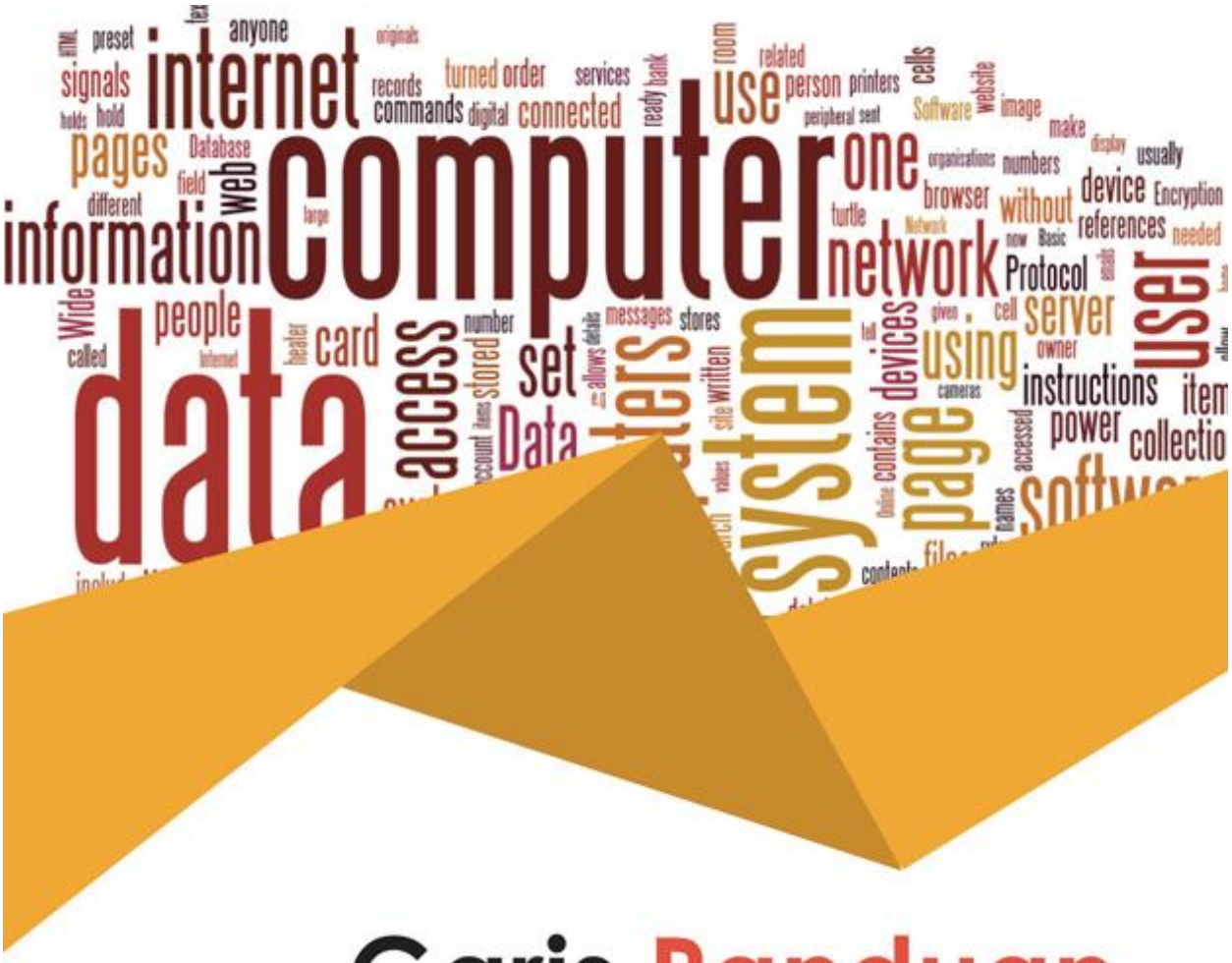

Garis Panduan

KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

(GPKTMK)

VERSI 3.0

PUSAT PEMBANGUNAN MAKLUMAT DAN KOMUNIKASI (IDEC)
UNIVERSITI PUTRA MALAYSIA

KELULUSAN

Dokumen ini merupakan Garis Panduan Keselamatan Teknologi Maklumat dan Komunikasi (GPKTMK) Universiti Putra Malaysia (UPM) Versi 3.0 yang telah diluluskan oleh Pengurusan Pusat Pembangunan Maklumat dan Komunikasi (iDEC), UPM pada 20 September 2017 untuk makluman dan kelulusan YBhg.

Disokong oleh:

.....

Rosmi bin Othman
Timbalan Pengarah Pengurusan Strategik & Sokongan Pengguna

ROSMI BIN OTHMAN
Timbalan Pengarah
Pengurusan Strategik & Sokongan Pengguna
Pusat Pemb. Maklumat & Komunikasi (iDEC)
Universiti Putra Malaysia
43400 UPM Serdang
Selangor Darul Ehsan

Diluluskan oleh:

.....

Prof. Madya Dr. Fatimah Sidi
Pengarah iDEC

PROF. MADYA DR. FATIMAH SIDI
Pengarah
Pusat Pemb. Maklumat & Komunikasi (iDEC)
Universiti Putra Malaysia
43400 UPM Serdang

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 perkhidmatan UPM dengan meminimumkan kesan insiden keselamatan ICT. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi. Garis Panduan ini bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi UPM. .

GPTMK ini digubal untuk memenuhi objektif utama Keselamatan ICT UPM iaitu :

a. Memastikan kesinambungan perkhidmatan UPM yang berasaskan ICT dan meminimumkan kerosakan atau kemusnahan.
b. Melindungi kepentingan pihak yang bergantung kepada sistem maklumat dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi.
c. Mencegah salah guna, pencerobohan atau kecurian aset ICT UPM
d. Mewajibkan pematuhan GPKTMK ke atas setiap pengguna/warga universiti yang mana sekiranya berlaku ketidakpatuhan.

