* kecuali mendapat kebenaran pentadbir sistem rangkaian;
iv. Memasang *Intrusion Prevention System (IPS)* bagi mengesan sebarang cubaan menceroboh dan aktiviti lain yang boleh mengancam sistem dan maklumat UPM;
v. Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang;
vi. Sebarang penyambungan rangkaian tanpa kelulusan adalah tidak dibenarkan;
vii. Sistem intranet UPM hanya boleh diakses menggunakan sistem rangkaian UPM sahaja seperti menggunakan teknologi *Virtual Private Network (VPN);* dan
viii. Semua peralatan ICT (termasuk peralatan bukan aset UPM) yang menggunakan sistem rangkaian UPM perlu selamat dan tidak mendatangkan risiko.

### 13.2 Kawalan Akses Rangkaian

**Objektif**
Menghalang akses tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.

**a) Perkhidmatan Rangkaian**
Pengguna hanya boleh mencapai perkhidmatan rangkaian yang dibenarkan sahaja.

**b) Akses Pengguna daripada Rangkaian Luar**
Kaedah akses yang bersesuaian perlu digunakan untuk mengawal akses dari rangkaian luar.

**c) Pengenalpastian Peralatan**
Pengenalpastian peralatan secara automatik perlu ada bertujuan untuk spesifikasi lokasi dan peralatan yang disahkan.

**d) Akses Internet**

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Penggunaan Internet di UPM hendaklah dipantau secara berterusan oleh Pentadbir Sistem Rangkaian bagi memastikan penggunaannya untuk tujuan akses yang dibenarkan sahaja. Amalan ini akan melindungi daripada kemasukan *malicious code*, virus dan bahan yang tidak sepatutnya ke dalam rangkaian UPM;

ii. Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan;

iii. 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;

iv. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pentadbir Sistem ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya;

v. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Pentadbir Sistem ICT yang diberi kuasa;

vi. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan;

vii. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada pegawai yang bertanggungjawab sebelum dimuat naik ke Internet;

viii. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;

ix. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh UPM;

x. Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; dan

xi. Pengguna adalah dilarang melakukan aktiviti berikut:

   a. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video atau lagu yang boleh menjejaskan tahap akses Internet; dan

   b. Menyedia, memuat naik, memuat turun dan menyimpan teks ucapan atau bahan yang mengandungi unsur lucah.

## 13.3 Pengurusan Pertukaran Maklumat

**Objektif**

Memastikan keselamatan pertukaran maklumat dan perisian antara UPM dan agensi luar terjamin.

**a) Pertukaran Maklumat**

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Persetujuan bertulis hendaklah diwujudkan untuk pertukaran maklumat dan perisian di antara UPM dengan agensi luar melalui penggunaan pelbagai jenis kemudahan komunikasi;

ii. Maklumat yang terdapat dalam mesej elektronik hendaklah dilindungi sebaik-baiknya; dan
iii. Media yang mengandungi maklumat hendaklah dilindungi daripada akses yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari UPM.

**b) Pengurusan Mel Elektronik (e-Mel)**

Penggunaan e-mel di UPM hendaklah dipantau secara berterusan oleh pentadbir sistem e-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk *"Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"* dan mana-mana undang-undang bertulis yang berkuat kuasa.

Perkara yang mesti dipatuhi dalam pengendalian mel elektronik adalah seperti berikut:

i. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh UPM sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;
ii. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh UPM;
iii. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;
iv. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul;
v. Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh megabait (10 Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;
vi. Pengguna hendaklah mengelak untuk membuka e-mel daripada penghantar yang tidak diketahui atau diragui;
vii. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;
viii. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan;
ix. E-mel tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;
x. Pengguna hendaklah memastikan tarikh dan masa sistem komputer adalah tepat;
xi. Pengguna hendaklah mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera;
xii. Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan
xiii. Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing.

## 14.0 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM MAKLUMAT

### 14.1 Keselamatan dalam Pembangunan Sistem dan Aplikasi

**Objektif**
Memastikan sistem yang dibangunkan untuk kegunaan UPM mempunyai ciri-ciri keselamatan ICT yang bersesuaian di setiap fasa pembangunan serta mengikut prosedur pembangunan yang telah ditetapkan.

