DASAR KESELAMATAN ICT V1.0

UNIVERSITI TEKNOLOGI MARA

sIKandungan

		Muka surat
1.0	PRINSIP DASAR KESELAMATAN ICT	3
2.0	DEFINISI DASAR	11
3.0	PENILAIAN RISIKO KESELAMATAN ICT	12
4.0	AKAUNTABILITI DAN INTEGRITI	14
5.0	CAPAIAN TEKNOLOGI MAKLUMAT	18
6.0	KERAHSIAAN MAKLUMAT	21
7.0	STAF & PIHAK KETIGA	24
8.0	OPERASI ICT	32
9.0	RANGKAIAN	41
10.0	PENGGUNAAN E-MEL	48
11.0	MEMBANGUN LAMAN WEB DAN TAPAK HOSTING	54
12.0	PENGURUSAN SISTEM APLIKASI DAN PANGKALAN DATA	57
13.0	PENGURUSAN PERKHIDMATAN SERVER PELAYAN	64
14.0	PENGURUSAN AKSES KE PUSAT DATA UTAMA UiTM	69
15.0	PENGURUSAN KESINAMBUNGAN PERKHIDMATAN	71
16.0	PENGUATKUASAAN & PEMATUHAN	75
17.0	GLOSARI	77

1

PRINSIP DASAR KESELAMATAN ICT

1.0 PENGENALAN

Dasar Keselamatan ICT (DKICT) Universiti Teknologi MARA merupakan sebuah dokumen yang menggariskan peraturan penggunaan aset dan kemudahan ICT UiTM dengan cara yang betul. Ia mesti dibaca dan dipatuhi oleh setiap penguna (warga atau pihak ketiga UiTM) bagi penggunaan kemudahan ICT universiti.

Dasar ini menjadi asas tadbir urus ICT UiTM bagi memastikan penggunaan ICT yang cekap dan berkesan dengan pelaburan yang optimum.

2.0 TUJUAN

Tujuan dasar ini adalah untuk memaklumkan peraturan-peraturan yang perlu dipatuhi oleh semua penguna, untuk mengguna kemudahan yang diberikan secara berhemah dan menjaga keselamatan aset ICT dari segi perkakasan, perisian dan maklumat.

Dasar dan prosedur yang disediakan adalah selaras dengan piawaian yang digunapakai.

3.0 PERNYATAAN DASAR

DKICT UiTM diwujudkan untuk memastikan penggunaan sumber dan aset ICT universiti oleh setiap penguna, dari segi infrastruktur, sistem aplikasi, kemudahan

ICT serta data, adalah mengikut peraturan dan undang-undang. Kepatuhan setiap penguna kepada DKICT UITM akan menjadikan persekitaran ICT UiTM berkualiti tinggi dan selamat bagi melindungi dan menjamin perkhidmatan universiti dapat dijalankan dengan semaksima mungkin.

Universiti Teknologi MARA beriltizam untuk mewujudkan perkhidmatan ICT yang sistematik bagi meningkatkan kebolehpercayaan dan keberkesanan penyampaian perkhidmatan, selaras dengan keperluan perundangan sedia ada.

Dasar ini hendaklah dibaca bersama akta, pekeliling kerajaan, pekeliling UiTM, pekeliling Bendahari, surat arahan kerajaan, Prosedur Keselamatan ICT UiTM dan prosedur yang berkaitan.

4.0 Prinsip-prinsip yang menjadi asas kepada DKICT dan perlu dipatuhi adalah seperti berikut :

1. 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;

2. 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, mengemas kini, mengubah atau membatalkan

sesuatu maklumat. Hak akses akan dikemaskini dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas;

3. Akauntabiliti

Pengguna adalah bertanggungjawab keatas semua aset ICT, hak capaian dan tindakan yang telah diamanahkan;

4. Pengasingan

Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data perlu diasingkan dan dipantau oleh pihak tertentu bagi mengelakkan daripada akses yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi, perancangan dan perolehan;

5. Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti sebarang ketakakuran berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Justeru, pemeliharaan semua rekod yang berkaitan tindakan keselamatan adalah diperlukan. Aset-aset ICT seperti komputer, pelayan, router, firewall, IPS, Antivirus dan peralatan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau jejak audit (audit trail);

6. Pematuhan

DKICT 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 meminumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan berpunca dari insiden atau bencana. Pemulihan boleh dilakukan melalui aktiviti penduaan (*backup*) dan pewujudan pelan pemulihan bencana atau pelan kesinambungan perkhidmatan; dan

h. Saling Bergantungan

Setiap prinsip di atas adalah saling lengkap melengkapi dan bergantungan antara satu sama lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisma keselamatan adalah perlu bagi menjamin keselamatan yang maksimum. UiTM tidak boleh bergantung kepada satu individu, organisasi atau peralatan dalam pelaksanaan keselamatan ICT.

4.0 OBJEKTIF

Objektif DKICT adalah seperti berikut:

1. Memastikan kelancaran operasi Universiti khasnya, berterusan, meminimumkan kerosakan atau kemusnahan melalui usaha pencegahan atau usaha mengurangkan kesan insiden yang tidak diingini;
2. melindungi kepentingan pengguna dan sistem aplikasi daripada menghadapi kegagalan dan/atau kelemahan kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;

3. memastikan aset ICT terlindung daripada ancaman pencerobohan/penggodaman, kecurian data, serangan *malware* dan penafian perkhidmatan; dan
4. mencegah kes-kes penyalahgunaan serta kehilangan aset ICT Universiti.

5.0 SKOP

Dasar ini meliputi semua aset dan kemudahan ICT yang digunakan seperti maklumat (contoh: fail, dokumen, data elektronik), perisian (contoh: sistem aplikasi, perisian *desktop* dan perisian kolaborasi) dan fizikal (contoh: Pusat Data, PC, *server*, peralatan komunikasi, media storan dan lain-lain). Prinsip ini adalah terpakai oleh semua pengguna sebagai perkakasan ICT Universiti.