3.0 PENYATAAN

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 membekal perkhidmatan yang berasaskan 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 rahsia 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 terhad kepada pengguna yang sah dan maklumat adalah dari sumber yang sah.

GPKTMK merangkumi perlindungan ke atas semua bentuk maklumat 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, tindakan ke arah menjamin KTMK hendaklah bersandarkan kepada;

a. Penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT dan ancaman yang wujud akibat daripada kelemahan tersebut.;
b. Risiko yang mungkin timbul dan tindakan pencegahan yang perlu diambil untuk menangani risiko berkenaan.

4.0 SKOP

Aset ICT UPM terdiri daripada peralatan, perisian, perkhidmatan, data atau maklumat dan manusia. Bagi memastikan keselamatan Aset ICT terjamin sepanjang masa, GPKTMK UPM ini merangkumi perlindungan semua bentuk maklumat UPM yang dimasuk, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dihantar, dan yang dibuat salinan keselamatan. Ini akan dilaksanakan 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, server, 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 (Contoh : LAN, WAN dan lain-lain).
ii. Sistem kawalan akses (Contoh: sistem kad akses).
iii. Perkhidmatan sokongan (Contoh: 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. (Contoh : 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 PELAKSANAAN PENYELENGGARAAN DAN PEMAKAIAN

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
Jawatankuasa Keselamatan Teknologi Maklumat dan Komunikasi (JKKTMK) UPM adalah bertanggungjawab memastikan GPKTMK dilaksanakan di UPM. .

b. Penyebaran
Garis panduan ini perlu disebarkan kepada semua pengguna UPM (termasuk staf, pelajar, pembekal, pakar runding dan pihak yang berkepentingan).

c. Penyelenggaraan
GPKTMK UPM adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa dari segi kawalan keselamatan, polisi, prosedur dan proses selaras dengan

perubahan teknologi, aplikasi, perundangan, dan kepentingan sosial. 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. Hebah kepada pengguna perubahan yang telah dipersetujui oleh JKKTMK; dan
iv. Semak semula Garis Panduan ini mengikut keperluan semasa (sekurang-kurangnya 1 tahun sekali).

d. Pemakaian

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 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 yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah, menghapus atau membatalkan sesuatu maklumat. Hak akses adalah dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna;

c. Akauntabiliti

Pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT;

d. Pengasingan

Tugas mewujud, memadam, mengemaskini, mengubah dan mengesah data perlu diasingkan bagi mengelakkan daripada capaian 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 keselamatan ICT atau mengenal pasti keadaan yang mengancam keselamatan ICT. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan ICT. Aset ICT seperti komputer, *server, router*, *firewall* dan rangkaian hendaklah berkebolehan untuk menjana dan menyimpan log tindakan keselamatan untuk tujuan jejak audit (*audit trail)*;

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 ketersediaan 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 bergantung antara satu sama lain. dan 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 kemungkinan risiko berlaku ke atas aset ICT akibat dari ancaman (*threat*) dan kelemahan (*vulnerability*) yang semakin meningkat hari ini. Justeru itu, UPM perlu mengambil langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenalpasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

UPM hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan tertakluk kepada perubahan teknologi dan keperluan keselamatan ICT.

Seterusnya mengambil tindakan susulan yang bersesuaian untuk mengurang atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat UPM termasuklah aplikasi, perisian, server, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber teknologi maklumat yang merangkumi pusat data, bilik media storan, kemudahan utiliti dan sistem sokongan lain.

UPM bertanggungjawab melaksanakan dan menguruskan risiko keselamatan maklumat 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 UPM;
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

Objektif :

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

6.1 STRUKTUR ORGANISASI DALAMAN

GELARAN JAWATAN	ENTITI UPM	PENERANGAN
Ketua Pegawai Teknikal (CTO)	Pengarah iDEC	Ketua bagi pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi UPM
Ketua Pegawai Operasi (COO)	Timbalan Pengarah iDEC (Pengurusan Strategik & Sokongan Pengguna)	Timbalan Ketua di pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi Universiti dan memegang portfolio pengurusan strategik dan sokongan pengguna
Pengurus Keselamatan ICT (ICTSM)	Timbalan Pengarah iDEC	Timbalan Ketua di pusat tanggungjawab yang dipertanggungkan dengan

	(Perkhidmatan ICT)	tanggungjawab hal ehwal teknologi maklumat dan komunikasi Universiti dan memegang portfolio perkhidmatan ICT.
Pegawai Keselamatan ICT (ICTSO)	Ketua Seksyen Rangkaian dan Keselamatan ICT iDEC	Ketua entiti yang dipertanggungkan dengan tanggungjawab keselamatan teknologi maklumat dan komunikasi UPM
Pentadbir Sistem ICT	Semua Ketua Bahagian, Ketua Seksyen dan Ketua Seksyen ICT (iDEC)	Ketua entiti di pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi UPM
Pengguna ICT	Warga UPM	Pengguna ICT UPM ialah individu yang menggunakan sebarang peralatan atau perisian ICT di UPM.
Pasukan Tindak Balas Insiden Keselamatan ICT UPM (UPMCERT)	**Penasihat** Pengurus Keselamatan ICT (ICTSM) **Pengerusi** Ketua Bahagian Infrastuktur ICT **Timb. Pengerusi** Ketua Bahagian Operasi Aplikasi **Ahli** 1. Pegawai Keselamatan ICT (ICTSO) 2. Pegawai Teknologi yang berkepakaran dalam bidang masing-masing	Ahli: Pegawai Teknologi Maklumat mengikut kepakaran: • Bidang Kepakaran - Keselamatan ICT) • Bidang Kepakaran - Rangkaian • Bidang Kepakaran - Pangkalan Data • Bidang Kepakaran - Aplikasi • Bidang Kepakaran - Server