**a) Keperluan Keselamatan Sistem Maklumat**

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira analisis keperluan dan keselamatan ICT;
ii. Ujian keselamatan yang dijalankan meliputi pengesahan identiti pengguna dan pengujian ke atas *input*, pemprosesan dan *output* sistem bagi memastikan keselamatan dan integriti data;
iii. Aplikasi perlu melalui semakan serta pengesahan identiti pengguna dan tahap akses tertentu yang dibenarkan bagi mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan;
iv. Ciri-ciri keselamatan sistem maklumat perlu dipantau secara berterusan bagi memastikan ketersediaan sistem, kerahsiaan dilindungi dan integriti dipelihara; dan
v. Semua sistem yang dibangunkan sama ada secara dalaman atau luaran hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.

**b) Kesahihan Data *Input* dan *Output***

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Data *input* aplikasi perlu disemak kesahihannya bagi memastikan data yang dimasukkan betul dan sesuai; dan
ii. Data *output* daripada aplikasi perlu disemak kesahihannya bagi memastikan maklumat yang dihasilkan adalah tepat.

**c) Melindungi Transaksi Perkhidmatan Aplikasi**

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Maklumat pengesahan kerahsiaan pengguna untuk semua pihak adalah sah dan disahkan;
ii. Mengekalkan tahap kerahsiaan, integriti dan kesediaan sesuatu transaksi;
iii. Privasi yang berkaitan dengan semua pihak yang terlibat dikekalkan;
iv. Laluan dan protokol komunikasi adalah selamat; dan
v. Data dan maklumat dilindungi mengikut mana-mana peruntukan undang-undang untuk perlindungan atau kerahsiaan.

## 14.2 Keselamatan dalam Operasi dan Penyelenggaraan Sistem Maklumat

**Objektif**
Menjaga dan menjamin keselamatan dan integriti sistem maklumat dan aplikasi dalam sebarang keadaan

**a) Prosedur Kawalan Perubahan**

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Sistem dan aplikasi hendaklah dikawal, diuji, didokumen dan disahkan sebelum digunapakai jika berlaku sebarang perubahan;
ii. Permohonan perubahan perlu dikemukakan oleh pemilik sistem dan perubahan dilakukan mematuhi tahap kawalan dan integriti tertentu;
iii. Dokumen kawalan versi sistem dan kod sumber perlu dikemaskini jika terdapat perubahan;
iv. Dokumentasi sistem, dokumentasi operasi dan panduan pengguna perlu dikemaskini secara berterusan mengikut perubahan sistem;
v. Sebarang perubahan platform/sistem pengoperasian terhadap aplikasi kritikal, kajian dan ujian terperinci perlu dilakukan bagi mengelak gangguan operasi sistem serta tidak mengganggu pelan kesinambungan organisasi;
vi. Sebarang perubahan ke atas pakej perisian hendaklah dikawal, dihadkan mengikut keperluan sahaja dan serasi dengan perisian lain yang digunakan; dan
vii. Sebarang ruang dan peluang kebocoran maklumat hendaklah dihalang.

**b) Pemantauan Perkhidmatan Sistem Maklumat**

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Pemantauan secara berterusan ke atas penyampaian perkhidmatan sistem maklumat; dan
ii. Mencegah atau menghalang sebarang aktiviti seperti pencerobohan, pecah kontrak, pendedahan dan pengubahsuaian maklumat yang tidak dibenarkan.

## 14.3 Persekitaran Pembangunan Selamat

**Objektif**
Mewujudkan dan melindungi persekitaran pembangunan yang selamat untuk pembangunan dan integrasi sistem bagi mengurangkan risiko keselamatan pembangunan secara dalaman.

**a) Prosedur Kawalan Persekitaran Selamat**

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Menjaga sensitiviti data untuk diproses, disimpan dan dihantar oleh sistem serta mengawal pergerakan data;
ii. Kebolehpercayaan kakitangan yang bekerja di persekitaran;
iii. Kawalan keselamatan yang telah dilaksanakan oleh organisasi yang menyokong pembangunan sistem;
    a. pengawalan akses kepada persekitaran pembangunan;
    b. keperluan bagi pengasingan di antara persekitaran pembangunan yang berbeza; dan

c. tahap akses khidmat luar yang berkaitan dengan pembangunan sistem;

iv. Pemantauan terhadap perubahan persekitaran dan kod yang disimpan di dalamnya; dan

v. *Backup* disimpan di lokasi lain yang selamat.