6.0 Definisi ICT

1. Perkakasan ICT

Semua peralatan yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan UiTM. Contoh komputer, *server*, peralatan komunikasi dan sebagainya;

2. 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, e-mel dan kolaborasi kepada UiTM;

3. Perkhidmatan

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contoh: Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain; Sistem halangan akses seperti kad akses; dan perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain;

4. Data atau Maklumat

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

5. Infrastruktur ICT

Infrastruktur ICT merangkumi sistem rangkaian dan Pusat Data UiTM. Sistem rangkaian yang dimaksudkan adalah sistem rangkaian berwayar, tanpa wayar, *Unified Communication, VPN,* Domain serta semua jenis peralatan komunikasi seperti *router, switch, firewall* dan lain-lain lagi. Pusat Data pula menempatkan *server,* perkakasan *back up* dan *recovery, VDI, Cloud Computing, HPC,* dan Storan.

6. Manusia

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

7. Premis Komputer Dan Komunikasi

Semua kemudahan serta premis yang digunakan untuk menempatkan

perkara (**1)** hingga **(6)** di atas. Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

7.0 PENAFIAN

UiTM menyediakan saluran elektronik untuk penyaluran maklumat dan bukannya penerbit. Oleh itu, melainkan ia adalah penerbitan rasmi universiti, UiTM tidak bertanggungjawab terhadap bahan atau komunikasi yang dibuat oleh satu atau lebih individu melalui *World Wide Web, internet*, atau rangkaian sosial; perkongsian fail; atau pengiriman melalui e-mel; atau sebarang tindakan yang dibuat melalui persekitaran maya. Walau bagaimanapun, dalam keadaan tertentu, UiTM boleh bertindak terhadap aduan mengenai bahan atau komunikasi tersebut.

1. UiTM berhak memasang perisian atau perkakasan penapisan e-mel dan virus (*e-mail filter and anti virus*) yang difikirkan sesuai. Ianya digunakan untuk mencegah, menapis, menyekat atau menghapuskan mana-mana *e-mail* yang disyaki mengandungi virus atau berunsur *spamming* daripada memasuki atau keluar *server*, stesen kerja atau rangkaian UiTM;
2. UiTM tidak bertanggungjawab terhadap sebarang kerosakan, kehilangan atau sebarang kesan lain kepada maklumat, aplikasi, *mailbox* atau fail yang disimpan oleh pengguna di dalam stesen kerja atau *server* akibat daripada penggunaan perkhidmatan rangkaian UiTM;
3. UiTM tidak bertanggungjawab terhadap pengguna yang menjadi penghantar *(sender)* atau penerima *(receiver)* kepada sebarang *e-mail* yang berunsur *spamming* atau penyebaran *e-mail* dengan kandungan tidak beretika;
4. Bagi kes kerosakan *e-mail*, pentadbir emel hanya bertanggungjawab untuk memulihkan kembali *(restore)* maklumat akaun staf dan bukannya

kandungan atau *mailbox* staf;

5. Fail yang mempunyai *extension .exe, .cmd, .bat, .hta, js, .vb, .mov, .avi, .mp3, .mpeg, .mpg, .wav, .rm, .ram, .rmx, .asf, .wmf, .wmp, .wsf, . wsh, .shs, .scr, .htm, .html, .qsm, .lnk, .wab, .dbx, .rar, .eml dan .zip* dan fail yang mempunyai kapasiti melebihi empat (4) *megabyte* akan dibuang secara automatik tanpa sebarang notis sekiranya dijumpai dalam tapak yang dihoskan; dan
6. *Pentadbir Emel* dengan kelulusan UiTM berhak menapis *e-mel* yang berkemungkinan memberi ancaman keselamatan ICT dan mengkaji ruang storan yang diberikan kepada staf dari semasa ke semasa atas keperluan audit dan keselamatan.

2

DEFINASI

1.0 AKTA UNIVERSITI

Akta universiti merupakan satu akta yang digubal oleh kerajaan Malaysia bagi penubuhan, penyelenggaraan dan pentadbiran universiti. Penubuhan UiTM adalah di bawah Peruntukan Perkara 153, Perlembagaan Persekutuan atau Akta 173. Ia juga dirujuk sebagai Akta 176 Universiti Teknologi MARA.

2.0 DASAR KESELAMATAN ICT

Dasar Keselamatan ICT adalah suatu rancangan tindakan yang telah dipersetujui secara rasmi sebagai asas untuk membuat dan melaksanakan keputusan berkaitan dengan teknologi maklumat (ICT).

3.0 PROSEDUR

Prosedur merupakan aturan atau tatacara menjalankan sesuatu aktiviti/tugas/kerja bagi memastikan tugas itu dijalankan dengan betul dan mengikut poisi dan peraturan yang telah ditetapkan.

4.0 GARIS PANDUAN

Garis panduan ialah penjelasan yang terperinci mengenai perkara yang harus dilakukan dalam menjalankan sesuatu aktiviti/tugas/kerja. Ia merupakan lanjutan daripada dasar tersebut.

3

PENILAIAN RISIKO KESELAMATAN ICT

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

UiTM hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk DKICT dalam mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat UiTM termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis-premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain. UiTM bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bil. 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

UiTM 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 pengurusan atasan;
c. Mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan
d. Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

4

AKAUNTABILITI DAN INTEGRITI ICT

1.0 TUJUAN

Ia menyatakan tanggungjawab pihak yang terlibat dengan penggunaan kemudahan ICT di UiTM seperti berikut:

1. Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap sumber ICT UiTM;
2. Melindungi kepentingan pengguna ICT apabila berlaku kejadian perlanggaran atau pencabulan dasar-dasar keselamatan ICT yang lain; dan
3. Memelihara akauntabliti dan integriti sumber-sumber ICT UiTM.