6.1.1 Ketua Pegawai Teknikal (CTO)

Ketua Pegawai Teknikal (CTO) bagi UPM ialah Ketua bagi pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi UPM. Peranan dan tanggungjawab CTO adalah seperti berikut:

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

6.1.2 Ketua Pegawai Operasi (COO)

Ketua Pegawai Operasi (COO) bagi UPM ialah Timbalan Ketua di pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi Universiti dan memegang portfolio pengurusan strategik dan sokongan pengguna. Peranan dan tanggungjawab COO adalah seperti berikut:

a. Membantu CTO dalam melaksanakan tugas yang melibatkan keselamatan ICT;
b. Menyelaras keperluan keselamatan ICT yang melibatkan keseluruhan operasi ICT UPM;
c. Menyelaras penyediaan GPKTMK UPM dan pengurusan risiko serta pengauditan; dan
d. Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT.

6.1.3 Pengurus Keselamatan ICT (ICTSM)

Pengurus Keselamatan ICT (ICTSM) bagi UPM ialah Timbalan Ketua di pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi Universiti dan memegang portfolio perkhidmatan ICT. Peranan dan tanggungjawab ICTSM adalah seperti berikut:

a. Mengurus keseluruhan program keselamatan ICT UPM;
b. Menguatkuasa pelaksanaan GPKTMK UPM;
c. Memberi penerangan dan pendedahan berkenaan GPKTMK UPM kepada semua pengguna;
d. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan GPKTMK UPM;
e. Melaksanakan pengurusan risiko;
f. Melaksanakan audit, mengkaji semula, merumus tindak balas pengurusan UPM berdasarkan hasil penemuan dan menyediakan laporan mengenainya;
g. Melaporkan insiden keselamatan ICT kepada Pasukan Tindak Balas Insiden Keselamatan ICT UPM (UPMCERT) dan Ketua Pegawai Teknikal (CTO); dan
h. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah baik pulih dengan segera.

6.1.4 Pegawai Keselamatan ICT (ICTSO)

ICTSO bagi UPM ialah Ketua entiti yang dipertanggungkan dengan tanggungjawab keselamatan teknologi maklumat dan komunikasi UPM. Peranan dan tanggungjawab ICTSO adalah seperti berikut:

a. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti serangan virus dan memberi khidmat nasihat serta menyediakan kaedah perlindungan yang bersesuaian;
b. Menyedia dan melaksana program kesedaran mengenai keselamatan ICT;
c. Melapor sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSM; dan
d. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT.

6.1.5 Pentadbir Sistem ICT

Pentadbir Sistem ICT bagi UPM ialah semua Ketua entiti di pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi UPM. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut:

a. Mengambil tindakan yang sewajarnya dengan segera apabila dimaklumkan mengenai staf yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas;
b. Menentukan ketepatan dan kesempurnaan sesuatu tahap akses berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam GPKTMK UPM;
c. Memantau aktiviti akses harian sistem aplikasi pengguna;
d. Mengenal pasti aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan mengambil tindakan memberhentikannya dengan serta merta;
e. Menganalisis dan menyimpan rekod jejak audit;
f. Menyedia laporan mengenai aktiviti akses secara berkala; dan
g. Memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.

6.1.6 Pengguna

Pengguna ICT UPM ialah individu yang menggunakan sebarang peralatan atau perisian ICT di UPM. Pengguna mempunyai peranan dan tanggungjawab seperti berikut:

a. Membaca, memahami dan mematuhi GPKTMK UPM;
b. Melepasi tapisan keselamatan mengikut keperluan UPM;
c. Melaksana prinsip GPKTMK UPM dan menjaga kerahsiaan maklumat UPM;
d. Melapor sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;
e. Menghadiri program kesedaran mengenai keselamatan ICT;

f. Melaksana langkah perlindungan seperti berikut:
   i. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
   ii. memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;
   iii. menentukan maklumat sedia ada untuk digunakan;
   iv. menjaga kerahsiaan kata laluan;
   v. mematuhi standard, prosedur, arahan kerja dan garis panduan keselamatan ICT yang ditetapkan;
   vi. mematuhi peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

g. Mengawal aktiviti penggunaan media sosial seperti berikut:
   i. mengelakkan ketirisan maklumat;
   ii. mengelakkan sebarang komen/pernyataan/isu yang menyentuh perkara yang boleh menjejaskan imej UPM dan dasar kerajaan;
   iii. menghindar penyebaran maklumat yang berbentuk fitnah, hasutan dan lucah atau cuba memprovokasikan sesuatu isu yang menyalahi peraturan dan undang-undang atau perkara yang menyentuh sensitiviti individu atau kumpulan tertentu; dan
   iv. mengelak menggunakan saluran media sosial hingga mengganggu fokus dalam urusan kerja.

h. Menandatangani perjanjian sebagaimana berikut:
   i. Pelajar menandatangani surat akujanji pelajar;
   ii. Staf menandatangani surat akujanji staf; dan
   iii. Pihak ketiga menandatangani Surat Aku Janji Pihak Luar.