**b) Pengujian Pembangunan atau Penaiktarafan Sistem**

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Sistem yang dibangunkan perlu diuji secara menyeluruh oleh pembangun sistem sepanjang proses pembangunan termasuk ujian keselamatan fungsian, proses *input* dan proses *output* bagi memastikan sistem dibangunkan seperti yang diharapkan serta mematuhi ciri-ciri keselamatan yang ditetapkan;

ii. Ujian penerimaan sistem perlu dijalankan yang merangkumi pengujian keperluan keselamatan maklumat dan kepatuhan kepada amalan pembangunan sistem yang selamat. Pengujian yang dijalankan perlu dijalankan di persekitaran sebenar bagi memastikan sistem tersebut selamat daripada sebarang ancaman; dan

iii. Semua data pengujian yang digunakan perlu dipilih dengan teliti, dilindungi dan dikawal semasa dan selepas proses pengujian sistem bagi memastikan keselamatan data pengujian yang digunakan.

**c) Pembangunan Sistem Aplikasi oleh Pihak Ketiga**

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Pembangunan aplikasi oleh pihak ketiga perlu diselia dan dipantau pada setiap peringkat pembangunan;

ii. Kod sumber (*source code*) bagi semua sistem aplikasi yang dibangunkan khusus untuk UPM adalah menjadi hak milik UPM;

iii. Pihak ketiga perlu menandatangani *Non-disclosure Agreement* (NDA) sebelum pembangunan aplikasi; dan

iv. Latihan kesedaran (*awareness training*) diberi kepada kakitangan yang terlibat, mengenai perkara berikut:

a. Polisi perolehan pembangunan aplikasi, proses serta prosedur yang berkaitan.

b. Tatacara pengurusan pengendalian pihak ketiga.

c. Tahap akses kepada sistem aplikasi dan maklumat UPM, mengikut kategori pihak ketiga.

## 14.4 Keselamatan dalam Pembangunan Infrastruktur ICT

**Objektif**

Memastikan keperluan infrastruktur ICT yang dibangunkan mengambil kira ciri-ciri keselamatan data yang bersesuaian dan mengikut prosedur pembangunan yang telah ditetapkan.

a) Keperluan Keselamatan Infrastruktur Pra-pembangunan Infrastruktur ICT. Perancangan pembangunan dilaksanakan bagi memastikan perkara berikut:

i. Mengurangkan gangguan kepada sistem yang sedia ada; dan

ii. Meminimakan sebarang impak negatif terhadap perkhidmatan Universiti.

b) Keperluan Keselamatan Infrastruktur semasa Pembangunan Infrastruktur ICT. Perkara yang mesti dipatuhi adalah seperti berikut:
   i. Memastikan akses sistem terkawal; dan
   ii. Memastikan integriti dan keselamatan data yang dipindahkan terjamin.

c) Keperluan Keselamatan Infrastruktur selepas Pembangunan Infrastruktur ICT. Perkara yang mesti dipatuhi adalah seperti berikut:
   i. Memastikan pengujian Infrastruktur baharu mematuhi keperluan; dan
   ii. Memastikan dokumentasi penyerahan adalah lengkap.

## 15.0 HUBUNGAN DENGAN PEMBEKAL

### 15.1 Pihak Ketiga

**Objektif**
Menjamin keselamatan semua aset ICT yang digunakan oleh Pihak Ketiga.

**a) Keperluan Keselamatan Kontrak dengan Pihak Ketiga**
Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal.

Perkara yang mesti dipatuhi adalah seperti berikut:
i. Memastikan pihak ketiga membaca, memahami dan mematuhi GPKTMK UPM;
ii. Mengenal pasti keperluan keselamatan sebelum memberi kebenaran akses atau penggunaan kepada pihak ketiga;
iii. Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran akses;
iv. Memastikan akses kepada aset ICT UPM berlandaskan kepada perjanjian kontrak;
v. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai;
   a. GPKTMK UPM;
   b. Tapisan Keselamatan;
   c. Perakuan Akta Rahsia Rasmi 1972; dan
   d. Hak Harta Intelek.
vi. Menandatangani Surat Akuan Pematuhan GPKTMK UPM.

### 15.2 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.

**a) Penyampaian Perkhidmatan**

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Memastikan kawalan keselamatan, skop perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksana dan diselenggarakan oleh pihak ketiga; dan

ii. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga hendaklah sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa.

## 15.3 Perancangan dan Penerimaan Sistem

**Objektif**

Meminimumkan risiko yang boleh menyebabkan gangguan atau kegagalan sistem.

**a) Perancangan Kapasiti (Keupayaan)**

i. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang bertanggungjawab bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT.

ii. 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.