2.0 OBJEKTIF

Skop adalah meliputi tanggungjawab pengguna dan UiTM. Ia berkaitan dengan penggunaan, pencapaian, pemprosesan, penyimpanan maklumat atau perkhidmatan yang berkaitan dengan ICT yang merangkumi:

1. Perkhidmatan-perkhidmatan ICT;
2. Penyelenggaraan dan penyeliaan perkhidmatan-perkhidmatan ICT;
3. Penggunaan perkhidmatan-perkhidmatan ICT.

3.0 PENYATAAN

Jabatan Infostruktur sebagai pihak utama yang menyedia kemudahan dan peralatan ICT bertanggungjawab ke atas perkara berikut:

1. Menyedia peralatan ICT seperti komputer peribadi, komputer server, pencetak, alat-alat rangkaian (seperti *router, switch*, dan sebagainya), untuk memberi infrastruktur asas bagi pengguna-penggunanya menjalankan tugas;
2. Menyediakan perkhidmatan ICT;
3. Menyelenggara dan membaik pulih peralatan ICT yang berada di bawah tanggungjawab Jabatan Infostruktur;
4. Menyelenggara dan mengkonfigurasikan ciri-ciri keselamatan perkhidmatan ICT supaya selamat diguna pakai oleh pengguna;
5. Mengikuti perkembangan semasa keselamatan ICT dan mengambil langkah bersesuaian untuk meningkatkan kekebalan keselamatan peralatan dan perkhidmatan ICT;
6. Pentadbir sistem maklumat / pangkalan data bertanggungjawab membuat penyalinan (backup) data dan maklumat pengguna yang terdapat pada komputer-komputer server yang diselenggarakan;
7. Menyedia dan mengambil langkah-langkah keselamatan lain seperti penyediaan pendinding keselamatan (*firewall*), peralatan pemantauan, dan lain-lain peralatan dan perkhidmatan keselamatan yang difikirkan perlu;
8. Menyedia kemudahan auditan dengan merekod aktiviti pengguna ICT sama ada secara automatik atau manual menerusi penggunaan peralatan/perisian khusus atau menerusi kemasukan data-data tertentu ke dalam buku-buku log; dan
9. Melaksanakan polisi penyiasatan sebagaimana yang disediakan oleh MAMPU untuk menangani insiden-insiden pencabulan keselamatan.

3.1 Bukan Tanggungjawab UiTM

Sekiranya berlaku kesilapan mekanikal ke atas peralatan ICT yang disediakan oleh Jabatan Infostruktur yang menyebabkan keselamatan, integriti dan kandungan maklumat atau data yang dilindungi terjejas, dan kesilapan ini berlaku di luar jangkaan dan keperluan teknikal Jabatan Infostruktur, maka Jabatan Infostruktur tidak bertanggungjawab terhadap kemudaratan yang disebabkan oleh kesilapan mekanikal peralatan tersebut. Contohnya, jika berlaku *power surge* menyebabkan peralatan ICT seperti komputer peribadi, server dan sebagainya terbakar atau meletup maka ia bukan tanggungjawab Jabatan Infostruktur.

3.2 Melibatkan Tanggungjawab Pengguna dan Jabatan

Mematuhi peraturan-peraturan yang telah ditetapkan oleh Universiti:-

1. Bertanggungjawab terhadap kerosakan, kerugian, kehilangan atau gangguan perkhidmatan ke atas sistem-sistem lain, sekiranya aktiviti-aktiviti yang dilakukannya menyebabkan perkara-perkara tersebut berlaku, dan kegiatan tersebut dilakukan pada peralatan atau menggunakan perkhidmatan yang disediakan oleh UiTM.
2. Tidak memberi atau membenarkan dengan sengaja orang perseorangan atau individu lain menggunakan kemudahan dan perkhidmatan ICT yang disediakan oleh UiTM di atas identiti beliau.
3. Bertanggungjawab ke atas sebarang instalasi mana-mana perisian yang tidak disahkan (perisian tidak berlesen) oleh UiTM, dan sekiranya instalasi perisian tersebut mengakibatkan kerosakan, gangguan, atau ancaman keselamatan UiTM.

4. PTJ/Kampus Negeri perlu memastikan data dan maklumat dibawah pengurusannya sentiasa tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;

5. PTJ/Kampus Negeri perlu bertanggungjawab membuat salinan (*backup*) data, fail dan program kepunyaan sendiri yang dimiliki dan disimpan di komputer atau server masing-masing.

5

CAPAIAN TEKNOLOGI MAKLUMAT

1.0 TUJUAN

Ia menerangkan peraturan capaian kepada sumber-sumber ICT yang terdapat di UiTM. Semua capaian kepada komputer peribadi / server / komputer riba, rangkaian maklumat dan infrastruktur ICT UiTM adalah tidak dibenarkan kecuali setelah mendapat kebenaran atau kelulusan secara jelas dan nyata.

2.0 OBJEKTIF

1. Memelihara keselamatan dan integriti sumber ICT UiTM.
2. Memastikan perkongsian sumber yang saksama.

3.0 SKOP

Capaian kepada sumber ICT ini merangkumi akaun pengguna bagi sistem-sistem komputer berbilang pengguna, capaian kepada komputer peribadi dan nod rangkaian serta alamat IP bagi penyambungan sesuatu komputer kepada rangkaian UiTM. Capaian boleh diberikan kepada pelajar, staf dan sesiapa yang berkenaan untuk tujuan pengajaran, pembelajaran, penyelidikan, perundingan dan pentadbiran.