6.1.7 Pasukan Tindak Balas Insiden Keselamatan ICT UPM (UPMCERT)

Keanggotaan UPMCERT adalah seperti berikut:

Penasihat
Pengurus Keselamatan ICT (ICTSM)
Pengerusi
Ketua Bahagian Infrastuktur ICT

Timbalan Pengerusi
Ketua Bahagian Operasi Aplikasi

Ahli
Pegawai Keselamatan ICT (ICTSO)

Pegawai Teknologi Maklumat (Bidang Kepakaran - Keselamatan ICT)
Pegawai Teknologi Maklumat (Bidang Kepakaran - Rangkaian)
Pegawai Teknologi Maklumat (Bidang Kepakaran - Pangkalan Data)
Pegawai Teknologi Maklumat (Bidang Kepakaran - Aplikasi)
Pegawai Teknologi Maklumat (Bidang Kepakaran - Server)

Bidang Kuasa

a. Menerima dan mengesah aduan keselamatan ICT serta menilai tahap dan klasifikasi insiden;
b. Merekod dan menjalankan siasatan awal insiden yang diterima;
c. Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih;
d. Menasihat pengguna untuk mengambil tindakan pemulihan dan pengukuhan;
e. Menyebar makluman berkaitan pengukuhan keselamatan ICT kepada pengguna; dan
f. Menjalankan penilaian tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden dapat dielakkan.

6.2 PERANTI MUDAH ALIH DAN TELEWORKING

Objektif :

Memastikan keselamatan maklumat semasa menggunakan peralatan peranti mudah alih dan kemudahan teleworking.

6.2.1 Peranti Mudah Alih

Semasa menggunakan peranti mudah alih, perkara yang mesti dipatuhi bagi memastikan keselamatan maklumat adalah seperti berikut:

a. Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.
b. Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, data, pendedahan maklumat dan capaian tidak sah.
c. Perkhidmatan sokongan hendaklah terhad kepada pengguna bagi tujuan konfigurasi, tetapan dan penggunaan peralatan mudah alih bagi capaian ke sistem aplikasi yang dibenarkan untuk urusan rasmi sahaja;
d. Kata laluan hendaklah dikonfigurasi pada peranti mudah alih bagi mengelakkan akses yang tidak dibenarkan;
e. Perisian *EndPoint Protection* hendaklah dipasang pada peranti mudah alih;
f. Kehilangan peranti mudah alih hendaklah dilaporkan kepada pihak polis, Ketua PTJ dan ICTSO dalam tempoh masa 24 jam; dan

g. Kemudahan 'remote wipe' (sekiranya ada) hendaklah diaktifkan bagi memadam maklumat rasmi dari peranti mudah alih sekiranya berlaku perkara yang tidak diingini.

6.2.2 Teleworking

Kemudahan capaian sistem maklumat dan aplikasi melalui *teleworking* adalah terhad kepada perkhidmatan yang dibenarkan sahaja. Perkara yang mesti dipatuhi adalah seperti berikut :

a. *Teleworking* hendaklah melalui perantara yang dibenarkan sahaja;
b. Tindakan perlindungan hendaklah dilaksanakan bagi menghalang pendedahan maklumat dan capaian tidak sah serta penyalahgunaan;
c. Keselamatan maklumat terperingkat hendaklah terjamin semasa menjalankan *teleworking*, terutamanya yang menggunakan rangkaian awam atau komputer guna sama ditempat awam; dan
d. Capaian *teleworking* hendaklah diputuskan (*logout*) setelah selesai melaksanakan kerja.

7.0 KESELAMATAN SUMBER MANUSIA

Objektif

Memastikan semua staf UPM, pembekal, pakar runding dan pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa hendaklah dipatuhi oleh semua pihak yang terlibat .

7.1 Sebelum Perkhidmatan

Perkara yang mesti dipatuhi adalah seperti berikut:

a. Peranan dan tanggungjawab staf UPM serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan hendaklah dinyatakan dengan lengkap dan jelas;
b. Terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang ditetapkan hendaklah dipatuhi; dan
c. Penyaringan keselamatan dan/atau pengesahan latar belakang pihak yang terlibat hendaklah dilakukan berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.

7.2 Dalam Perkhidmatan

Perkara yang mesti dipatuhi adalah seperti berikut:

a. Staf UPM serta pihak ketiga yang berkepentingan hendaklah mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh UPM;
b. Latihan kesedaran mengenai pengurusan keselamatan aset ICT hendaklah diberi kepada pengguna ICT UPM secara berterusan dan kepada pihak ketiga yang berkepentingan, sekiranya perlu, dari semasa ke semasa;
c. Tindakan disiplin dan/atau undang-undang ke atas staf UPM serta pihak ketiga yang berkepentingan hendaklah diambil sekiranya berlaku pelanggaran terhadap perundangan dan peraturan yang ditetapkan oleh UPM; dan
d. Pengetahuan berkaitan dengan penggunaan aset ICT hendaklah dimantapkan bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT.

7.3 Bertukar atau Tamat Perkhidmatan

Perkara yang mesti dipatuhi adalah seperti berikut:

a. Semua aset ICT hendaklah dikembalikan kepada UPM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan
b. Semua kebenaran akses ke atas maklumat dan kemudahan proses maklumat hendaklah dibatalkan 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

Semua aset ICT hendaklah diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang mesti dipatuhi adalah seperti berikut:

i. Semua aset ICT hendaklah dikenal pasti, maklumat aset direkod dalam sistem pengurusan aset dan sentiasa dikemaskini;
ii. Semua aset ICT hendaklah didaftarkan pemiliknya dan dikendalikan oleh pengguna yang dibenarkan sahaja;
iii. Semua pengguna hendaklah mengesahkan penempatan aset ICT sama ada di dalam atau di luar UPM mengikut peraturan yang telah ditetapkan;
iv. Peraturan pengendalian aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan; dan

v. Pengguna hendaklah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.

