Kandungan

GARIS PANDUAN KESELAMATAN DAN ETIKA PENGGUNA ICT

1.0 Tujuan

Garis Panduan Keselamatan Dan Etika Pengguna ICT diwujudkan untuk menjamin kesinambungan urusan Universiti dengan meminimumkan kesan insiden keselamatan ICT dengan mematuhi keperluan piawai ISO/IEC 27001:2013 Sistem Pengurusan Keselamatan Maklumat (Information Security Management Systems, ISMS). Polisi ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi Universiti.

2.0 Dokumen Rujukan

Antara dokumen yang berkaitan adalah:

1. MS ISO/IEC 27001:2013 Information Technology Security Techniques-Information Security Management Systems-Requirements;

2. Surat Arahan Ketua Pengarah MAMPU bertarikh 24 November 2010:
   Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam;

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

4. MS ISO/IEC 27002:2013 Code of Practise-Information Techniques –Security Techniques-Code of Practice for Information Security Management System;

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

6. Pekeliling Am Bilangan 3 Tahun 2000: Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan.

3.0 Definisi

BIL.	ISTILAH	MAKSUD
1.	Aset	Bermaksud semua aset ICT terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia yang mempunyai nilai kepada agensi.
2.	Ancaman	Bermaksud apa sahaja kejadian yang berpotensi atau tindakan yang boleh menyebabkan berlaku kemusnahan atau musibah.
3.	Garis Panduan Keselamatan Dan Etika Pengguna ICT	Bermaksud dokumen yang mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT). Dasar hendaklah juga menerangkan kepada semua pengguna mengenai peranan dan tanggungjawab dalam melindungi aset ICT.
4.	Integriti	Bermaksud data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan.

5.	Insiden keselamatan	Bermaksud musibah yang berlaku ke atas sistem maklumat dan komunikasi (ICT) atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar Garis Panduan Keselamatan Dan Etika Pengguna ICT samada yang ditetapkan secara tersurat atau tersirat.
6.	Kerahsiaan	Bermaksud maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran.
7.	Kebolehsediaan	Bermaksud data dan maklumat hendaklah boleh diakses pada bila-bila masa.
8.	Kawalan	Bermaksud langkah-langkah pengukuhan yang diguna pakai untuk mengurus risiko.
9.	Keselamatan maklumat	Bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan.
10.	Kawalan Rekod	Bermaksud peraturan bagi memastikan rekod sentiasa diselenggara dan disimpan dengan teratur supaya mudah dikesan apabila diperlukan untuk rujukan.
11.	Keterdedahan (vulnerability)	Bermaksud sebarang kelemahan pada aset atau sekumpulan aset yang boleh dieksploitasi oleh ancaman.
12.	Kajian Semula	Bermaksud langkah-langkah untuk mengendalikan kajian semula ke atas pengurusan keselamatan maklumat bagi menilai keberkesanannya serta peluang penambahbaikan secara berterusan.
13.	Pengurusan Sistem Keselamatan Maklumat	Bermaksud perkara-perkara yang perlu diberikan tumpuan untuk mewujud, melaksana, memantau, menyemak, menyelenggara dan menambah baik keselamatan maklumat.
14.	Pelan Penguraian Risiko (Risk Treatment Plan-RTP)	Bermaksud strategi untuk menangani risiko keselamatan ICT.

15.	Proses	Bermaksud proses yang mengguna pakai model Plan-Do-Check-Act (PDCA). Setiap proses hendaklah dirancang (Plan); dilaksana dan diselenggara (Do); dipantau, dinilai dan dikaji semula (Check) dan ditambah baik (Act).
16.	Prosedur	Bermaksud peranan dan tanggungjawab serta langkah-langkah yang perlu dilaksanakan dalam sesuatu proses atau aktiviti.
17.	Penilaian Risiko	Bermaksud penilaian ke atas kemungkinan berlakunya bahaya atau kerosakan atau kehilangan aset.
18.	Penyataan Pemakaian (Statement of Applicability-SoA)	Bermaksud menyenaraikan justifikasi pemilihan kawalan, Annex dalam MS ISO/IEC 27001:2013 dan sebarang rujukan dalam melindungi keselamatan aset ICT.
19.	Rekod	Bermaksud data/maklumat yang bertulis/elektronik hasil daripada aktiviti ISMS sebagai bukti pelaksanaan.
20.	Risiko	Bermaksud kemungkinan yang boleh menyebabkan bahaya, kerosakan dan keraguan.
21.	Tindakan Pembetulan	Bermaksud tindakan segera bagi mengelak kejadian berulang yang boleh menjejaskan sistem keselamatan maklumat.
22.	Tindakan Pencegahan	Bermaksud tumpuan untuk menghapuskan sebab-sebab sesuatu kesilapan mungkin berlaku supaya ianya tidak akan berlaku.

4.0 Prinsip-Prinsip Pengurusan Sistem Keselamatan Maklumat

Prinsip-prinsip asas standard ISO/IEC 27001:2013 adalah untuk melindungi kerahsiaan, integriti dan kebolehsediaan maklumat. Prinsip ini bermaksud:

1. maklumat hendaklah dilindungi dari pihak lain yang tidak diberi kuasa menggunakan maklumat;
2. maklumat hendaklah sentiasa tepat, lengkap dan kemaskini semasa ianya diproses; dan
3. maklumat hendaklah sentiasa tersedia jika diperlukan oleh pihak lain yang diberi kuasa mencapai maklumat tersebut.

5.0 Penyataan Garis Panduan Keselamatan dan Etika Pengguna ICT

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

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

1. Melindungi maklumat rahsia rasmi dan maklumat rasmi Kerajaan dari capaian tanpa kuasa yang sah;
2. Menjamin setiap maklumat adalah tepat dan sempurna;
3. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
4. Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

Garis Panduan Keselamatan Dan Etika Pengguna ICT UTHM merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri- ciri utama keselamatan maklumat adalah seperti berikut:

1. Kerahsiaan — Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;

2. Integriti—Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;
3. Tidak Boleh Disangkal—Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;
4. Kesahihan—Data dan maklumat hendaklah dijamin kesahihannya; dan
5. Ketersediaan—Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

6.0 Keselamatan Sumber Manusia

6.1 Sebelum diterima Berkhidmat/Belajar

6.1.1 Penyaringan

1. Menyatakan dengan lengkap dan jelas tentang peranan dan tanggungjawab setiap pengguna, pembekal, perunding dan pihak-pihak lain yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan
2. Menjalankan tapisan keselamatan untuk setiap pengguna, pembekal, perunding dan pihak-pihak lain yang terlibat selaras dengan keperluan perkhidmatan.

6.1.2 Terma dan Syarat Perkhidmatan

1. Semua warga UTHM yang dilantik, pelajar dan pihak ketiga hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan serta peraturan semasa yang berkuat kuasa; dan
2. Warga UTHM yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972.

6.2 Semasa Berkhidmat/Belajar

6.2.1 Tanggungjawab Pengurusan

1. Memastikan staf UTHM serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh UTHM.
2. Ketua Jabatan perlu memastikan setiap staf menandatangani Surat Akuan Pematuhan Polisi ICT UTHM.

6.2.2 Kesedaran, Pendidikan dan Latihan Berkaitan Keselamatan ICT

1. Setiap warga UTHM perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT secara berterusan dalam melaksanakan tugas dan tanggungjawabnya. Program latihan akan melibatkan semua pegawai UTHM dan dilaksanakan secara berterusan.
2. Laman Intranet akan dijadikan sebagai medium penyebaran maklumat berkaitan keselamatan ICT bagi meningkatkan tahap kesedaran pegawai UTHM berkaitan kepentingan keselamatan ICT.
3. Pegawai teknikal yang dipertanggungjawabkan menjaga keselamatan sumber ICT di mana ianya menyediakan perkhidmatan berpusat kepada pengguna (seperti server, *storage*, *firewall*, *router*, *antivirus* berpusat dan lain-lain) akan dipastikan menjalani latihan yang spesifik berkaitan bidang tugas mengikut spesifikasi model yang digunakan.

6.2.3 Proses Tatatertib

Pelanggaran Dasar Keselamatan ICT UTHM akan dikenakan tindakan mengikut peraturan semasa.

6.3 Penamatan dan Perubahan Perkhidmatan/Belajar

6.3.1 Penamatan dan Perubahan Perkhidmatan/Belajar

1. Peraturan yang berkaitan dengan pertukaran perkhidmatan/belajar atau tamat perkhidmatan/belajar perlu ditakrifkan dengan jelas.
2. Perkara-perkara yang perlu dipatuhi termasuk yang berikut:
   a. Memastikan semua aset ICT dikembalikan kepada UTHM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan
   b. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh UTHM dan/atau terma perkhidmatan.

7.0 Klasifikasi Maklumat

7.1 Klasifikasi Maklumat

1. Memastikan setiap maklumat diberi perlindungan yang bersesuaian berdasarkan kepada tahap klasifikasi masing-masing.
2. Maklumat hendaklah dikelaskan dan dilabelkan dengan betul berdasarkan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal kepada kerajaan.
3. Setiap maklumat yang dikelaskan sebagai Rahsia Besar, Rahsia, Sulit dan Terhad mestilah diuruskan mengikut peringkat keselamatan seperti dinyatakan dalam dokumen Arahan Keselamatan.