4.0 PENYATAAN

1. Kemudahan capaian adalah diberikan kepada seseorang pengguna secara individu dan pengguna tidak boleh memberi kemudahan tersebut kepada orang lain termasuk ahli keluarga, pelajar atau staf UiTM. Ini termasuk berkongsi akaun pengguna dan kata laluan serta membenarkan komputer dan perisian digunakan oleh orang lain. Pengguna adalah bertanggungjawab penuh ke atas semua capaian yang dibuat melalui akaunnya.
2. Pengguna yang menggunakan sumber-sumber ICT UiTM mestilah mematuhi dasar penggunaan ICT dan menghormati hak intelek serta hak mencapai sumber-sumber yang sama oleh pengguna-pengguna yang lain. Pengguna tidak dibenarkan :

    a. Menggunakan sumber ICT UiTM untuk mendapat atau cuba mendapat capaian tidak sah kepada mana-mana sistem komputer sama ada di dalam atau di luar UiTM. Ini termasuk membantu, mendorong, menyembunyikan percubaan untuk mencapai sistem-sistem komputer tersebut atau mencapai sumber ICT UiTM dengan menggunakan identiti pengguna yang lain;
    b. Menggunakan sumber ICT UiTM untuk mencapai mana-mana perisian, fail teks, imej atau muzik atau apa jenis fail termasuk yang bersifat lucah, *abusive*, hasutan, *slanderous*, *defamatory* atau yang melanggar (*violate*) undang-undang negara; termasuk tetapi tidak terhad kepada mencapai dan menyebar muzik / video berhakcipta (dalam bentuk fail *mp3, ra, rm, ram, mpeg*, dsb), perisian komputer serta teks dan imej yang berhakcipta, program-program komputer yang berbentuk pemusnah (seperti virus, *worm*, *trojan* atau *back-door*);

c. Mencapai sumber ICT UiTM untuk menghantar *e-mel* yang berbentuk *spam*, pengeboman mel, *e-mel* palsu, *e-mel* berantai dan *e-mel* yang berbentuk hasutan, lucah, gangguan seksual dan bersifat perkauman;

d. Mencapai atau cubaan mencapai sumber elektronik (data, paparan, *keystrokes*, fail atau media storan) dalam sebarang bentuk yang dimiliki oleh pengguna lain tanpa mendapat kebenaran/kelulusan pengguna terbabit terlebih dahulu. Ini termasuk membaca, menyalin, menukar, merosak atau memadam data, program dan perisian. Penggunaan penganalisis rangkaian (*network analyser*) atau pengintip (*sniffer*) adalah dilarang;

e. Menyambungkan alat/peranti elektronik/komputer (termasuk tetapi tidak terhad kepada komputer peribadi, komputer riba dan *hub* atau *switch* peribadi serta modem) ke UiTM dengan tujuan untuk mendapat capaian kepada sumber-sumber ICT UiTM perlu mendapat kebenaran/kelulusan bertulis daripada Pengarah Jabatan Infostruktur atau PTJ/Kampus Negeri. Kebenaran/kelulusan ini adalah bergantung kepada tahap piawai dan keselamatan untuk alat/peranti elektronik/komputer tersebut yang telah ditetapkan oleh JPPIT;

f. Pengguna adalah digalak untuk menggunakan sumber ICT UiTM dengan sebaik mungkin bagi memberi manfaat kepada misi dan matlamat UiTM dalam bidang pengajaran, pembelajaran, penyelidikan, perundingan dan pentadbiran.

6

KERAHSIAAN MAKLUMAT UiTM

1.0 TUJUAN

Ia menerangkan aktiviti-aktiviti yang dilakukan oleh pentadbir operasi yang melibatkan capaian data, maklumat atau kegiatan pengguna yang difikirkan rahsia atau sulit. Seksyen ini memberi gambaran munasabah terhadap perkara-perkara yang disebutkan di atas di mana pengguna perlu tahu.

2.0 OBJEKTIF

1. Memelihara kerahsiaan data dan maklumat UiTM
2. Memelihara integriti data dan maklumat UiTM
3. Memelihara keberadaan data dan maklumat UiTM

3.0 PENYATAAN

3.1 Capaian Maklumat Sulit

1. Pentadbir operasi sesuatu sistem atau sumber ICT berkuasa untuk mencapai, merekod, atau memantau data, maklumat atau kegiatan pengguna dari semasa ke semasa sebagai rutin pemantauan keselamatan ICT. Maklumat-maklumat yang direkodkan ini akan digunakan untuk tujuan penjagaan keselamatan ICT. Contohnya, arahan dalam sistem komputer server UNIX seperti *last, syslogd, acctcom, pacct* yang berfungsi merekod aktiviti pengguna untuk tujuan pengauditan.

2. Jika pengguna disyaki melanggar Dasar Keselamatan Operasi ICT, pentadbir operasi mempunyai mandat tanpa mendapat kebenaran terlebih dahulu daripada CIO, untuk memantau dengan lebih jitu kegiatan dan aktiviti pengguna berkenaan. Segala maklumat yang direkodkan boleh digunakan sebagai bukti. Sekiranya didapati pelanggaran Dasar Keselamatan Operasi ICT tersebut serius seperti menggunakan identiti pengguna lain untuk mencuri data atau merosakkan sumber ICT, maka bukti-bukti yang dikumpul akan dimajukan kepada Unit Pengurusan Risiko Universiti.
3. Sebagai langkah pemeliharaan bukti, pentadbir operasi boleh membuat salinan sama ada dalam bentuk bercetak atau digital kesemua atau sebahagian kandungan akaun pengguna. Pentadbir operasi dengan kebenaran ICTSO boleh mencapai maklumat atau data sulit atau rahsia pengguna seperti e-mel atau fail-fail yang tersimpan dalam akaunnya.
4. Pengguna diberi jaminan bahawa selain daripada perkara-perkara yang disebutkan di atas, data, maklumat rahsia atau sulit yang terdapat dalam akaun pengguna tidak akan dicapai oleh sesiapa pun. Sekiranya ada individu atau pengguna lain mencapai data atau maklumat pengguna lain tanpa kebenaran, maka individu tersebut (pengguna biasa atau pentadbir operasi) telah melanggar Dasar Capaian Teknologi Maklumat.
5. Pengguna ditegah menyimpan data atau maklumat sensitif, rahsia atau sulit di dalam akaunnya.
6. Sebarang permohonan untuk mendapatkan data perlu mendapat kelulusan pemilik data terlebih dahulu.