8.2 Pengkelasan dan Pengendalian Maklumat

Objektif
Memastikan setiap maklumat diberikan tahap perlindungan yang bersesuaian.

a. Pengkelasan 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 Sulit
iii. 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 atau 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 fail 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 mesti dipatuhi adalah seperti berikut:

i. Melabel semua media mengikut tahap klasifikasi sesuatu maklumat;
ii. Menghad dan menentukan akses media kepada pengguna yang dibenarkan sahaja;
iii. Menghad pengedaran data atau media untuk tujuan yang dibenarkan sahaja;
iv. Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan atau pendedahan yang tidak dibenarkan;
v. Menyimpan semua media di tempat yang selamat; dan
vi. Memastikan 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, direkod dan dikemaskini 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. Bercuti panjang dalam tempoh waktu melebihi tiga (3) bulan;
ii. Bertukar bidang tugas serta skop kerja;
iii. Bertukar ke agensi lain;

b. Bersara atau ditamatkan perkhidmatan

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

c. Kata Laluan

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

d. Pengurusan Kata Laluan

Pengurusan kata laluan hendaklah 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. kemudahan *password screen saver* atau *logout* hendaklah diamalkan apabila meninggalkan komputer;
ii. bahan sensitif hendaklah disimpan di dalam laci atau kabinet fail yang berkunci; dan

iii. semua dokumen hendaklah 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 hendaklah dikawal mengikut prosedur pemantauan akses.

b. **Pengenalan dan Pengesahan Pengguna**

Setiap pengguna hendaklah diberi pengenalan diri (ID) yang unik.

c. Penggunaan *System Tools*

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

d. **Session *Time-out***

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

e. Had Masa Akses

Had masa akses hendaklah 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 hendaklah mematuhi prosedur yang telah ditetapkan;
ii. Kod sumber atau atur cara sistem yang telah dikemaskini hanya boleh digunakan selepas diuji; dan
iii. Akses ke atas kod sumber atau atur cara sistem hendaklah dikawal.

10.0 KRIPTOGRAFI

Objektif
Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui 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
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. Keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) hendaklah digunakan untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;
v. Semua pintu di kawasan keselamatan fizikal hendaklah dipasang dengan alat penggera, dipantau dan diuji supaya mematuhi piawaian yang ditetapkan; dan
vi. Sistem pencegahan pencerobohan yang sesuai hendaklah dipasang dalam kawasan keselamatan fizikal.

b. Kawalan Akses Fizikal

Mengawal akses secara fizikal terhadap premis UPM. Kawalan akses merupakan aktiviti utama dalam aspek keselamatan maklumat. Kawalan akses 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

Memastikan keselamatan fizikal pejabat, bilik dan kemudahan sentiasa terjamin. Perkara yang mesti dipatuhi adalah seperti berikut:

i. Kemudahan utama hendaklah diasingkan daripada akses umum;
ii. Papan tanda dan maklumat mengenai fungsi bangunan tidak didedahkan pada umum;
iii. Kemudahan hendaklah dikonfigurasi supaya aktiviti atau maklumat sulit tidak dilihat atau didengar dari luar. Perlindungan elektromagnetik juga hendaklah dititik beratkan; dan
iv. Buku panduan dan buku telefon dalaman yang mengandungi kemudahan pemprosesan maklumat yang sulit hendaklah dikawal daripada akses pihak yang tidak dibenarkan.

e. Kawalan Persekitaran

Bagi menghindarkan kerosakan dan gangguan terhadap premis ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa ataumengubahsuai, hendaklah dirujuk terlebih dahulu kepada pihak Pejabat Keselamatan dan Kesihatan Pekerjaan; dan Pejabat Pembangunan dan Pengurusan Aset di UPM Perkara yang mesti dipatuhi adalah seperti berikut:

i. Pelan keseluruhan susun atur Pusat Data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) hendaklah dirancang dan disediakan 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. Peralatan elektrik yang tidak berkaitan hendaklah dielak penggunaannya;
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. Kewujudan kawasan keselamatan dan aktivitinya hendaklah diketahui oleh semua staf;

ii. Pelaksanaan aktiviti tanpa penyeliaan hendaklah dielak bagi tujuan keselamatan dan bagi mencegah sebarang peluang pencerobohan;
iii. Kawasan keselamatan yang tidak digunakan hendaklah 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 hendaklah 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 bahan bahaya yang lain sebelum dialih ke kawasan penghantaran dan pemunggahan;
v. Bahan yang diterima hendaklah didaftarkan mengikut prosedur pengurusan aset;
vi. Penghantaran masuk dan keluar hendaklah diasingkan jika boleh; dan
vii. Bahan yang diterima hendaklah diperiksa untuk mengesan sebarang *tampering* sewaktu proses penghantaran dan jika didapati ada unsur *tampering*, laporan kepada pihak keselamatan hendaklah 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 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 hendaklah disediakan.

i) Keselamatan Kabel

Kabel letrik dan rangkaian hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah atau mengalami kerosakan.