**b) Penerimaan Sistem**

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

# 16.0 PENGURUSAN INSIDEN KESELAMATAN ICT

## 16.1 Mekanisme Pelaporan Insiden Keselamatan ICT

**Objektif**

Memastikan insiden keselamatan ICT dikendalikan dengan cepat dan berkesan.

**a) Mekanisme Pelaporan**

Insiden keselamatan ICT yang perlu dilaporkan kepada ICTSO dan UPMCERT UPM dengan kadar segera adalah seperti berikut:

i. Maklumat didapati hilang atau disyaki hilang;

ii. Maklumat didedahkan kepada pihak yang tidak diberi kuasa atau disyaki sedemikian;

iii. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;

iv. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki sedemikian;

v. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan masalah komunikasi; dan

vi. Berlaku percubaan menceroboh, penyelewengan dan insiden yang tidak dijangka.

Prosedur Pelaporan Insiden Keselamatan ICT berdasarkan pekeliling berikut:

a. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi MAMPU; dan
b. Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam rujukan MAMPU.

Bagi sumber manusia dan aset fizikal, pelaporan hendaklah mengikut prosedur yang ditetapkan pihak yang menguruskan keselamatan dan kesihatan; dan pihak yang menguruskan pembangunan serta pengurusan aset di UPM.

## 16.2 Pengurusan Maklumat Insiden Keselamatan ICT

**Objektif**

Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.

**a) Pengurusan Maklumat Insiden Keselamatan ICT**

Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengurangkan 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 UPM.

Bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan.

Kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut:

i. Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti;
ii. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;
iii. Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan;
iv. Menyediakan tindakan pemulihan segera; dan
v. Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.

## 17.0 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

### 17.1 Dasar Kesinambungan Perkhidmatan

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

**a) Pelan Pengurusan Kesinambungan Perkhidmatan (PKP)**

Pelan Pengurusan Kesinambungan Perkhidmatan (Business Continuity Management) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses penyediaan perkhidmatan organisasi. Pelan PKP mestilah diluluskan oleh Pengurusan UPM.

Perkara yang perlu diberi perhatian adalah seperti berikut:

i. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;
ii. Mengenal pasti kebarangkalian dan impak yang boleh mengakibatkan gangguan terhadap perkhidmatan serta keselamatan ICT;
iii. Melaksanakan prosedur kecemasan agar pemulihan dapat dilakukan dengan segera;
iv. Mendokumentasikan proses dan prosedur diuruskan secara berpusat;
v. Mengadakan program latihan prosedur kecemasan kepada pegawai yang bertanggungjawab dan berkaitan;
vi. Menyediakan *backup*; dan
vii. Menguji dan menyemak pelan PKP dari semasa ke semasa atau mengikut keperluan.

Pelan PKP perlu dibangunkan dan hendaklah mengandungi perkara berikut:

i. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;
ii. Senarai staf UPM dan pembekal berserta maklumat untuk dihubungi (faksimili, telefon dan e-mel). Senarai kedua hendaklah disediakan bagi tujuan gantian staf yang tidak dapat hadir untuk menangani insiden;
iii. Senarai lengkap maklumat yang memerlukan backup dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;
iv. Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan
v. Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan.

Perkara yang mesti dipatuhi adalah seperti berikut:

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

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

## 18.0 PEMATUHAN

### 18.1 Pematuhan dan Keperluan Perundangan

**Objektif**
Meningkatkan tahap keselamatan ICT melalui pematuhan GPKTMK UPM bagi mengelakkan daripada pelanggaran undang-undang atau peraturan yang berkuatkuasa.

**a) Pematuhan GPKTMK UPM**
Pengguna UPM perlu membaca, memahami dan mematuhi GPKTMK UPM. Sebarang penggunaan aset ICT UPM yang berpotensi mengganggu gugat urus tadbir selain daripada maksud dan tujuan rasmi adalah merupakan penyalahgunaan sumber UPM.

**b) Pematuhan Kaedah-Kaedah UPM (Teknologi Maklumat dan Komunikasi), Piawaian dan Keperluan Teknikal**
ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi Kaedah-Kaedah UPM (Teknologi Maklumat dan Komunikasi), piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi piawaian pelaksanaan keselamatan ICT.

**c) Pematuhan Keperluan Audit Keselamatan Sistem Maklumat**
Perkara yang perlu dipatuhi adalah seperti berikut:
i. Pematuhan kepada keperluan audit bertujuan meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit;
ii. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan; dan
iii. Penggunaan peralatan audit perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.