3.2. Pemantauan Data dalam Rangkaian

1. Sebagai sebahagian daripada rutin penjagaan keselamatan sumber ICT, pentadbir operasi berkuasa untuk memantau dan merekodkan data-data

yang berada dalam rangkaian. Peralatan rangkaian seperti router atau sistem komputer server yang menggunakan perisian-perisian tertentu mampu merekodkan data-data dalam rangkaian. Jaminan diberikan bahawa data-data yang direkodkan tidak akan didedahkan melainkan jika berlaku kejadian pelanggaran Dasar Keselamatan Operasi ICT.

2. Sama seperti kes capaian maklumat di atas sekiranya pentadbir operasi mengesyaki pengguna melanggar Dasar Keselamatan Operasi ICT, maka pentadbir operasi mempunyai mandat tanpa mendapat kebenaran Jawatankuasa JPPIT untuk memantau dan merekodkan data-data atas talian yang melibatkan aktiviti pengguna dengan lebih teliti. Data komunikasi sesi daripada mesin/peralatan yang digunakan oleh pengguna yang disyaki akan direkodkan, dan setiap *keystroke* juga akan direkodkan. Data-data ini kemudiannya akan digunakan sebagai bahan bukti dan untuk proses pengauditan yang akan dilakukan oleh Juruaudit Keselamatan ICT UiTM.

3. Jaminan adalah diberikan kepada pengguna bahawa selain daripada perkara-perkara yang dinyatakan di atas, adalah menjadi kesalahan jika pengguna (pentadbir operasi atau pengguna biasa) memantau atau merekodkan data-data yang berada dalam rangkaian.

7

STAF & PIHAK KETIGA

1.0 KESELAMATAN PERALATAN ICT

Melindungi aset ICT daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.

1.1. Peralatan ICT

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:-

1. Staf hendaklah menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan sempurna;
2. Staf bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;
3. Staf dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan;
4. Staf adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;
5. Staf mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemaskini di samping melakukan imbasan ke atas media storan yang digunakan (jika tidak dihubungkan dengan sistem kawalan Anti Virus Berpusat);

6. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;
7. Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;
8. Peralatan ICT yang hendak dibawa keluar dari premis UiTM, perlulah mendapat kelulusan PTJ/Kampus Negeri dan direkodkan bagi tujuan pemantauan serta pemakluman kepada Polis Bantuan UiTM;
9. Staf perlu melaporkan segera kepada Polis Bantuan UiTM dan Polis Daerah sekiranya perkakasan tersebut hilang atau dicuri dalam tempoh 24 jam kehilangan dan membuat laporan berdasarkan Pekeliling Bendahari Bil 1/1998 – Aturcara Kehilangan Wang/Harta Benda UiTM bagi peralatan yang dibekalkan oleh UiTM.
10. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;
11. Staf tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran PTJ/Kampus Negeri;
12. Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada *Help Desk/* Meja Bantuan/Bahagian ICT PTJ/Kampus Negeri untuk dibaik pulih;
13. Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;
14. Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;
15. Staf dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password*) yang telah ditetapkan oleh Pentadbir Sistem ICT;
16. Staf bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;
17. Staf hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "*OFF*" apabila meninggalkan pejabat; dan

18. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada Pengarah Jabatan Infostruktur/PTJ/Kampus Negeri.

1.2. Komputer Riba

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

1. Komputer riba hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan; dan
2. Memastikan komputer riba tidak disimpan di dalam kenderaan bagi mengelakkan daripada dikesan oleh pencuri.

1.3. Media Storan

Media Storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* dan media storan lain.

1. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan;
2. Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; dan
3. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.

1.4. Kabel Peralatan ICT

Kabel peralatan ICT hendaklah dilindungi kerana ia adalah salah satu punca maklumat.

Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan oleh Unit Rangkaian, Jabatan Infostruktur.

1.5. *Clear Desk* dan *Clear Screen*

Clear Desk dan tidak meninggalkan maklumat yang sensitif dan terperingkat terdedah samada di atas meja atau di paparan skrin apabila pemilik tidak berada di tempatnya.

Berikut adalah tindakan yang perlu diambil oleh staf:

1. Gunakan kemudahan *password screen saver* atau log keluar apabila meninggalkan computer peribadi; dan
2. Maklumat sensitif dan terperingkat hendaklah disimpan dalam laci atau kabinet fail yang berkunci.

2.0 PENGURUSAN PENYAMPAIAN PERKHIDMATAN PIHAK KETIGA

Perkara-perkara yang mesti dipatuhi adalah seperti berikut:

1. Pihak ketiga perlu memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan;
2. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula oleh pihak yang berkaitan dan diaudit dari semasa ke semasa; dan

3. Pengurusan perubahan garis panduan perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.

3.0 PENGURUSAN PERTUKARAN MAKLUMAT

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

Garis panduan, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi.

4.0 KAWALAN CAPAIAN

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja staf yang berbeza. Ia perlu direkodkan, dikemaskini dan menyokong garis panduan kawalan capaian staf sedia ada.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

1. Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan staf;
2. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;
3. Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan
4. Kawalan ke atas kemudahan pemprosesan maklumat.