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Kabel letrik dan kabel rangkaian hendaklah menepati Sistem Pengkabelan Berstruktur (Structured Cabling System) dan spesifikasi yang telah ditetapkan;
ii. Kabel letrik dan rangkaian hendaklah dilindungi daripada kerosakan yang disengajakan atau tidak disengajakan;
iii. Kabel letrik dan kabel rangkaian hendaklah diasingkan untuk mengelakkan gangguan;

iv. kabel rangkaian hendaklah dilabelkan dengan jelas dan hendaklah 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 difail dan dilabel mengikut klasifikasi keselamatan;
ii. Pergerakan fail dan dokumen hendaklah direkod 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 hendaklah bertanggungjawab sepenuhnya ke atas peralatan ICT dengan memastikan peralatan ICT yang berkaitan dilengkapi dengan antivirus dan laksana imbasan secara berkala masing-masing dan digunakan sepenuhnya bagi urusan rasmi sahaja;
ii. Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna;

iii. Pengguna hendaklah 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 pentadbir (*administrator password*) peralatan yang telah ditetapkan; dan
vii. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO.

b. Media Storan Mudah Alih

Media storan merupakan perkakasan 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 ketersediaan 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 hendaklah 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 yang mengandungi data hendaklah dilupuskan dengan teratur dan selamat; dan
vii. Penghapusan maklumat atau kandungan media hendaklah 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 hendaklah dikawal supaya tidak 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. Pengguna hendaklah menggunakan hanya perisian yang diperakui bagi kegunaan UPM;
ii. Sistem aplikasi dalaman hendaklah dikawal supaya ianya tidak didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurusan UPM;
iii. Lesen perisian (Kod Pendaftaran, nombor siri, *CD-keys*) hendaklah 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 hendaklah 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 hanyhendaklah diselenggara oleh staf UPM atau pihak ketiga yang dibenarkan sahaja;
iii. Staf hendaklah bertanggungjawab terhadap setiap peralatan bagi penyelenggaraan peralatan sama ada dalam tempoh jaminan atau telah tamat tempoh jaminan;
iv. Semua peralatan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan;
v. Pengguna hendaklah dimaklumkan sebelum penyelenggaraan dilaksanakan 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 terhadap peralatan hendaklah dibuat apabila peralatan dikembalikan ke dalam premis;
iv. Rekod keluar masuk peralatan hendaklah disimpan;
v. Peralatan hendaklah sentiasa dilindungi dan dikawal;
vi. Penyimpanan atau penempatan peralatan di luar premis hendaklah mengambil kira ciri-ciri keselamatan yang bersesuaian dan menilai risiko 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 dilupuskan hendaklah melalui prosedur pelupusan semasa. Pelupusan hendaklah 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 sepenuhnya dengan cara yang selamat sebelum sesuatu peralatan ICT dilupuskan atau dipindah milik;
ii. Sekiranya maklumat perlu disimpan, pengguna hendaklah membuat penduaan mengikut kaedah yang ditetapkan;
iii. Peralatan yang akan 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

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Semua peralatan yang ditinggalkan dalam apa jua bentuk media hendaklah dikawal / dipastikan keselamatannya.
ii. 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.
iii. Kemudahan *password screen saver* atau *logout* hendaklah digunakan apabila meninggalkan peralatan komputer;
iv. Bahan sensitif hendaklah disimpan di dalam laci atau kabinet fail yang berkunci ; dan
v. Semua dokumen hendaklah 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 hendaklah disimpan dengan selamat bila tidak digunakan;
ii. Komputer dan terminal hendaklah di *logoff,* dipasang *screen saver* atau mekanisme mengunci papan kekunci digunakan; dan
iii. Peralatan pencetak, mesin fotostat atau alat penyalin hendaklah dikawal penggunaannya

12.0 PENGURUSAN OPERASI KESELAMATAN

12.1 Prosedur Operasi

Objektif

Memastikan-engurusan 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 hendaklah 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 hendaklah 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 hendaklah diasingkan bagi mengurangkan peluang 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 operasi.

d) Pengurusan Kapasiti

Pengurusan kapasiti hendaklah dilaksanakan dalam pengurusan ICT Universiti dengan merancang kapasiti bagi sesuatu pembangunan atau penaiktarafan infrastruktur dan infostruktur.

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Perancangan kapasiti hendaklah dibuat sebelum sesuatu pembangunan ICT dilaksanakan bagi mengoptimumkan keupayaan sesuatu infrastruktur ICT; dan
ii. Pengawalan penggunaan sumber hendaklah 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. sistem keselamatan seperti *Anti Virus, Intrusion Detection System (IDS)* dan *Intrusion Prevention System (IPS)* hendaklah dipasang untuk mengesan perisian atau fail berbahaya;
ii. perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa hendaklah dipasang dan digunakan;
iii. Pengguna hendaklah mengimbas perisian atau sistem dengan anti virus sebelum menggunakannya;
iv. Pengguna hendaklah memastikan antivirus dikemaskini dengan patch terkini;
v. Pengguna hendaklah menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;
vi. pengguna hendaklah mempunyai pengetahuan mengenai ancaman perisian berbahaya dan cara mengendalikannya;

vii. klausa liabiliti hendaklah dimasukkan di dalam kontrak yang akan ditawarkan kepada pihak ketiga. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;
viii. Ancaman keselamatan ICT seperti serangan virus hendaklah dihebahkan kepada pengguna; dan
ix. Akses kepada laman web yang disenarai hitamkan atau dikenal pasti merbahaya hendaklah disekat.

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. Perisian *antivirus hendaklah* sentiasa dikemaskini;
ii. Tetapan pelayar hendaklah diubah untuk menyekat aplikasi interaktif seperti *JavaScrip*t daripada beroperasi secara automatik; dan
iii. *Patches* pelayar hendaklah sentiasa dikemaskini.