**d) Keperluan Perundangan**
Setiap pengguna adalah tertakluk kepada segala undang-undang, peraturan dan seumpamanya mengenai penggunaan ICT yang sedang berkuatkuasa di Malaysia. Keperluan perundangan atau peraturan lain yang perlu dipatuhi oleh semua pengguna adalah seperti berikut:
i. Arahan Keselamatan;
ii. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi MAMPU;
iii. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002;
iv. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);

v. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi MAMPU;
vi. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
vii. Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;
viii. Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-Agensi MAMPU yang bertarikh 20 Oktober 2006;
ix. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) - Tatacara Penyediaan, Penilaian dan Penerimaan Tender;
x. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;
xi. Akta Keselamatan Pekerja;
xii. Akta Tandatangan Digital 1997;
xiii. Akta Rahsia Rasmi 1972;
xiv. Akta Jenayah Komputer 1997;
xv. Akta Hak Cipta (Pindaan) Tahun 1997;
xvi. Akta Komunikasi dan Multimedia 1998;
xvii. Perintah-Perintah Am;
xviii. Arahan Perbendaharaan; dan
xix. Arahan Teknologi Maklumat 2007.

**e) Pelanggaran GPKTMK UPM**

UPM berhak menentukan undang-undang dan tatatertib atau peraturan yang perlu berlandaskan undang-undang Malaysia jika berlaku sebarang pelanggaran penggunaan GPKTMK. UPM juga berhak mengambil tindakan yang sewajarnya ke atas pelanggaran GPKTMK.

## 19.0 DEFINISI / 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.

**Arahan Keselamatan**

a. Rahsia - Dokumen rasmi atau maklumat rasmi yang boleh menyebabkan kerosakan yang amat besar kepada negara.
b. Rahsia Besar - Dokumen rasmi atau maklumat rasmi yang boleh membahayakan keselamatan negara, kerosakan besar kepada kepentingan dan martabat negara atau memberi keuntungan besar kepada negara asing.
c. Sulit - Dokumen rasmi yang tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat negara atau kegiatan kerajaan, boleh

menyebabkan kesusahan kepada pentadbiran atau orang perseorangan dan menguntungkan sebuah kuasa asing.

d. Terhad - Dokumen rasmi selain daripada di atas tetapi masih perlu diberi perlindungan keselamatan.

**Aset**
ICT Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.

**Backup**
Proses penduaan sesuatu dokumen atau maklumat.

**Bandwidth**
Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.

**Denial of service**
Halangan pemberian perkhidmatan.

**Encryption**
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).

**UPMCERT**
*UPM Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT UPM. Organisasi yang ditubuhkan untuk membantu Pegawai ICT PTJ mengurus pengendalian insiden keselamatan ICT di PTJ masing-masing.

**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.

**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 dalam rangkaian tersebut agar sentiasa berasingan.

**Intrusion Detection System (IDS)**
Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.

**Intrusion Prevention System (IPS)**
Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.

**LAN**
*Local Area Network* - Rangkaian Kawasan Setempat yang menghubungkan komputer.

**Log-on**
Masuk kepada sesuatu sistem atau aplikasi komputer.

**Malicious Software**
Perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, trojan horse, worm, spyware dan sebagainya.

**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.

**Pihak Ketiga**
Adalah selain agensi berikut; MAMPU, Kementerian Pendidikan Malaysia, Jabatan Perdana Menteri dan Kementerian Kewangan.

**Agensi Luar**
Adalah agensi berikut; MAMPU, Kementerian Pendidikan Malaysia, Jabatan Perdana Menteri dan Kementerian Kewangan.

**Public-Key Infrastructure (PKI)**
Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.

**Router**
Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya: pencapaian Internet.

**Server**
Komputer pelayan.

**Threat**
Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.

**Uninterruptible Power Supply (UPS)**
Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan daripada sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.

**Virus**
Atur cara yang bertujuan merosakkan data atau sistem aplikasi.

**Wireless**
LAN Jaringan komputer yang terhubung tanpa melalui kabel.

## 20.0 RUJUKAN


a. Dasar Keselamatan ICT, Unit Pemodenan Tadbiran Dan Perancangan Pengurusan Malaysia (MAMPU), (Versi 5.3).
b. Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.
c. Arahan Teknologi Maklumat 2007.
d. Arahan Keselamatan.(Buku – Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia).
e. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002.