4.1. PENGURUSAN CAPAIAN STAF

4.1.1. Akaun Staf

Setiap staf adalah bertanggungjawab ke atas sistem ICT yang digunakan.

Bagi mengenal pasti staf dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi:

1. Akaun yang diperuntukkan oleh UiTM sahaja boleh digunakan;
2. Akaun staf mestilah unik dan hendaklah mencerminkan identiti staf;
3. Akaun staf yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem terlebih dahulu;
4. Pemilikan akaun staf bukan hak mutlak seseorang dan ia tertakluk kepada peraturan UiTM. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;
5. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan
6. Pemilik Sistem boleh membekukan atau menamatkan akaun staf atas sebab-sebab salah guna hak capaian sistem; atau tidak lagi berkhidmat dengan UiTM.

4.1.2. Pengurusan Kata Laluan

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

1. Dalam apa jua keadaan dan sebab, kata laluan bagi peralatan ICT UiTM hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;
2. staf hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;

3. panjang kata laluan mestilah di antara 8-16 aksara dengan gabungan aksara, angka dan aksara khusus;
4. kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun;
5. kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;
6. kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;
7. kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula;
8. kata laluan hendaklah berlainan daripada pengenalan identiti staf;
9. had masa *idle* selama lima belas minit (15) minit dan selepas had itu, sesi ditamatkan;
10. kata laluan hendaklah ditukar selepas 6 bulan ; dan
11. mengelakkan penggunaan semula kata laluan yang baru digunakan.

5.0 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

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

5.1. Mekanisme Pelaporan

Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar DKICT sama ada yang ditetapkan secara tersurat atau tersirat.

Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan GCERT MAMPU dengan kadar segera sekiranya:

1. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang;
2. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;
3. Kata laluan atau mekanisme kawalan akses 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 dijangka.

   Prosedur pelaporan insiden keselamatan ICT berdasarkan:

   i. Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan
   ii. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.

5.2. Prosedur Pengurusan Maklumat Insiden Keselamatan ICT

Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada MAMPU. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut:

1. Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti;
2. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;
3. Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan;
4. Menyediakan tindakan pemulihan segera; dan
5. Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.

8

OPERASI ICT

1.0 TUJUAN

Untuk memastikan pengawalan dan pengurusan keselamatan ke atas perkakasan, perisian, aplikasi dan operasi komputer di UiTM.

2.0 OBJEKTIF

1. Menjamin semua aset ICT (kemudahan komputer, perisian, data, rangkaian dan peralatan) adalah dilindungi secukupnya daripada kehilangan, disalah guna atau penyelewengan;
2. Meminimumkan kerosakan ke atas aset ICT yang telah dikenal pasti;
3. Menjamin urusan ICT yang lancar serta berterusan; dan
4. Melindungi kepentingan mereka yang bergantung pada teknologi maklumat, daripada kesan kegagalan atau kelemahan ICT dari segi kerahsiaan, integriti, kebolehsediaan dan tidak boleh dipertikaikan.

3.0 SKOP

Merangkumi pelbagai aspek perkakasan dan perisian seperti sistem komputer, data, sistem pengoperasian, pangkalan data dan sistem aplikasi.

4.0 KESELAMATAN SISTEM PENGKOMPUTERAN

4.1 Kawalan Capaian Fizikal

1. Kawalan terhadap individu/staf yang masuk ke bilik komputer dan juga kawalan akses kepada semua sistem pengkomputeran, dan

2. Mewujudkan mekanisme kawalan capaian fizikal untuk staf/individu mencapai sistem pengkomputeran berkenaan.

4.2 Kawalan Capaian Logikal

Kawalan dibuat semasa instalasi agar hanya mereka yang dibenarkan sahaja boleh mencapai sistem. Di antara mekanisme kawalan capaian adalah seperti berikut:

1. Pentadbir sistem terdiri daripada individu atau kumpulan pengguna yang berkongsi akaun kumpulan pengguna yang sama. Pentadbir sistem perlu bertanggungjawab ke atas keselamatan sistem yang digunakan. Di antara langkah-langkah yang diambil oleh pentadbir sistem untuk mengenalpasti pengguna yang sah ialah:
   a. memberi satu ID yang unik kepada setiap pengguna.
   b. menyimpan dan menyelenggara semua ID pengguna yang bertanggungjawab untuk setiap aktiviti;
   c. memastikan adanya pengauditan untuk menyemak semua aktiviti pengguna;
   d. memastikan semua ID pengguna yang diwujudkan adalah berdasarkan permohonan, dan
   e. perubahan ID pengguna untuk sistem aplikasi perlu mendapat kebenaran daripada pemilik sistem tersebut.

2. Bagi memastikan ID pengguna yang tidak aktif tidak disalahgunakan:
   a. menggantung semua kemudahan (*privilege*) ID yang tidak digunakan selama 30 hari.
   b. Membatalkan semua kemudahan untuk pengguna yang berpindah ke agensi lain atau tamatkan perkhidmatan.

c. jejak audit untuk setiap aktiviti pengguna hendaklah disimpan dan diarkib.

3. Pengesahan Pengguna

Proses ini adalah untuk mengenalpasti sama ada pengguna tersebut adalah pengguna yang sah melalui penggunaan kata laluan. Panduan pemilihan dan penggunaan kata laluan adalah seperti berikut:

a. kata laluan dimasukkan dalam bentuk yang tidak boleh dilihat;
b. panjang kata laluan sekurang-kurangnya 8 aksara;
c. merupakan kombinasi daripada aksara, angka dan simbol-simbol;
d. dicadang ditukar sekurang-kurangnya enam (6) bulan sekali;
e. tidak boleh dikongsi oleh pengguna lain;
f. tidak menggunakan kata laluan yang mudah diteka seperti nombor staf, nama pasangan atau anak, nombor plat kereta, dan sebagainya;
g. kata laluan dienkrip semasa penghantaran;
h. fail kata laluan disimpan berasingan daripada data sistem aplikasi utama; dan
i. elakkan dari menggunakan semula 2 kata laluan terakhir.