7.1.1 Pelabelan Maklumat

1. Pelabelan maklumat perlu dilakukan bagi maklumat dalam bentuk elektronik dan salinan keras.
2. Fail elektronik perlu dilabelkan mengikut klasifikasi dokumen yang berkenaan.
3. Dokumen dalam bentuk salinan keras, perlu dilabelkan mengikut arahan yang telah dikeluarkan dalam Arahan Keselamatan, di Bab Keselamatan Dokumen, Seksyen III: Tanda Keselamatan.

7.1.2 Pengendalian Aset

1. Pengendalian maklumat seperti pewujudan, pengumpulan, pemprosesan, penyimpanan, penyalinan, penghantaran, penyampaian, penukaran dan pemusnahan hendaklah mengambil kira langkah-langkah keselamatan berikut:

   a. Penyimpanan Maklumat

   Penyimpanan dokumen yang telah diklasifikasikan mesti mengikut Arahan Keselamatan, di Bab Keselamatan Dokumen, Seksyen IV: Penyimpanan Perkara-perkara Terperingkat.

   b. Penghantaran Maklumat

   Penghantaran dokumen yang telah diklasifikasikan mesti mengikut Arahan Keselamatan, di Bab Keselamatan Dokumen:

   i. Seksyen V: Penghantaran Dokumen Terperingkat
   ii. Seksyen VI: Membawa Dokumen Terperingkat Keluar Pejabat
   iii. Seksyen VII: Pelepasan Perkara Terperingkat

   c. Pelupusan Maklumat

   Pelupusan dokumen yang telah diklasifikasikan mesti mengikut Arahan Keselamatan, di Bab Keselamatan Dokumen, Seksyen VIII: Pemusnahan Dokumen Terperingkat.

2. Keselamatan dokumen adalah bagi memastikan integriti maklumat. Langkah-langkah berikut hendaklah dipatuhi:
   a. Memastikan sistem dokumentasi dan penyimpanan maklumat adalah selamat dan terjamin. Dokumen tidak boleh

ditinggalkan terdedah, ditinggalkan di tempat yang mudah dicapai atau ditinggalkan tanpa kawalan;

b. Penyimpanan dilakukan di dalam laci atau kabinet yang berkunci bagi maklumat yang terperingkat;
c. Memastikan dokumen yang mengandungi maklumat sensitif diambil segera dari pencetak;
d. Menggunakan kata laluan atau *encryption* dalam penyediaan dan penghantaran dokumen sensitif;
e. Menggunakan kemudahan log keluar atau kata laluan *screen saver* apabila meninggalkan komputer; dan
f. Salinan cetakan yang mengandungi maklumat penting atau rahsia hendaklah dihapuskan dengan menggunakan kaedah yang sesuai seperti menggunakan mesin pencincang.

7.2 Pengendalian Media

7.2.1 Keselamatan Perisian Bahagian Luaran

1. Perlu menyediakan *backup system* yang baik bagi menjamin data penting universiti disimpan dengan selamat.
2. *Backup tape* perlu disimpan dalam ruang yang selamat daripada bencana kebakaran.
3. *External storage* untuk perisian yang asal perlu disimpan ditempat yang selamat.
4. *Backup* perlu dilakukan secara berjadual.
5. Perisian yang ada perlu dipastikan mempunyai kawalan capaian perisian yang sesuai bagi mengelakkan data/maklumat daripada terpadam.
6. Setiap perisian perlu mempunyai lesen perisian yang sah dari segi undang-undang.

7. Setiap perisian perlu ada perisian *backup* sebagai keselamatan data/maklumat.
8. Setiap perisian yang menggunakan konsep *client- server* perlu di selia bersama Pusat Teknologi Maklumat.
9. Satu salinan manual dan manual konfigurasi perlu disimpan di perpustakaan.

7.2.2 Pengurusan Media Boleh Alih

1. Media storan merupakan tempat penyimpanan maklumat seperti USB drive, disket, CD, DVD, pita, *external hard disk* dan sebagainya.

2. Langkah keselamatan adalah bagi mengelak maklumat atau data menjadi rosak (*corrupted*) atau tidak boleh dibaca. Langkah keselamatan yang perlu diambil ialah seperti berikut:

   a. Dilarang meninggalkan, memberi atau menyerahkan media storan yang mengandungi maklumat penting kepada orang lain bagi mengelakkan berlakunya pembocoran rahsia;

   b. Menyediakan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan seperti kabinet berkunci;

   c. Akses untuk memasuki kawasan penyimpanan media hendaklah dihadkan kepada pegawai yang bertanggungjawab atau pengguna yang dibenarkan sahaja; dan

   d. Media storan yang digunakan hendaklah bebas daripada serangan virus yang boleh mengganggu ketidakstabilan sistem komputer dan rangkaian. Gunakan perisian antivirus untuk mengimbas media storan sebelum menggunakannya.

3. Perkara-perkara yang perlu dipatuhi di dalam pengurusan pengendalian media adalah seperti berikut:

a. Melabelkan semua media;

b. Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja;

c. Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;

d. Mengawal dan merekodkan aktiviti penyenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan

e. Menyimpan semua media di tempat yang selamat.

7.2.3 Pelupusan Media

1. Proses penghapusan kandungan media storan perlu dirujuk di dalam prosedur yang telah ditetapkan.
2. Pelupusan media komputer hendaklah dipastikan data-data di dalam media tersebut perlu dihapuskan.

7.2.4 Pemindahan Fizikal Media

Media yang mengandungi maklumat perlu dilindungi supaya tidak diperolehi oleh orang yang tidak dibenarkan serta dilindungi daripada sebarang penyalahgunaan atau kerosakan semasa proses pemindahan atau pengangkutan.

8.0 Kawalan Akses

8.1 Dasar Kawalan Capaian

a. Mengawal capaian ke atas maklumat, kemudahan proses maklumat dan proses perkhidmatan berdasarkan keperluan perkhidmatan dan keperluan keselamatan.

b. Peraturan kawalan capaian hendaklah mengambil kira faktor *authentication, authorization* dan *accounting* (AAA).

8.2 Akses ke Rangkaian dan Perkhidmatan Rangkaian

1. Sebarang perisian yang boleh mengancam keselamatan rangkaian dan komunikasi tidak dibenarkan penggunaannya sama sekali melainkan mendapat kelulusan JICTU.

2. Kelulusan khas daripada JICTU adalah diperlukan bagi penyambungan rangkaian ke organisasi luar dan premis-premis yang bukan di bawah kawalan universiti.

3. Menyediakan *firewall* dan *Intrusion Detection System* (IDS) atau *Intrusion Prevention Sytem* (IPS) sebagai salah satu kaedah keselamatan komputer dari pencerobohan dan gangguan rangkaian.

4. Menyediakan perisian antivirus yang berkesan bagi mengawal penyebaran virus komputer.

5. Kebolehcapaian Pengguna (*User Accessibility*).

8.2.1 Rangkaian Setempat

1. Hanya kakitangan dan pelajar UTHM dibenarkan membuat penyambungan ke rangkaian UTHM.
2. Pengguna luar perlu mendapatkan kebenaran PTM sebelum membuat capaian ke rangkaian UTHM.
3. Penggunaan perisian pengintip (*sniffer*) atau penganalisis rangkaian (*network analyzer*) tidak dibenarkan.

8.2.2 Rangkaian Wi-Fi

1. Hanya kakitangan dan pelajar UTHM dibenarkan menggunakan rangkaian tanpa wayar di UTHM
2. Pengguna luar perlu mendapatkan kebenaran UTHM sebelum menggunakan rangkaian tanpa wayar.
3. Pengguna yang disahkan sahaja dibenarkan membuat capaian ke Rangkaian UTHM.
4. Penggunaan perisian sniffer atau *network analyzer* tidak dibenarkan.

8.2.3 Peranti Mudah Alih dan Telekerja

8.2.3.1 Dasar Peranti Mudah Alih

1. Peranti perlu mempunyai *antivirus* dan *patches* yang terkini: dan
2. Peranti mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.

8.2.3.2 Telekerja

1. Memastikan proses pengesahan pengguna *Remote* digunakan untuk mengawal capaian logikal ke atas kemudahan *port diagnosis* dan konfigurasi jarak jauh; dan
2. Sebarang capaian ke dalam dari luar UTHM hanya dibenarkan dengan akses melalui VPN (*Virtual Private Network*) rasmi UTHM dan perlu mendapat kelulusan ICT *Security Officer* (ICTSO).

8.3 Dasar Kawalan Akses

8.3.1 Pendaftaran dan Nyahdaftar Pengguna

Proses pendaftaran dan nyahdaftar pengguna perlu melalui sistem keselamatan berpusat dengan kawalan capaian penggunaan satu pengenalan diri (ID) dan kata laluan untuk semua aplikasi yang berkaitan.

8.3.2 Peruntukan Akses Pengguna

Pemberian kata laluan perlu dikawal melalui satu proses pengurusan yang formal.

8.3.3 Pengurusan Keutamaan Capaian Pengguna Pengesahan Maklumat Rahsia

1) Penggunaan akaun khas (*super user*) mesti dihadkan untuk pengguna khas sahaja berdasarkan kepada keperluan penggunaan dan perlu mendapat kelulusan daripada Pengurus ICT.
2) Rekod penggunaan bagi setiap akaun khas yang diwujudkan mesti disimpan, dikaji dan diselenggara.
3) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja.

8.3.4 Semakan Hak Capaian Pengguna

Semakan kepada kebenaran hak capaian pengguna perlu dikaji setiap 12 bulan.

8.3.5 Penyahdaftaran dan Pelarasan Hak Capaian

PTM boleh menyahdaftar, membekukan atau membuat pelarasan semula akaun pengguna yang telah tamat perkhidmatan, tamat pengajian atau perubahan bidang tugas dan tanggungjawab.