12.3 Penyelenggaraan Maklumat

Objektif

Memastikan Integriti maklumat terjamin dan maklumat boleh diakses apabila diperlukan.

a) *Backup*

Backup hendaklah dilakukan bagi memastikan sistem dapat digunakan semula sekiranya berlaku bencana. Perkara yang mesti dipatuhi adalah seperti berikut:

i. *Backup* keselamatan hendaklah dibuat ke atas semua sistem perisian dan aplikasi secara berkala atau apabila terdapat perubahan versi;
ii. *Backup* hendaklah dibuat ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat;
iii. Sistem *backup* dan *restore* sedia ada hendaklah diuji bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan;
iv. Backup hendaklah disimpan sekurang-kurangnya setahun ataupun mengikut keperluan sistem;
v. Salinan *backup* hendaklah direkod dan disimpan di lokasi yang berlainan dan selamat;
vi. *Backup* hendaklah dilaksanakan selepas waktu pejabat untuk mengurangkan beban kepada infrastruktur ICT pada waktu puncak; dan
vii. *Backup Tools* hendaklah disimpan oleh staf ICT yang ditugaskan sahaja dan digunakan dengan kawalan dan kebenaran penyelia staf ICT tersebut.

b) *Housekeeping*

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

i. Perisian dan sistem aplikasi hendaklah dikemaskini; dan
ii. Fail sistem dan storan hendaklah diuruskan seperti pembersihan log dan fail sementara (*temporary file*).

12.4 *Logging* dan Pemantauan

Objektif
Memastikan ktiviti pemprosesan maklumat direkodkan dan bukti aktiviti dapat diberikan jika diperlukan.

a) *Event Logging*

i. Sistem log hendaklah diwujudkan bagi merekodkan semua aktiviti harian pengguna (bebas ralat) dan maklumat keselamatan aktiviti; dan
ii. Sistem log hendaklah disemak secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaikpulih dengan segera.

Log aktiviti mesti mengandungi maklumat berikut:

i. Rekod setiap aktiviti transaksi;
ii. 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. Aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.

b) Perlindungan Maklumat Log

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

c) Pentadbir dan Operator Log

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

d) Pelarasan Masa

Masa sistem pengoperasian hendaklah diselaraskan dengan satu masa rujukan (time.upm.edu.my) yang telah ditetapkan.

12.5 Kawalan Ke atas Perisian Pengoperasian

Objektif
Memastikan integriti bagi sistem pengoperasian.

a) Instalasi Perisian Sistem Pengoperasian.

Kawalan hendaklah dilaksanakan bagi pemasangan perisian ke atas sistem pengoperasian. Perkara yang mesti dipatuhi adalah seperti berikut:

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

i. maklumat kerentanan teknikal yang tepat pada masanya terhadap sistem maklumat yang digunakan hendaklah diperolehi;
ii. Tahap pendedahan hendaklah dinilai bagi mengenal pasti risiko yang bakal dihadapi; dan
iii. Langkah-langkah kawalan hendaklah diambil untuk mengatasi risiko berkaitan.

b) Mengehadkan Instalasi Perisian

Peraturan instalasi perisian oleh pengguna hendaklah diwujudkan dan dilaksanakan.

Organisasi hendaklah 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.

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 hendaklah dilarang menggunakan perisian *sniffer* atau *network analyzer* kecuali mendapat kebenaran pentadbir sistem rangkaian;
iv. *Intrusion Prevention System (IPS)* hendaklah dipasang bagi mengesan sebarang cubaan menceroboh dan aktiviti lain yang boleh mengancam sistem dan maklumat UPM;
v. *Web Content Filtering* hendaklah dipasang pada *Internet Gateway* untuk menyekat aktiviti yang dilarang;
vi. Sebarang penyambungan rangkaian tanpa kelulusan hendaklah tidak dibenarkan;
vii. Sistem intranet UPM hendaklah terhad akses 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 hendaklah 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 hendaklah terhad kepada capaian perkhidmatan rangkaian yang dibenarkan sahaja.

b) Akses Pengguna daripada Rangkaian Luar

Kaedah akses yang bersesuaian hendaklah digunakan untuk mengawal akses dari rangkaian luar.

c) Pengenalpastian Peralatan

Pengenalpastian peralatan secara automatik hendaklah ada bertujuan untuk spesifikasi lokasi dan peralatan yang disahkan.

d) Akses Internet

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

Perkara yang mesti dipatuhi adalah seperti berikut:

i. Kaedah *Content Filtering* hendaklah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan;
ii. Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) hendaklah diamalkan bagi menguruskan penggunaan jalur lebar (bandwidth) yang maksimum dan lebih berkesan;
iii. Penggunaan Internet hendaklah terhad untuk kegunaan rasmi sahaja. Pentadbir Sistem ICT berhak menentukan pengguna yang dibenarkan menggunakanInternet atau sebaliknya;
iv. Laman yang dilayari hendaklah yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Pentadbir Sistem ICT yang diberi kuasa;
v. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan;
vi. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada pegawai yang bertanggungjawab sebelum dimuat naik ke Internet;
vii. Pengguna hendaklah dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;
viii. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh UPM;

ix. Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; dan
x. Pengguna hendaklah 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 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. Subjek dan kandungan e-mel hendaklah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;
iv. e-mel rasmi hendaklah dihantar 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 hendaklah 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 hendaklah meliputi pengesahan identiti pengguna dan pengujian ke atas *input*, pemprosesan dan *output* sistem bagi memastikan keselamatan dan integriti data;
iii. Aplikasi ~~perlu~~ hendaklah 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 hendaklah 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 hendaklah disemak kesahihannya bagi memastikan data yang dimasukkan betul dan sesuai; dan
ii. Data *output* daripada aplikasi hendaklah 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 hendaklah sah dan disahkan;
ii. Tahap kerahsiaan, integriti dan kesediaan sesuatu transaksi hendaklah dikekalkan;
iii. Privasi yang berkaitan dengan semua pihak yang terlibat hendaklah dikekalkan;
iv. Laluan dan protokol komunikasi hendaklah selamat; dan
v. Data dan maklumat hendaklah 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 hendaklah dikemukakan oleh pemilik sistem dan perubahan dilakukan hendaklah mematuhi tahap kawalan dan integriti tertentu;
iii. Dokumen kawalan versi sistem dan kod sumber hendaklah dikemaskini jika terdapat perubahan;