4. Had Cubaan Capaian

Cubaan capaian dihadkan kepada tiga (3) kali sahaja. ID pengguna berkenaan perlu digantung selepas tiga (3) kali cubaan gagal yang berturut.

4.3 Jejak Audit

Jejak audit adalah rekod aktiviti yang digunakan untuk mengenalpasti akauntabiliti pengguna sekiranya berlaku sebarang masalah. Penggunaan jejak audit untuk sistem komputer dan manual operasi perlu diwujudkan untuk:

1. capaian maklumat yang kritikal;
2. capaian perkhidmatan rangkaian; dan
3. capaian fungsi-fungsi *superuser*.
4. Maklumat jejak audit merangkumi :
    a. identiti pengguna;
    b. fungsi, sumber dan maklumat yang digunakan atau dikemaskini;
    c. tarikh dan masa;
    d. alamat IP di mana capaian dibuat.
    e. transaksi dan program yang dijalankan secara spesifik.

Langkah-langkah keselamatan yang dilakukan dalam menyediakan jejak audit:

1. meneliti dan melaporkan sebarang aktiviti yang diragui dengan segera;
2. meneliti jejak audit secara berjadual;
3. meneliti dan melaporkan sebarang masalah berkaitan keselamatan dan sesuatu kejadian yang di luar kebiasaan;
4. menyimpan maklumat jejak audit untuk jangka masa tertentu untuk keperluan operasi; dan
5. mengawal maklumat jejak audit daripada dihapus dan diubahsuai.

4.4 *Backup*

Bagi memastikan sistem dapat dipulihkan sepenuhnya jika berlaku sebarang masalah atau kerosakan, proses *backup* secara berjadual perlu dilakukan

termasuk apabila berlakunya perubahan konfigurasi pada sistem pengoperasian. Media *backup* perlu disimpan di dalam bilik yang selamat.

Langkah-langkah bagi penyediaan backup ialah:

1. prosedur *backup* dan *restore* didokumenkan;
2. menyimpan 3 generasi *backup*;
3. menyimpan salinan media *backup* di tempat lain yang selamat yang telah dikenal pasti oleh pihak pengurusan Jabatan Infostruktur: dan
4. media *backup* dan prosedur *restore* diuji dua (2) kali setahun.

4.5 Penyelenggaraan

Antara langkah-langkah yang perlu diambil bagi memastikan integriti sistem pengoperasian tidak terdedah kepada sebarang pencerobohan keselamatan:

1. Melaksanakan *patches* bagi mengatasi kelemahan sistem.
2. Dapatkan *patches* yang terkini daripada agensi keselamatan berdaftar seperti MyCERT (*Malaysian Computer Emergency Response Team*) di alamat web http://www.mycert.org.my/ , Microsoft atau syarikat perisian yang berkaitan.
3. Melakukan peningkatan (*upgrades*) perisian dan *firmware*
4. Wujudkan prosedur pengemaskinian sistem pengoperasian daripada serangan dan ancaman.

5.0 KESELAMATAN SISTEM APLIKASI

Semua capaian ke sistem aplikasi mestilah oleh pengguna yang berdaftar. Langkah-langkah pengawalan perlu dilaksanakan bagi menjamin keselamatan sistem.

5.1 Perisian Aplikasi

Di dalam perisian aplikasi, kawalan keselamatan perlu dilaksanakan untuk mengelakkan berlakunya capaian, pengubahsuaian, pendedahan atau penghapusan maklumat oleh pengguna yang tidak sah. Kawalan tersebut merangkumi :

1. Pengurusan ID pengguna secara berpusat;
2. Profil capaian berpandukan peranan dan keperluan capaian;
3. kawalan capaian yang konsisten berdasarkan had capaian pengguna.
4. kawalan aplikasi yang menentukan akauntabiliti tertentu kepada setiap pengguna untuk setiap transaksi.

5.2 Pangkalan Data

Kawalan perlu dilaksanakan untuk menghalang capaian kepada pangkalan data dari sebarang pengubahsuaian atau pemusnahan data secara tidak sah. Integriti maklumat yang disimpan di dalam pangkalan data boleh dikekalkan melalui:

1. Sistem pengurusan pangkalan data yang memastikan integriti dalam pengemaskinian dan capaian maklumat. Kawalan perlu dilaksanakan untuk pangkalan data yang dikongsi bersama;
2. Kawalan capaian kepada maklumat ditentukan oleh Pentadbir Pangkalan Data;
3. Mekanisme kawalan capaian kepada sumber maklumat fizikal dan pelaksanaan tugas-tugas rutin pangkalan data seperti :

    a. semakan *database consistency*
    b. semakan penggunaan ruang storan
    c. pemantauan aktiviti pangkalan data
    d. pemantauan aktiviti server dan pengguna

e. melaksanakan *backup* dan *restore*

f. *performance tuning*.

5.3 Pengujian Aplikasi

Salah satu aspek pembangunan sistem aplikasi ialah pengujian yang dilaksanakan pada beberapa peringkat iaitu pemprograman, modul, sistem aplikasi, integrasi sistem aplikasi dan pengujian pengguna. Ia melibatkan pengujian aplikasi baru, penambahbaikan kepada aplikasi semasa atau pemindahan daripada perkakasan lama kepada baru. Pengujian perlu bagi memastikan sistem berfungsi mengikut spesifikasi yang ditetapkan.