8.4 Tanggungjawab Pengguna

8.4.1 Penggunaan Pengesahan Maklumat Rahsia

1. Pengguna hendaklah merahsiakan kata laluan daripada pengetahuan orang lain;
2. Pengguna diminta menukar kata laluan sekurang-kurangnya setiap dua belas bulan sekali bagi mengelak akaun mudah dicerobohi;
3. Pengguna adalah dilarang melakukan pencerobohan ke atas akaun pengguna lain. Perkongsian akaun juga adalah dilarang; dan
4. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna.

8.5 Kawalan Capaian Sistem dan Aplikasi

8.5.1 Menghadkan Capaian Maklumat

Capaian terhadap sistem aplikasi adalah terhad kepada pengguna dan bagi tujuan yang dibenarkan.

8.5.2 Menghadkan Kawalan Capaian Maklumat

8.5.2.1 Perisian Aplikasi

Kawalan keselamatan dilaksana untuk mengelakkan berlakunya capaian oleh pengguna yang tidak sah, pengubahsuaian, pendedahan atau penghapusan maklumat. Universiti bertanggungjawab menyediakan kawalan dan kemudahan seperti berikut:

1. Sistem keselamatan berpusat dengan kawalan capaian penggunaan satu nama pengguna (ID) dan kata laluan untuk semua aplikasi yang berkaitan.
2. Profil capaian yang menghad tahap capaian maklumat serta fungsi-fungsi berdasarkan peranan pengguna.
3. Kawalan peringkat sistem aplikasi yang menentukan akauntabiliti tertentu kepada pengguna.
4. Penetapan pemilik (*ownership*) maklumat.

8.5.3 Prosedur *"Log-on"* yang Selamat

1. Mengesahkan pengguna yang dibenarkan selaras dengan peraturan UTHM;
2. Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log-on* yang terjamin;
3. Menjana amaran *(alert)* sekiranya berlaku pelanggaran ke atas peraturan keselamatan sistem;
4. Menyedia kaedah sesuai untuk pengesahan capaian *(authentication)*;
5. Menghadkan tempoh penggunaan mengikut kesesuaian;
6. *Session time out* perlu diaktifkan bagi satu tempoh yang ditetapkan; dan
7. Mewujudkan *audit trail* ke atas semua capaian sistem operasi terutama pengguna bertaraf khas *(super user).*

8.5.4 Sistem Pengurusan Kata Laluan

Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh UTHM seperti berikut:

1. Sistem pengurusan kata laluan perlu interaktif dan mampu mengekalkan kualiti kata laluan;
2. Pengguna hendaklah menggunakan kata laluan yang sukar diteka, sekurang-kurangnya lapan (8) aksara dengan gabungan *alphanumeric*; dan
3. Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekalipun; dan
4. Bagi mengelakkan pencerobohan data/maklumat daripada berlaku, *administrator password* perlu selalu kerap diubah.

8.5.5 Penggunaan Perisian Utiliti Khas

Penggunaan program utiliti yang berkemungkinan mampu untuk mengatasi kawalan sistem aplikasi perlu dihadkan dan dikawal ketat.

8.5.6 Kawalan Capaian kepada Program Kod Sumber

Kawalan capaian ke atas kod sumber atau aturcara program dilakukan bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian.

9.0 Kriptografi

9.1 Kawalan Kriptografi

9.1.1 Dasar Penggunaan Kawalan Kriptografi

1. Pengguna hendaklah membuat penyulitan (*encryption*) ke atas maklumat sensitif atau terperingkat.
2. Pengguna yang terlibat dalam menguruskan transaksi maklumat penting secara elektronik hendaklah menggunakan tandatangan digital yang dikeluarkan oleh Pihak Berkuasa Persijilan (*Certification Authority*) yang ditauliahkan oleh Kerajaan Malaysia atau badan-badan *Certification Authority* antarabangsa yang diiktiraf.

9.1.2 Pengurusan Kunci

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

10.0 Keselamatan Fizikal dan Persekitaran

10.1 Kawasan Terkawal

10.1.1 Ruang

1. Ruang tidak terlalu sempit;
2. Adanya kawalan keselamatan lain seperti pengesan asap (*Smoke Detector*)*;*
3. Menggunakan kaedah penghawa dingin yang dipasang dari lantai bagi mengelak air penghawa dingin menitik diatas komputer atau lain-lain kaedah yang bersesuaian untuk Bilik dan Bilik Suis;
4. Tahap pencahayaan yang sesuai perlu diambil kira bagi mengelakkan cahaya yang terlalu gelap atau terlalu terang;
5. Memastikan bilangan *power socket* yang mencukupi;
6. Semua kerja-kerja pendawaian perlu diperkemaskan menggunakan saluran *trunking* yang sesuai;
7. Memastikan alat litar pintas yang terkawal atau yang asing dipasang bagi mengelakkan kebakaran besar berlaku;
8. Memastikan bahawa jeriji pintu dan pintu keluar keselamatan disediakan di setiap makmal komputer; dan
9. Memastikan penyelenggaraan alat pencegahan kebakaran dilakukan secara berkala.

10.1.2 Kawalan Kemasukan Fizikal

1. Setiap warga UTHM hendaklah memakai pas pekerja, pelajar dan pelawat sepanjang waktu di kawasan UTHM;
2. Setiap pelawat hendaklah mendapatkan pas pelawat dan hendaklah dipulangkan selepas tamat lawatan;
3. Kehilangan pas mestilah dilaporkan dengan segera kepada Pegawai Keselamatan UTHM; dan
4. Maklumat pelawat seperti tarikh, masa dan tempat dituju hendaklah direkod dan dikawal.

10.1.3 Kawalan Pejabat, Bilik dan Kemudahan

Merekabentuk dan melaksanakan kawalan kemasukan fizikal di dalam pejabat, bilik dan kemudahan. Setiap warga UTHM hendaklah memakai pas pekerja/pelajar/pelawat.

10.1.4 Perlindungan Terhadap Ancaman Luaran dan Persekitaran

1. Merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana;
2. Kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan alat pengesan asap;
3. Peralatan perlindungan hendaklah dipasang di tempat yang sesuai, mudah dikenali, dikendalikan dan disenggarakan dengan baik;

4. Kecemasan persekitaran seperti kebakaran dan kebocoran air hendaklah dilaporkan segera kepada pihak yang bertanggungjawab;
5. Pentadbir server perlu memastikan keselamatan server daripada pencerobohan. Ini termasuk kepada membuat pemeriksaan ke atas proses tersembunyi (*hidden processes*), *daemon*, mengemaskini dan mengenalpasti pengguna-pengguna. Pusat Tanggungjawab (PTj) penyedia *server* boleh menyedia *firewall* khusus untuk tujuan ini;
6. Server yang melibatkan penyimpanan maklumat penting dan kritikal perlu mempunyai *backup* yang lengkap untuk mengelak kehilangan maklumat dan mengurangkan masa *downtime*. Urusan operasi penduaan adalah di bawah tanggungjawab penyedia server;
7. Server yang digunakan untuk projek pelajar perlu mendapat kelulusan daripada penyelia projek atau Dekan. Alamat IP (*Internet Protocol*) dalaman statik akan digunakan untuk server ini. Manakala alamat IP global boleh diberikan kepada projek yang memerlukan capaian Internet;
8. Pentadbir server di PTj bertanggungjawab memastikan server tidak disalahguna untuk tujuan yang bukan sepatutnya;
9. Semua pentadbir/penyedia server perlu mematuhi peraturan berikut:

    a. Pertukaran alamat IP tidak dibenarkan sama sekali tanpa kebenaran pentadbir alamat IP.
    b. Login dan kata laluan untuk *root* dan *super-user* adalah di bawah kawalan dan tanggungjawab pentadbir server sepenuhnya.

10. Untuk memastikan Pusat Data sentiasa selamat dari pencerobohan atau gangguan beberapa langkah boleh diambil seperti:
    a. Semua server perlu didaftarkan dengan Pusat Teknologi Maklumat, berada di dalam domain UTHM dan perlu menyatakan dengan jelas fungsi server tersebut;
    b. Semua server untuk kegunaan dalaman akan diberi alamat IP dalaman statik. Alamat IP global boleh dipertimbangkan oleh Pusat Teknologi Maklumat untuk keperluan mencapai fail daripada internet melalui server;
    c. Sistem penghawa dingin hendaklah dihidupkan 24 jam sehari dan berfungsi dengan baik;
    d. Kesemua aset ICT di Pusat Data hendaklah dilengkapi dengan kemudahan *Uninterruptible Power Supply* (UPS) dan *Generator*;
    e. Alat pemadam api hendaklah diletakkan di tempat yang mudah dilihat, tidak terhalang oleh sesuatu, mudah dicapai, tidak melepasi tarikh luput serta disenggarakan dengan baik;
    f. Hanya pegawai atau pelawat yang dibenarkan boleh memasuki Pusat Data;
    g. Pembekal dibenarkan memasuki Pusat Data dengan diiringi oleh pegawai bertanggungjawab dan hendaklah dicatat di buku log yang disediakan; dan
    h. Setiap pelayan hendaklah dilabelkan bagi memudahkan pentadbir ICT menjalankan tugas.

10.1.5 Bekerja di Kawasan Terkawal

1. Kawasan larangan ialah kawasan yang dihadkan kemasukan untuk pihak tertentu sahaja seperti Pusat Data, bilik fail dan bilik sulit yang menempatkan data dan maklumat sulit.