iv. Dokumentasi sistem, dokumentasi operasi dan panduan pengguna hendaklah dikemaskini secara berterusan mengikut perubahan sistem;
v. Sebarang perubahan platform/sistem pengoperasian terhadap aplikasi kritikal, kajian dan ujian terperinci hendaklah 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. Penyampaian perkhidmatan sistem maklumat hendaklah dipantau secara berterusan; dan
ii. Sebarang aktiviti seperti pencerobohan, pecah kontrak, pendedahan dan pengubahsuaian maklumat yang tidak dibenarkan hendaklah dicegah dan dihalang.

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. Sensitiviti data untuk diproses, disimpan dan dihantar oleh sistem hendaklah dijaga serta dikawal pergerakan datanya;
ii. Kebolehpercayaan kakitangan yang bekerja di persekitaran hendaklah dipantau;
iii. Kawalan keselamatan hendaklah 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 hendaklah 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 hendaklah dijalankan yang merangkumi pengujian keperluan keselamatan maklumat dan kepatuhan kepada amalan pembangunan sistem yang selamat. Pengujian yang dijalankan hendaklah dijalankan di persekitaran sebenar bagi memastikan sistem tersebut selamat daripada sebarang ancaman; dan

iii. Semua data pengujian yang digunakan hendaklah 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 hendaklah diselia dan dipantau pada setiap peringkat pembangunan;

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

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

iv. Latihan kesedaran (*awareness training*) hendaklah 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 hendaklah dilaksanakan bagi memastikan perkara berikut:

   i. gangguan kepada sistem yang sedia ada hendaklah dikurangkan; dan
   ii. sebarang impak negatif terhadap perkhidmatan Universiti hendaklah diminimakan.

b) Keperluan Keselamatan Infrastruktur semasa Pembangunan Infrastruktur ICT.

Perkara yang mesti dipatuhi adalah seperti berikut:

   i. akses sistem hendaklah terkawal; dan
   ii. integriti dan keselamatan data yang dipindahkan hendaklah terjamin.

c) Keperluan Keselamatan Infrastruktur selepas Pembangunan Infrastruktur ICT. Perkara yang mesti dipatuhi adalah seperti berikut:

   i. pengujian Infrastruktur baharu hendaklahmematuhi keperluan; dan
   ii. dokumentasi penyerahan hendaklah 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

memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal.

Perkara yang mesti dipatuhi adalah seperti berikut:

i. pihak ketiga hendaklah membaca, memahami dan mematuhi GPKTMK UPM;
ii. keperluan keselamatan hendaklah dikenalpasti sebelum memberi kebenaran akses atau penggunaan kepada pihak ketiga;
iii. risiko keselamatan maklumat dan kemudahan pemprosesan maklumat hendaklah dikenalpasti serta kawalan yang sesuai hendaklah dilaksanakan sebelum memberi kebenaran akses;
iv. akses kepada aset ICT UPM hendaklah berlandaskan kepada perjanjian kontrak;
v. semua syarat keselamatan hendaklah 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. Surat Aku Janji Pihak Luar

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. kawalan keselamatan, skop perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian hendaklah 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 hendaklah 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 oleh 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 hendaklah 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 diselenggara.

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

i. jejak audit dan *backup* secara berkala hendaklah disimpan dan integriti semua bahan bukti hendaklah dilindungi;
ii. bahan bukti hendaklah disalin dan semua maklumat aktiviti hendaklah direkodkan;
iii. pelan kontingensi hendaklah disediakan dan pelan kesinambungan perkhidmatan hendaklah diaktifkan;
iv. tindakan pemulihan segera hendaklah disediakan; dan
v. pihak berkuasa perundangan hendaklah dimaklumkan dan nasihat didapatkan 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. semua tanggungjawab dan prosedur kecemasan atau pemulihan hendaklah dikenalpasti;
ii. kebarangkalian dan impak yang boleh mengakibatkan gangguan terhadap perkhidmatan serta keselamatan ICT hendaklah dikenalpasti;
iii. prosedur kecemasan agar pemulihan dapat dilakukan dengan segera hendaklah dilaksanakan;
iv. dokumentasi proses dan prosedur hendaklah diurus secara berpusat;
v. program latihan prosedur kecemasan kepada pegawai yang bertanggungjawab dan berkaitan hendaklah dijalankan;
vi. *backup* hendaklah disediakan; dan
vii. pelan PKP hendaklah diuji dan disemak dari semasa ke semasa atau mengikut keperluan.

Pelan PKP hendaklah dibangunkan dan mengandungi perkara berikut:

1) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;
2) 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 hendaklah disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama.
ii. Pelan PKP hendaklah diuji sekurang-kurangnya sekali setahun dan apabila terdapat perubahan dalam persekitaran atau fungsi perkhidmatan untuk memastikan ia sentiasa kekal berkesan;

iii. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan; dan
iv. 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 hendaklah 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 hendaklah diperiksa secara berkala bagi mematuhi piawaian pelaksanaan keselamatan ICT.

c. Pematuhan Keperluan Audit Keselamatan Sistem Maklumat

Perkara yang mesti dipatuhi keperluan audit bertujuan meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit hendaklah dipatuhi;

i. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi hendaklah dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan; dan
ii. peralatan audit hendaklah dijaga dan diselia penggunaannya 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.

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.