2. Pihak ketiga dilarang memasuki kawasan larangan kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal. Mereka hendaklah dipantau sepanjang masa sehingga tugas di kawasan berkenaan selesai.

10.1.6 Kawasan Penghantaran dan Pemunggahan

Penghantaran dan pemunggahan perlu dilakukan di kawasan yang telah ditetapkan bagi menjamin keselamatan.

10.2 Peralatan

10.2.1 Keselamatan Fizikal

1. **Peralatan ICT**

   a. Bekalan elektrik yang stabil perlu disediakan.

   b. *Lightning Arrestor* perlu disediakan pada bangunan tinggi bagi melindungi panahan kilat.

   c. Perkakasan komputer dan rangkaian perlu dipasangkan UPS dan Surge *Arrestor* bagi menstabilkan bekalan elektrik disamping dapat mencegah daripada kemusnahan data/maklumat.

   d. Perlu disimpan atau diletakkan di tempat yang sesuai dan terkawal.

   e. Tidak dibenarkan mengubah lokasi alatan ICT tanpa kebenaran JTMB.

   f. Alatan ICT tidak boleh diletakkan pada tempat yang berhampiran dengan saluran paip atau di bawah alatan yang boleh menghasilkan air seperti alat penghawa dingin.

   g. Alatan keselamatan perlu diselenggara secara berjadual.

10.2.2 Keselamatan dan Etika Penggunaan

1. Perisian tidak boleh disalahgunakan seperti:
    a. Menggunakan kemudahan perisian universiti bagi tujuan yang tidak bermoral dan tidak berfaedah.
    b. Membuat salinan perisian yang berlesen kecuali mendapat kebenaran.
2. Pengguna dilarang untuk memuat turun perisian-perisian yang bukan bertujuan akademik.
3. Bagi mengelakkan daripada kecurian komputer:
    a. Peralatan-peralatan komputer tidak boleh diletakkan di kawasan laluan umum dan bilik tanpa ciri-ciri keselamatan.
    b. Perlu diletakkan pelekat "*Hak Milik UTHM*".
    c. Semua peralatan ICT mesti berada dalam tahap kawalan dan keselamatan yang sempurna.
4. Semua staf adalah tertakluk kepada Akta Rahsia Rasmi 1972.
5. Semua emel yang dibina atau disimpan di dalam sistem boleh dicapai oleh universiti jika terdapat keperluan undang-undang.

10.2.3 Utiliti Sokongan

1. Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada aset ICT.
2. Perkara yang perlu dipatuhi bagi menjamin keselamatan bekalan kuasa adalah seperti berikut:
    a. Melindungi semua aset ICT dari kegagalan bekalan elektrik dan menyalurkan bekalan yang sesuai kepada aset ICT;
    b. Menggunakan peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan Penjana (*generator*) bagi perkhidmatan kritikal seperti di Pusat Data supaya mendapat bekalan kuasa berterusan; dan
    c. Menyemak dan menguji semua peralatan sokongan bekalan kuasa secara berjadual.

10.2.4 Keselamatan Pengkabelan

Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah berikut hendaklah diambil:

1. Menggunakan kabel mengikut standard dan spesifikasi yang ditetapkan;
2. Kabel dan laluan pemasangan kabel sentiasa dilindungi; dan
3. Mematuhi piawaian pengkabelan yang ditetapkan oleh pihak UTHM.

10.2.5 Penyelenggaraan Peralatan

1. Peralatan hendaklah disenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti.

2. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut:

    a. Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang disenggara;

    b. Memastikan perkakasan hanya disenggara oleh staf atau pihak yang dibenarkan sahaja;

    c. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyenggaraan;

    d. Memaklumkan pihak pengguna sebelum melaksanakan penyenggaraan mengikut jadual yang ditetapkan atau atas keperluan;

    e. Bertanggungjawab terhadap setiap perkakasan bagi penyenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; dan

    f. Semua penyenggaraan mestilah mendapat kebenaran daripada Pengurus ICT/Pentadbir ICT.

10.2.6 Keselamatan Inventori

1. Pengguna yang dipertanggungjawabkan hendaklah bertanggungjawab menjaga keselamatan perkakasan peralatan ICT yang dipertanggungjawabkan.
2. Sebarang kehilangan perkakasan/peralatan ICT adalah tanggungjawab pengguna/pemilik yang dipertanggungjawabkan.
3. Pengguna adalah tidak dibenarkan membuka peralatan ICT untuk tujuan meminda, mengubah, mengambil atau membuang alatan sama ada berlaku kerosakan atau tidak. Sebarang kerosakan atau kehilangan alatan adalah tanggungjawab pengguna/pemilik yang dipertanggungjawabkan.

4. Sebarang kerosakan atau permasalahan yang berlaku kepada perkakasan dan peralatan ICT hendaklah dilaporkan kepada Pusat Teknologi Maklumat.
5. Pengguna tidak dibenarkan menukar atau memindah kedudukan perkakasan/peralatan ICT yang berkaitan KECUALI mendapat kelulusan atau kebenaran.
6. Pengguna tidak dibenarkan memasang (*install*) perisian-perisian cetak rompak.

10.2.7 Keselamatan Peralatan dan Aset di Luar Kawasan

1. Peralatan dan maklumat yang dibawa keluar dari pejabat hendaklah mendapat kelulusan pegawai berkaitan dan tertakluk kepada tujuan yang dibenarkan sahaja. Peralatan dan maklumat perlu dilindungi dan dikawal sepanjang masa.
2. Memastikan aktiviti peminjaman dan pemulangan aset ICT direkodkan dan menyemak peralatan yang dipulangkan supaya berada dalam keadaan baik dan lengkap.
3. Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh UTHM bagi membawa masuk/keluar peralatan.
4. Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih. Peralatan hendaklah disimpan atau dikunci di tempat yang selamat apabila tidak digunakan.

10.2.8 *Clear Desk* dan *Clear Screen Policy*

1. Semua Pengguna ICT UTHM adalah disarankan untuk menggunakan *Clear Desk* dan *Clear Screen* supaya tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada di atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.
2. Perkara yang perlu dipatuhi adalah seperti berikut:

a. Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer.

b. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci.

c. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat. Kemaskini secara berkala mengikut keperluan.

11.0 Keselamatan Operasi

11.1 Prosedur Operasi dan Tanggungjawab

11.1.1 Mendokumenkan Prosedur Operasi

1. Pengendalian Prosedur Operasi bertujuan memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat.
2. Semua prosedur keselamatan ICT yang diwujudkan, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal.
3. Setiap prosedur hendaklah mengandungi arahan-arahan yang jelas, teratur dan lengkap. Semua prosedur hendaklah dikemas kini dari masa ke semasa mengikut keperluan.
4. Menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka pada dokumen.

11.1.2 Pengurusan Perubahan

1. Pengubahsuaian mestilah mendapat kebenaran pihak pengurusan atau pemilik aset ICT terlebih dahulu.
2. Aktiviti-aktiviti seperti pemasangan, penyenggaraan, mengemas kini komponen aset dan sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan dan kemahiran atau terlibat secara langsung dengan aset ICT berkenaan.
3. Aktiviti perubahan atau pengubahsuaian hendaklah mematuhi spesifikasi atau kriteria yang ditetapkan dan hendaklah direkodkan serta dikawal bagi mengelakkan berlakunya ralat.

11.1.3 Pengurusan Kapasiti

1. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan
2. Penggunaan peralatan dan sistem mestilah dipantau dan perancangan perlu dibuat bagi memenuhi keperluan kapasiti pada masa akan datang untuk memastikan prestasi sistem berada di tahap optimum.

11.1.4 Pengasingan Persekitaran Pembangunan, Pengujian dan Operasi

Persekitaran untuk pembangunan, pengujian dan operasi hendaklah diasingkan untuk mengurangkan risiko berlakunya hak capaian yang tidak dibenarkan ke atas persekitaran operasi.

11.2 Keselamatan Daripada Ancaman Virus Komputer

11.2.1 Antivirus

Setiap sistem pengoperasian di UTHM perlu dipasang dengan perisian antivirus yang disediakan oleh Pusat Teknologi Maklumat.

1. Setiap pemilik komputer/*server* adalah bertanggungjawab memastikan komputer/*server* mereka telah dipasang dengan perisian antivirus (*pattern* dan *scan engine* terkini) yang disediakan oleh Pusat Teknologi Maklumat.
2. Ketua makmal komputer bertanggungjawab memastikan komputer/*server* mereka telah dipasang dengan perisian antivirus (*pattern* dan *scan engine* terkini) yang disediakan oleh Pusat Teknologi Maklumat.

3. Pusat Teknologi Maklumat tidak bertanggungjawab ke atas data jika komputer/*server* itu diserang virus akibat sistem pengoperasian yang tidak mempunyai perisian antivirus.

11.2.2 Perubahan Versi (*version*)

Versi baru perisian bagi aplikasi dan sistem pengoperasian sentiasa dikeluarkan secara berkala bagi mengatasi masalah pepijat dan ancaman serta meningkatkan fungsinya. Perubahan versi perisian perlu dikawal bagi memastikan integriti perisian apabila perubahan dibuat dan ini memerlukan pematuhan kepada prosedur kawalan perubahan.

\

11.2.3 Kod Jahat

1. Bagi memastikan integriti maklumat daripada pendedahan atau kemusnahan daripada kod jahat seperti virus maka kawalan berikut perlu digunakan:

    a. Melaksanakan prosedur untuk menguruskan kod jahat.

    b. Mewujudkan polisi berkaitan memuat turun, penerimaan dan penggunaan perisian *freeware* dan *shareware*.

    c. Menyebarkan arahan dan maklumat untuk mengesan kod jahat kepada semua pengguna.

    d. Mendapatkan bantuan sekiranya disyaki dijangkiti virus.

2. Bagi masalah serangan virus, ikuti langkah-langkah berikut:

    a. Gunakan perisian anti virus yang telah diluluskan.

    b. Imbasan virus menggunakan kemudahan yang disediakan oleh perisian antivirus.

    c. Hapus dan buang virus berkenaan dengan segera.

    d. Menyemak status imbasan di dalam laporan log.

    e. Tidak melaksana (*run*) atau membuka fail lampiran (*attachment*) daripada emel yang meragukan.

11.3 *Backup*

11.3.1 Penduaan Maklumat

1. Perlu menyediakan *backup* sistem yang baik bagi menjamin data penting universiti disimpan dengan selamat.

2. Penduaan dari pelayan atau komputer ke media storan lain perlu dilakukan dari masa ke semasa untuk mengelak kehilangan data sekiranya berlaku kerosakan *human error* atau *hardware error*.

3. Kekerapan penduaan data bergantung kepada keperluan operasi dan kepentingan data tersebut sama ada secara harian, mingguan atau pun bulanan.

4. Penduaan sistem aplikasi dan sistem pengoperasian perlu diadakan sekurang-kurangnya sekali bagi setiap versi.

5. Penduaan data yang melibatkan saiz data yang besar hendaklah dibuat di luar waktu bekerja untuk mengelakkan kesesakan serta mengganggu prestasi.

6. Penduaan data yang penting dan kritikal dicadangkan dibuat satu (1) salinan dan disimpan di tempat yang berasingan bagi mengelakkan kemusnahan atau kerosakan fizikal disebabkan oleh bencana seperti kebakaran, banjir atau sebagainya. Lokasi tempat perlu dirujuk di dokumen Pelan Pemulihan Bencana ICT UTHM.

7. Sistem penduaan sedia ada hendaklah diuji bagi memastikan ianya dapat berfungsi, boleh dipercayai dan berkesan apabila digunakan *(restoration).*

8. Faktor ketahanan dan jangka hayat media storan perlu diambil kira dalam melakukan penduaan serta merancang penyalinan semula kepada media storan yang baru.

9. Setiap perisian perlu ada salinan pendua sebagai keselamatan data/maklumat.

11.4 Perekodan Pemantauan

11.4.1 Perekodan Log

1. Mewujudkan sistem log bagi merekodkan aktiviti harian pengguna dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;

2. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan

3. Mengaktifkan *audit log* bagi merekodkan aktiviti pengemaskinian untuk tujuan statistik, pemulihan, pemantauan dan keselamatan.

11.4.2 Perlindungan Terhadap Maklumat Log

1. Maklumat log dan kemudahan log perlu dilindungi daripada sebarang pencerobohan dan pindaan.

2. Sekiranya wujud aktiviti-aktiviti tidak sah seperti kecurian maklumat dan pencerobohan hendaklah dilaporkan.

11.4.3 Pentadbir dan Operator Log

Aktiviti yang dijalankan oleh pentadbir ICT yang menguruskan sistem perlu dilogkan dan disemak.

11.4.4 Penyelarasan Masa

Waktu pelayan dan peralatan ICT yang berpusat dan kritikal perlu diselaraskan dengan satu sumber waktu yang piawai.

11.5 Kawalan Perisian Operasi

11.5.1 Pemasangan Perisian ke atas Sistem Yang Beroperasi

1. Perisian merujuk kepada atur cara/program yang dilaksanakan oleh sistem komputer. Perisian yang digunakan perlu dilindungi supaya kebocoran maklumat dan gangguan perkhidmatan dapat dielakkan.
2. Keperluan bagi memasukkan perisian yang baru hendaklah dirujuk kepada prosedur yang telah ditetapkan.
3. Perisian yang ada perlu dipastikan mempunyai kawalan capaian perisian yang sesuai bagi mengelakkan data/maklumat daripada terpadam.
4. Setiap perisian yang menggunakan konsep *client-server* perlu di selia bersama Pusat Teknologi Maklumat.
5. Perisian-perisian antivirus yang terkini perlu disediakan bagi mengelakkan serangan virus komputer.

11.6 Pengurusan Keterdedahan Teknikal

11.6.1 Pengurusan Keterdedahan Teknikal

Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut:

1. Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan;
2. Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan
3. Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.

11.6.2 Sekatan ke atas Pemasangan Perisian

1. Pengguna dilarang memasukkan perisian yang tidak sah ke dalam komputer masing-masing.
2. Sebarang pemasangan perisian yang tidak sah serta mengakibatkan kerosakan atau kehilangan data akan dipertanggungjawabkan sepenuhnya kepada pengguna terbabit.

11.7 Pertimbangan Semasa Audit Sistem Aplikasi

11.7.1 Objektif

Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem aplikasi.

11.7.2 Pangkalan Data

Universiti bertanggungjawab mengadakan kawalan capaian kepada pangkalan data. Integriti maklumat yang disimpan di dalam pangkalan data dikekal dan dijamin secara:

1. Pengurusan pangkalan data memastikan integriti dalam pengemaskinian dan capaian maklumat.
2. Kawalan capaian kepada maklumat ditentukan oleh Pentadbir.

11.7.3 Pengawalan Audit Sistem Aplikasi

1. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan.
2. Capaian ke atas peralatan audit sistem aplikasi perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.

12.0 Keselamatan Rangkaian Dan Komunikasi / Pengurusan Keselamatan Komunikasi

12.1 Dasar dan Prosedur Pemindahan Maklumat

Maklumat yang akan dipindahkan kepada entiti luar perlu mendapat kelulusan pemilik maklumat.

12.2 Keselamatan Maklumat / Pemindahan Maklumat

12.2.1 Had-Had Pengambilan Maklumat Peribadi

Penggunaan maklumat peribadi seseorang mestilah menyatakan tujuan penggunaan maklumat itu dengan jelas dan nyata seperti berikut:

1. Apabila maklumat peribadi diambil daripada seseorang individu itu, maklumat itu mestilah diberikan oleh tuan punya maklumat.
2. Pemberi maklumat perlu diberitahu/dimaklum untuk mengesahkan (tandatangan) sesuatu maklumat yang telah diberikan.

12.2.2 Kaedah Pengambilan Data dilakukan dengan Cara yang disebutkan di bawah:

1. Pengambilan maklumat peribadi dengan kaedah yang mengikut dasar, peraturan atau undang- undang yang dibenarkan.

2. Maklumat peribadi tidak boleh diambil dengan menipu tujuan maklumat itu diambil ataupun dengan cara *hacking.*
3. Maklumat peribadi juga boleh diambil menerusi lamanweb UTHM yang telah diberi mandat untukmendapatkan maklumat peribadi seseorang.

12.2.3 Larangan Terhadap Pengambilan Maklumat yang Mengandungi Isu-Isu Sensitif

1. Maklumat peribadi tidak boleh diambil, digunakan atau dihebahkan kecuali maklumat itu diambil setelah mendapat kebenaran pemilik maklumat.
2. Semua maklumat hendaklah dinyatakan dengan jelas tujuan penggunaannya semasa permohonan mendapatkan maklumat dilakukan.
3. Maklumat kesihatan hanya boleh diambil oleh Pegawai Perubatan yang bertauliah yang menguruskan pesakit-pesakit sahaja.

12.2.4 Had-Had Pengambilan Data Selain Daripada Pemberi Maklumat (Bukan Tuan Punya Maklumat)

Bagi kes di mana maklumat diambil daripada orang ketiga, tuan punya maklumat hendaklah dimaklumkan tentang maklumat yang diambil dan tujuan penggunaan maklumat tersebut. Apabila maklumat yang diberi oleh seseorang kepada seseorang yang lain dengan izin pemilik maklumat, perkara berikut hendaklah diikuti:

1. Tujuan pengambilan maklumat.
2. Jenis maklumat yang diambil.
3. Tanggungjawab untuk memastikan maklumat dijaga atau disimpan dengan baik.

12.2.5 Had-Had Penggunaan Maklumat Peribadi

Maklumat peribadi mestilah digunakan untuk tujuan yang telah dinyatakan ketika maklumat itu diperolehi daripada pemberi maklumat dalam skop yang dibenarkan oleh UTHM.

12.2.6 Perjanjian Dalam Pemindahan Maklumat

1. Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara UTHM dengan entiti luar.
2. Memastikan pemindahan maklumat selaras dengan perjanjian.

12.3 Mesej Elektronik

12.3.1 Maklumat Umum Mesej Elektronik

1. Akaun e-mel bukanlah hak mutlak seseorang. Ia merupakan kemudahan yang tertakluk kepada peraturan UTHM dan boleh ditarik balik jika penggunaannya melanggar peraturan.
2. Kandungan dan penyenggaraan *mailbox* pada komputer peribadi adalah menjadi tanggungjawab pengguna.
3. Langkah-langkah keselamatan bagi penggunaan e-mel adalah seperti berikut:

    a) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi yang diperuntukkan oleh UTHM. E-mel persendirian tidak boleh digunakan untuk tujuan rasmi;

    b) Alamat e-mel penerima hendaklah dipastikan betul;

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

d) Pengguna hendaklah memastikan tarikh dan masa sistem komputer adalah tepat;

e) Penyimpanan salinan e-mel pada sumber storan kedua adalah digalakkan bagi tujuan keselamatan;

f) Pengguna hendaklah mengelak dari membuka e-mel dari penghantar yang tidak dikenali atau diragui;

g) Pengguna adalah dilarang melakukan pencerobohan ke atas akaun pengguna lain, menggunakan akaun orang lain, berkongsi akaun atau memberi akaun kepada orang lain;

h) Aktiviti *spamming*, *mail-bombing*, penyebaran virus, bahan-bahan negatif, bahan yang menyalahi undang-undang, tidak beretika, surat berantai, maklumat berbau politik, hasutan atau perkauman atau apa-apa maklumat yang menjejaskan reputasi jabatan dan perkhidmatan awam adalah dilarang;

i) Penggunaan kemudahan e-mel *group* hendaklah dengan cara yang beretika dan benar-benar perlu sahaja bagi mengelakkan bebanan ke atas sistem e-mel UTHM. Penghantaran e-mel yang berulang-ulang juga adalah dilarang;

j) Pentadbir ICT berhak memasang sebarang jenis perisian *antivirus* atau perkakasan penapisan e-mel yang difikirkan sesuai bagi mencegah, menapis atau menyekat mana-mana e-mel diterima atau dikirim yang mengandungi virus atau berunsur *spamming*;

k) Pentadbir ICT boleh memeriksa, memantau dan melihat isi kandungan e-mel dan ruang storan pengguna e-mel (seperti atas keperluan audit dan keselamatan) dengan kebenaran pengguna;

l) Pentadbir ICT boleh memberi peringatan atau amaran kepada pengguna sekiranya didapati terdapat aktiviti yang mengancam sistem e-mel UTHM; dan

m) Semua lampiran menggunakan format *executable file* (.exe, .com dan .bat) tidak dibenarkan kerana format ini berisiko membawa dan menyebarkan virus. Pentadbir e-mel berhak menapis sebarang penghantaran serta penerimaan kandungan e-mel yang berisiko dari semasa ke semasa.

12.3.2 Kawalan Terhadap Penggunaan Akaun Emel

1. Pengguna digalakkan tidak membuka lampiran yang diragui mengandungi *letterbomb* atau virus yang boleh merosakkan komputer dan rangkaian UTHM. *Attachment* yang sering mengandungi virus ialah fail yang mempunyai *extension* .exe, .zip, .pif, .scr dan sebagainya.
2. Pengguna digalakkan tidak menjawab emel yang tidak berkenaan seperti *spam*, ugutan atau ofensif kerana dengan menjawab emel yang sedemikian pengguna mendedahkan diri kepada aktiviti yang tidak bertanggungjawab. Pengguna adalah bertanggungjawab untuk melaporkan kepada *Postmaster*.
3. *Postmaster* dengan kelulusan Pihak Pengurusan Pusat Teknologi Maklumat berhak memeriksa dan melihat isi kandungan emel dan ruang storan pengguna dari semasa ke semasa bagi keperluan audit dan keselamatan.

4. Setiap emel yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan.

12.3.3 Kawalan Terhadap Penyelenggaraan *Mailbox*

1. Pengguna bertanggungjawab menyelenggara kandungan *mailbox* pada PC.
2. Pengguna perlu sentiasa mengimbas fail dalam *mailbox* dengan perisian anti virus bagi memastikan fail yang disimpan, dihantar atau diterima melalui *attachment* bebas daripada virus.
3. Emel hendaklah tidak mengandungi maklumat rahsia atau sulit yang boleh disalahguna untuk merosakkan akaun, stesen kerja, *server* dan rangkaian UTHM.
4. Pengguna bertanggungjawab menghapuskan kandungan emel yang tidak penting, tidak mempunyai nilai arkib dan yang tidak diperlukan lagi.

12.4 Perjanjian Kerahsiaan atau Ketidaktirisan Maklumat

Keperluan bagi perjanjian kerahsiaan atau ketidaktirisan maklumat yang mencerminkan keperluan organisasi untuk melindungi maklumat perlu dikenalpasti, dikaji secara berkala jika perlu dan didokumenkan.

13.0 Perolehan, Pembangunan dan Penyelenggaraan Sistem Aplikasi Universiti

13.1 Keperluan Keselamatan Sistem Aplikasi

13.1.1 Analisis Keperluan Maklumat dan Spesifikasi Keselamatan Maklumat

1. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu proses dan ketepatan maklumat.
2. Aplikasi perlu menjalani proses semakan dan pengesahan untuk mengelakkan sebarang kesilapan pada maklumat akibat daripada pemprosesan atau perlakuan yang tidak disengajakan.

13.1.2 Kawalan Keselamatan Aplikasi di Rangkaian Awam

Kawalan keselamatan aplikasi di rangkaian awam perlu dikawal dan disemak secara berkala untuk memastikan kawalan keselamatan yang sesuai dapat diterapkan ke dalam aplikasi bagi menghalang sebarang bentuk kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat daripada berlaku kepada sistem aplikasi. Semua maklumat rasmi yang hendak dimuatkan di sistem yang berasaskan web di UTHM hendaklah mendapatkan kelulusan daripada pihak yang bertanggungjawab.

13.1.3 Melindungi Transaksi Perkhidmatan Aplikasi

Maklumat yang terlibat dalam transaksi perkhidmatan aplikasi hendaklah dilindungi untuk mencegah penghantaran yang tidak lengkap, salah penghantaran dan pendedahan, pengubahan mesej dan duplikasi mesej yang tidak dibenarkan atau berulang.

13.2 Keselamatan dalam Pembangunan dan Proses Sokongan

13.2.1 Polisi Pembangunan Perisian

Pembangunan perisian dan sistem serta sebarang pembangunan yang melibatkan proses sokongan maklumat dan aplikasi perlu dilaksanakan mengikut keperluan dan ianya hendaklah dikaji dan disemak secara berkala untuk memastikan keberkesanannya.

13.2.2 Prosedur Kawalan Perubahan Sistem

1. Mewujudkan peraturan dan garis panduan keselamatan yang bersesuaian untuk mengawal pelaksanaan perubahan.
2. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja.

13.2.3 Semakan Teknikal bagi Aplikasi Setelah Pertukaran Platform Sistem Pengoperasian

Apabila pengoperasian sistem ditukar, aplikasi yang kritikal mesti disemak dan diuji untuk memastikan tiada kesan sampingan terhadap keselamatan dan operasi UTHM secara khususnya dan organisasi secara amnya daripada berlaku.

13.2.4 Sekatan ke atas Perubahan Pakej Perisian

1. Mengawal perubahan dan pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja
2. Pengggunaan *Versioning Control Software* (VCS) di dalam pembangunan dan penyelenggaraan sistem bagi memastikan terdapat kawalan perubahan pada pakej sistem.
3. Akses kepada kod sumber aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja.

13.2.5 Prinsip Keselamatan Berkaitan Kejuruteraan Sistem

Prinsip keselamatan dalam pembangunan dan sokongan sistem yang berkaitan dengan kejuruteraan sistem perlu diwujudkan dan direkodkan.

13.2.6 Pengujian Aplikasi

1. Universiti bertanggungjawab menguji aturcara, modul, sistem aplikasi dan integrasi sistem aplikasi bagi memastikan sistem berfungsi mengikut spesifikasi yang ditetapkan.
2. Universiti mengambil langkah berikut semasa pengujian aplikasi:
   a) Menggunakan data ujian (*dummy*) atau data lapuk (*historical*).
   b) Mengawal penggunaan data sulit (*classified*).
   c) Menghadkan capaian kepada kakitangan yang terlibat sahaja.
   d) Menghapuskan maklumat yang digunakan setelahselesai pengujian (terutamanya apabila menggunakan data lapuk).
   e) Menggunakan persekitaran yang berasingan untukpembangunan dan pengoperasian sistem aplikasi.

13.2.7 Ujian Keselamatan Sistem

Ujian keselamatan sistem hendaklah dijalankan ke atas input sistem untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan output sistem untuk memastikan data yang telah diproses adalah tepat.

13.2.8 Ujian Penerimaan Sistem

Ujian penerimaan sistem perlu dijalankan ke atas sesuatu sistem aplikasi yang telah dibangunkan. Ianya merangkumi pengujian keperluan keselamatan maklumat dan kepatuhan kepada amalan pembangunan sistem yang selamat. Pengujian perlu dijalankan di persekitaran sebenar bagi memastikan sistem tersebut selamat daripada sebarang ancaman. Sistem aplikasi yang telah siap dibangunkan akan diserahkan kepada pemilik sistem.

Langkah-langkah yang perlu dilaksanakan untuk ujian penerimaan sistem:

1. Menghadkan capaian kepada kakitangan yang terlibat sahaja.
2. Menghapuskan maklumat yang digunakan setelah selesai pengujian (terutamanya apabila menggunakan data lapuk).

13.3 Data Ujian

Jenis tindakan yang boleh digunakan bagi tujuan pengujian data:

1. Menggunakan data ujian (*dummy*) atau data lapuk (*historical*).
2. Mengawal penggunaan data sulit (*classified*).

13.3.1 Pelindungan Terhadap Data Ujian

Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal.

14.0 Hubungan dengan Pembekal

14.1 Polisi Keselamatan Maklumat Berhubung dengan Pembekal

14.1.1 Polisi Keselamatan Maklumat Berhubung dengan Pembekal

Pihak UTHM hendaklah memastikan keselamatan penggunaan maklumat dan kemudahan pemprosesan maklumat oleh kontraktor/pihak ketiga dikawal seperti prosedur yang telah ditetapkan. Perkara yang perlu dipatuhi adalah seperti berikut:

1. Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian;
2. Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pembekal. Capaian kepada aset ICT UTHM perlu berlandaskan kepada perjanjian kontrak; dan
3. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan disenggarakan oleh pembekal.

14.1.2 Elemen Keselamatan dalam Perjanjian dengan Pembekal

Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pembekal.

14.1.3 Keperluan Keselamatan ICT Terhadap Rantaian Pembekal

Perjanjian dengan pembekal atau pihak ketiga harus merangkumi keperluan keselamatan untuk menangani sebarang risiko keselamatan maklumat yang berkaitan dengan ICT dan rantaian bekalan produk/perkhidmatan.

14.2 Pengurusan Perkhidmatan Penyampaian Pembekal

14.2.1 Memantau dan Menyemak Perkhidmatan Pembekal

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

14.2.2 Mengurus Perubahan untuk Perkhidmatan Pembekal

1. Sebarang perubahan skop perkhidmatan yang diberikan oleh pihak ketiga perlu diurus mengikut keperluan semasa. Ia termasuklah bekalan, perubahan terhadap perkhidmatan sedia ada dan pertambahan perkhidmatan baru.
2. Penilaian risiko perlu dilakukan berdasarkan tahap kritikal sesuatu sistem dan impak yang wujud terhadap perubahan tersebut.

15.0 Pengurusan Insiden Keselamatan Maklumat

15.1 Pengurusan Insiden Keselamatan Maklumat dan Penambahbaikan

15.1.1 Tanggungjawab dan Prosedur

1. Tanggungjawab pasukan UTHM *Computer Emergency Response Team* (UTHMCERT):

    a. Menerima dan mengambil tindakan ke atas insiden keselamatan yang dilaporkan.

    b. Menyediakan laporan tindakan insiden keselamatan kepada JICTU dan Pasukan Tindak balas Insiden Keselamatan ICT Kerajaan (GCERT).

    c. Menyebarkan maklumat bagi membantu pengukuhan keselamatan ICT di UTHM dari semasa ke semasa.

    d. Menyediakan khidmat nasihat kepada pelanggan dalam mengesan, mengenal pasti dan menangani sesuatu insiden keselamatan ICT.

    e. Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden.

    f. Merekod dan menjalankan siasatan awal insiden yang diterima. Mengambil tindak balas insiden keselamatan ICT dan mengambil tindakan baik pulih.

    g. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden dapat dielakkan.

    h. Meningkatkan pengetahuan dan kesedaran keselamatan ICT melalui program kesedaran keselamatan ICT.

i. Setiap pengguna perlu diberikan program kesedaran dan latihan ICT dalam melaksanakan tugas dan tanggungjawab mereka.

j. Menjalankan program menangani insiden sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT.

2. Prosedur pelaporan insiden keselamatan ICT perlu dilaksanakan berdasarkan:

a. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan

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

c. Prosedur Pengendalian Insiden Keselamatan ICT

15.1.2 Melaporkan Insiden Keselamatan Maklumat

Insiden keselamatan maklumat mesti dilaporkan kepada UTHMCERT mengikut Prosedur Pengendalian Insiden Keselamatan ICT dengan kadar segera. Insiden keselamatan ICT adalah seperti berikut:

1. Maklumat disyaki atau didapati hilang dan didedahkan kepada pihak-pihak yang tidak diberi kuasa;
2. Sistem aplikasi digunakan tanpa kebenaran atau disyaki sistem aplikasi digunakan tanpa kebenaran;
3. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;
4. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan
5. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini.

15.1.3 Melaporkan Kelemahan Keselamatan Maklumat

1. Kelemahan keselamatan maklumat mesti dilaporkan kepada ICTSO dengan kadar segera bagi mengelakkan insiden keselamatan maklumat.
2. Pengguna, kontraktor dan pihak ketiga adalah dilarang daripada membuktikan sebarang kelemahan sistem tanpa kebenaran.
3. Ujian untuk membuktikan kelemahan sistem tanpa kebenaran boleh ditafsirkan sebagai penyalahgunaan sistem dan boleh menyebabkan kerosakan kepada sistem maklumat atau perkhidmatan. Ini boleh mengakibatkan tindakan undang-undang bagi individu yang menjalankan ujian tersebut.

15.1.4 Penilaian dan Keputusan Insiden Keselamatan Maklumat

1. Pasukan tindak balas insiden terdiri daripada pasukan UTHMCERT dan pemilik proses yang berkenaan. Pasukan ini bertanggungjawab untuk menganalisis; mengesahkan setiap insiden; dan juga mendokumenkan setiap langkah yang diambil.
2. Bagi setiap insiden yang dikenal pasti, pasukan tersebut harus melaksanakan analisis awal bagi menentukan skop insiden seperti:
    a. Rangkaian, sistem atau perkhidmatan yang terlibat;
    b. Siapa atau apa yang menyebabkan insiden; dan
    c. Bagaimana insiden berlaku.
3. Analisis awal tersebut perlu merangkumi maklumat yang cukup untuk membolehkan pasukan tindak balas insiden menyusun aktiviti-aktiviti seterusnya seperti pembendungan insiden dan analisis mendalam bagi melihat kesan daripada insiden tersebut.
4. Pasukan tindak balas insiden ini perlu berhati-hati untuk melindungi data yang berkaitan dengan sesuatu insiden seperti maklumat sistem yang dicerobohi atau pengguna yang telah terbabit dalam tindakan yang menyalahi peraturan.

5. Semua insiden keselamatan maklumat yang dikenal pasti mesti disusun mengikut keutamaan dan berdasarkan kepada impak negatif yang berpotensi terhadap maklumat dan/atau sistem aplikasi.

6. Menyusun keutamaan dalam mengendalikan insiden merupakan satu keputusan yang kritikal dalam proses pengendalian insiden.

15.1.5 Tindakbalas Terhadap Insiden Keselamatan Maklumat

1. Semasa pengendalian insiden, pasukan tindakbalas insiden mesti memaklumkan status semasa insiden tersebut kepada pihak UTHMCERT.

2. Apabila insiden telah dikenal pasti dan dianalisis, pasukan tindak balas insiden harus mengawal insiden tersebut sebelum merebak dan mengakibatkan kerosakan yang lebih serius.

3. Proses pembendungan ini harus dipertimbangkan sebagai sebahagian daripada proses pengendalian insiden pada peringkat awal dan mesti melibatkan pihak pengurusan dalam memberi keputusan seperti penutupan sesuatu sistem atau perkhidmatan. Ciri-ciri penentuan strategi yang sesuai termasuk:

    a. Ketersediaan perkhidmatan;

    b. Kerosakan yang berpotensi kepada sumber-sumber sedia ada;

    c. Keperluan untuk pemeliharaan bahan bukti;

    d. Masa dan sumber-sumber yang diperlukan untuk melaksanakan strategi;

    e. Keberkesanan strategi; dan

    f. Tempoh bagi suatu penyelesaian.

15.1.6 Mengambil Pengajaran dari Insiden Keselamatan Maklumat

1. Pasukan tindak balas insiden mesti mempunyai pengetahuan seiring dengan ancaman dan teknologi yang terkini.
2. Mesyuarat harus diadakan dengan semua pihak yang terbabit selepas berlaku sesuatu insiden yang besar dan secara berkala bagi insiden-insiden yang kecil bagi tujuan:
    a. Analisis insiden;
    b. Analisis punca insiden;
    c. Tindakan pembetulan yang telah diambil dan keberkesanan tindakan tersebut; dan
    d. Tindakan pencegahan yang mungkin untuk diambil bagi mengurangkan kebarangkalian pengulangan insiden.

15.1.7 Pengumpulan Bahan Bukti

1. Pasukan tindak balas insiden mesti mendokumenkan dengan jelas bagaimana bahan-bahan bukti termasuk sistem yang telah dikompromi akan dipelihara.
2. Log mesti disimpan sebagai bahan bukti.
3. Secara umum, bukti yang jelas mesti diwujudkan berdasarkan perkara-perkara berikut:
    a. Bagi salinan keras *(hardcopy)*: Salinan asal mesti disimpan dengan selamat dengan merekod butiran lanjut seperti individu yang menemui dokumen tersebut; lokasi dokumen ditemui, tarikh dan masa ditemui; dan saksi bagi penemuan bahan bukti.
    b. Bagi maklumat di dalam media komputer: imej cermin *(mirror image)* atau salinan daripada media boleh ubah, maklumat di dalam cakera keras atau di dalam memori mesti diambil untuk memastikan ketersediaan; dan log bagi semua tindakan semasa proses salinan mesti disimpan.

16.0 Aspek Keselamatan Maklumat dalam Pengurusan Kesinambungan Perkhidmatan

16.1 Kesinambungan Keselamatan Maklumat

16.1.1 Merancang Kesinambungan Keselamatan Maklumat

1. Pelan Kesinambungan Perkhidmatan hendaklah dibangunkan dengan mengambil kira faktor-faktor keselamatan maklumat bagi menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini adalah untuk memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi kepada pelanggan.
2. Pelan Kesinambungan Perkhidmatan perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut:
    a. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;
    b. Senarai pegawai UTHM dan pembekal berserta nombor yang boleh dihubungi (telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan pegawai tidak dapat hadir untuk menangani insiden.
    c. Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta prosedur pemulihan maklumat dan kemudahan yang berkaitan;
    d. Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan
    e. Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan yang berkaitan.

16.1.2 Melaksanakan Kesinambungan Keselamatan Maklumat

Perkara-perkara berikut perlu diberi perhatian:

1. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;
2. Mengenalpasti insiden yang boleh menyebabkan gangguan, kemungkinan dan kesan gangguan serta akibat terhadap keselamatan ICT;
3. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;
4. Mendokumentasikan proses dan prosedur yang telah dipersetujui;
5. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan.

16.1.3 Mengesah, Menyemak dan Menilai Kesinambungan Keselamatan Maklumat

1. Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.
2. Pengesahan perlu dilaksanakan setiap kali selesai kerja-kerja pengujian kesinambungan keselamatan maklumat.

16.2 *Redundancies*

16.2.1 Kesediaan Kemudahan Pemprosesan Maklumat

Bagi memenuhi keperluan ketersediaan sistem sepertimana yang dinyatakan di dalam Pelan Kesinambungan Perkhidmatan, kemudahan pemprosesan maklumat perlu dilaksanakan di dalam persekitaran

redundancies; termasuk tetapi tidak terhad kepada server dan perkakasan rangkaian di dalam Pusat Data UTHM.

17.0 Pematuhan

17.1 Pematuhan kepada Keperluan Perundangan dan Kontrak

17.1.1 Mengenalpasti Keperluan Perundangan dan Kontrak yang Berkaitan

Berikut adalah keperluan perundangan atau peraturan-peraturan lain yang berkaitan yang perlu dipatuhi oleh semua pengguna ICT UTHM dari masa ke semasa iaitu seperti:

1. Akta Universiti dan Kolej Universiti (AUKU);
2. Arahan Keselamatan
3. Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
4. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002;
5. Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
6. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan;
7. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
8. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;
9. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;

10. Surat Arahan Ketua Pengarah MAMPU – Langkah-langkah Mengenai Penggunaan Mel Elektronik di Agensi-agensi Kerajaan yang bertarikh 1 Jun 2007;
11. Surat Arahan Ketua Pengarah MAMPU – Langkah-langkah Pemantapan Pelaksanaan Sistem Mel Elektronik D agensi-agensi Kerajaan yang bertarikh 23 November 2007;
12. Surat Arahan KSN – 2006 Langkah-langkah Untuk Mengukuhkan Keselamatan *Wireless* LAN di Agensi-agensi Kerajaan;
13. Surat Arahan KSN – 2007 Langkah-langkah Keselamatan Perlindungan Untuk Larangan Penggunaan Telefon Bimbit atau Lain-lain Peralatan Komunikasi;
14. Pekeliling Perbendaharaan Bilangan 5 Tahun 2007 – Tatacara Pengurusan Aset Alih Kerajaan (TPA);
15. Pekeliling Am Bil. 53 Tahun 2011 UTHM/PP/100-6/5/1 Bertarikh 22 Julai 2011 - Amalan Terbaik Penggunaan Media Jaringan Sosial Di Universiti Tun Hussein Onn Malaysia;
16. Surat Pekeliling Perbendaharaan 5 Tahun 2007 – Tatacara Pengurusan Perolehan Kerajaan Secara Tender;
17. Surat Pekeliling Perbendaharaan Bilangan 5 Tahun 2009 – Perubahan Had Nilai dan Tatacara Pengurusan Perolehan Secara Sebut Harga;
18. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010;
19. Akta Rahsia Rasmi 1972;
20. Akta Tandatangan Digital 1997;
21. Akta Jenayah Komputer 1997;
22. Akta Hak Cipta (pindaan) tahun 1997;
23. Akta Komunikasi dan Multimedia 1998;
24. Suruhanjaya Komunikasi dan Multimedia Malaysia 1998;
25. Pekeliling Am Bil. 6 Tahun 1999: Garis Panduan Pelaksanaan Perkongsian Pintar Antara Agensi-agensi Kerajaan Dalam Bidang Teknologi Maklumat yang dikeluarkan oleh MAMPU;
26. Pekeliling Am Bil. 3 Tahun 2000: Dasar Keselamatan ICT Kerajaan yang dikeluarkan oleh *Malaysian Administrative Modernisation and Management Planning Unit* (MAMPU);

27. Pekeliling Am Bil.1 Tahun 2000: Garis Panduan Malaysian Civil Service Link (MCSL) dan Laman Web Kerajaan yang dikeluarkan oleh MAMPU;
28. Pekeliling Am Bil.1 Tahun 2001: Mekanisme Pelaporan Insiden Keselamatan ICT (ICT) yang dikeluarkan oleh MAMPU;
29. Surat Pekeliling Am Bilangan 3 2015 Garis Panduan Permohonan Kelulusan Teknikal Dan Pemantauan Projek Teknologi Maklumat & Komunikasi (ICT) Agensi Sektor Awam;
30. Arahan Teknologi Maklumat 2007;
31. Akta Aktiviti Kerajaan Elektronik 2007 (Akta 680);
32. Peraturan-peraturan Pegawai Awam (Kelakuan dan Tatatertib) 1993;
33. Akta Perlindungan Data Peribadi 2010;
34. Akta *Tele-medicine* 1997;
35. Dasar-dasar, Pekeliling, Polisi ICT UTHM yang dikeluarkan dari semasa ke semasa;
36. Akta, Pekeliling, Arahan, Arahan Perbendaharaan, Garis Panduan, Perintah-Perintah Am dan surat pekeliling yang dikeluarkan dari semasa ke semasa; dan
37. Dasar-dasar kerajaan yang berkaitan.

17.1.2 Hak Harta Intelek

Prosedur berikut perlu dipatuhi dalam penggunaan material yang mempunyai hak cipta dan perisian *propritery*:

1. Akta Hakcipta 1997 hendaklah sentiasa dipatuhi bagi menghalang aktiviti meniru hak cipta orang lain;
2. Penggunaan perisian yang sah;
3. Pembelian dari sumber yang sahih;
4. Mengekalkan daftar aset dan mengenalpasti semua keperluan perlindungan terhadap aset;
5. Memastikan bilangan had lesen tidak melebihi had ditetapkan;

6. Menjalankan pemeriksaan perisian yang sah dan produk berlesen digunakan; dan

7. Pengguna adalah dilarang daripada menyalahgunakan kemudahan pemprosesan maklumat untuk tujuan yang tidak dibenarkan.

17.1.3 Perlindungan Rekod

Rekod yang penting perlu dilindungi daripada kecurian, kemusnahan dan pemalsuan seperti yang tertakluk dalam Akta Keselamatan.

17.1.4 Privasi dan Perlindungan ke atas Data Peribadi yang Dikenalpasti

Perlindungan data peribadi perlu diwujudkan selaras dengan undang-undang sekiranya berkaitan.

17.1.5 Peraturan Kawalan Kriptografi

Kawalan kriptografi perlu tertakluk kepada undang-undang yang berkaitan.

17.2 Kajian Semula Keselamatan Maklumat

17.2.1 Kajian Semula Keselamatan Maklumat oleh Pihak Berkecuali

Pendekatan UTHM untuk menguruskan keselamatan maklumat dan pelaksanaan hendaklah dikaji secara berkala atau apabila perubahan ketara berlaku pada sebarang maklumat ICT UTHM dan jika perlu dilakukan oleh pihak berkecuali atau pihak bebas.

17.2.2 Pematuhan Polisi dan Piawaian

1. Semua pengguna di UTHM perlu membaca, memahami dan mematuhi Polisi ICT UTHM dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa dari masa ke semasa.
2. ICT *Security Officer* (ICTSO) perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing adalah mematuhi dasar, piawaian dan keperluan teknikal. Sistem aplikasi perlu diperiksa secara berkala bagi mematuhi piawai pelaksanaan keselamatan ICT.

17.2.3 Kajian Semula Pematuhan Teknikal

Sistem Perkhidmatan ICT mestilah diperiksa secara berkala untuk memastikan ia mematuhi Polisi ICT UTHM yang sedia ada. Sebarang semakan pematuhan teknikal mestilah dijalankan oleh individu yang kompeten yang diberi kebenaran.

18.0 Etika Pengguna

1. Perisian tidak boleh disalahgunakan seperti:
    a. Menggunakan kemudahan perisian universiti bagi tujuan yang tidak bermoral dan tidak berfaedah.
    b. Membuat salinan perisian yang berlesen kecuali mendapat kebenaran.

2. Pengguna dilarang untuk memuat turun perisian- perisian yang bukan bertujuan akademik.

3. Bagi mengelakkan daripada kecurian komputer:

    a. Peralatan-peralatan komputer tidak boleh diletakkan di kawasan laluan umum dan bilik tanpa ciri-ciri keselamatan.

    b. Perlu diletakkan pelekat "*Hak Milik UTHM*".

    c. Semua peralatan ICT mesti berada dalam tahap kawalan dan keselamatan yang sempurna.

4. Semua staf adalah tertakluk kepada Akta Rahsia Rasmi 1972.

5. Semua emel yang dibina atau disimpan di dalam sistem boleh dicapai oleh universiti jika terdapat keperluan undang-undang.

Lampiran A

SURAT AKUAN PEMATUHAN POLISI ICT

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

Nama (Huruf Besar) : ……

No. Kad Pengenalan : ……

Jawatan : ……

Agensi/Jabatan/Bahagian/Syarikat : ……

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:-

1. Saya memahami dan mematuhi peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT UTHM dan Polisi ICT UTHM;
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Saya mengaku semua maklumat yang diberikan dalam dokumen adalah betul dan benar.

Sebarang kenyataan palsu boleh menyebabkan saya diambil tindakan tatatertib.

Tanda tangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT (ICTSO)

.....

(Nama Pegawai Keselamatan ICT)

Tarikh: .....

TERHAD