Bagi menghalang maklumat daripada didedah atau diproses secara tidak sepatutnya, persekitaran yang berbeza untuk pembangunan sistem dan pengoperasian sistem perlu diwujudkan. Sekiranya persekitaran berasingan untuk pembangunan sistem tidak dapat dilaksanakan, langkah-langkah berikut hendaklah dilakukan:

1. gunakan data *dummy* atau *historical* untuk tujuan pengujian
2. hapuskan maklumat yang digunakan semasa pengujian sistem (terutamanya apabila menggunakan data *historical*)
3. Menghadkan capaian kepada staf yang dibenarkan semasa ujian dilaksanakan.

5.4 Perisian Yang *Malicious* Dan Rosak (Defektif)

Pembangunan perisian boleh dikategorikan kepada dua iaitu pembangunan secara dalaman (*in-house*) atau *outsourcing*. Kedua-dua keadaan boleh terdedah kepada perisian yang tidak berfungsi sebagai mana ditetapkan. Kerosakan ini boleh dikesan semasa proses pengujian.

Untuk mengurangkan kemungkinan perisian yang defektif, kawalan berikut perlu dilaksanakan:

1. wujudkan program jaminan kualiti untuk semua perisian yang dibangunkan secara dalaman atau luaran.
2. pastikan semua perisian didokumenkan, diuji, disahkan fungsinya, tahan lasak (*robustness*) dan menepati spesifikasi.

5.5 Perubahan Versi

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

5.6 Penyimpanan Kod Sumber (*Source Code*)

Bagi sistem yang diperolehi dari pembekal luar, kod sumber diperlukan untuk tujuan *debugging* dan peningkatan sistem. Kawalan penyimpanan merangkumi:

1. mewujudkan prosedur untuk menyelenggara versi terkini perisian dan
2. mewujudkan perjanjian untuk keadaan di mana berlakunya kerosakan atau bencana dan kod sumber tidak ada.

5.7 Perisian Tidak Berlesen

Perisian tidak berlesen adalah tidak sah. Pastikan penggunaan perisian berlesen dan kawalan inventori direkod dan dikemaskini.

5.8 Kod Jahat (*Malicious Code*)

Bagi memastikan integriti maklumat terpelihara daripada *malicious code* seperti virus, kawalan berikut perlu digunakan:

1. melaksanakan prosedur untuk menguruskan *malicious code*;
2. Mematuhi dasar berkaitan memuat turun, penerimaan dan penggunaan perisian percuma (*freeware* dan *shareware*);
3. menyebarkan arahan dan maklumat untuk mengesan *malicious code* kepada semua pengguna; dan
4. mendapatkan bantuan sekiranya disyaki dijangkiti virus dan lain-lain.

Bagi memastikan keupayaan pemprosesan dapat dipulihkan akibat serangan *malicious code*, beberapa langkah perlu dilaksanakan termasuk:

1. menyimpan semua salinan utama untuk semua perisian, data dan maklumat untuk tujuan *restore*; dan
2. memastikan semua data di *backup* secara berkala.

Bagi masalah serangan virus, ikuti langkah- langkah berikut:

1. gunakan perisian anti virus yang telah diluluskan;
2. scan virus secara berkala.
3. tidak melaksana (*run*) atau membuka fail kepilan daripada *e*- mel yang meragukan.

9

RANGKAIAN

1.0 TUJUAN

Untuk menerangkan pelaksanaan keselamatan rangkaian UiTM bagi tujuan komunikasi dan perkongsian maklumat/sumber termasuk capaian ke internet termasuk rangkaian tanpa wayar.

2.0 OBJEKTIF

1. Keselamatan rangkaian UiTM lebih terjamin.
2. Pengguna dimaklumkan tentang kewujudan Dasar Keselamatan Rangkaian.
3. Mengelakkan ancaman *hacker.*
4. Mengelakkan berlaku tindanan saluran dan menyebabkan gangguan sistem rangkaian tanpa wayar.
5. Sistem rangkaian tanpa wayar dapat berfungsi dengan baik.

4.0 SKOP

Merangkumi semua jenis peralatan komunikasi data berwayar atau tanpa wayar yang bersambung ke rangkaian UiTM dan mampu menghantar peket data.

5.0 REKABENTUK KESELAMATAN RANGKAIAN

Melibatkan rekabentuk keselamatan rangkaian yang mengambil kira perkara-perkara berikut:

1. Matlamat, objektif dan skop keselamatan (sama ada meliputi *end-to-end security, inter-network security* atau keselamatan pada tahap sistem dalaman sahaja).
2. Aset-aset yang perlu dilindungi termasuk jenis-jenis maklumat dan tahap keselamatan yang diperlukan.
3. Menggunakan konsep VLAN (*virtual LAN*) dan sistem rangkaian berhiraki.
4. Potensi ancaman dan serangan keterdedahan serta mewujudkan sistem pencegahan, dasar dan prosedur untuk melindungi maklumat.

6.0 KAWALAN KESELAMATAN RANGKAIAN

Kawalan yang sewajarnya hendaklah diwujudkan untuk memastikan keselamatan data di dalam rangkaian daripada ancaman dalaman dan luaran serta melindunginya daripada capaian tanpa kebenaran.

Peralatan atau perisian bagi tujuan memantau rangkaian hendaklah di pasang seperti *Intrusion Prevention System (IPS)* bagi mengesan sebarang cubaan menceroboh atau aktiviti yang luar biasa. *Intrusion Detection System (*IDS) hanya boleh mengesan aktiviti seperti *ping, scanning, denial of service attack* dan meneka kata frasa yang rapuh.

7.0 KESELAMATAN PERALATAN RANGKAIAN

7.1 Keselamatan Fizikal

1. Peralatan rangkaian ditempatkan di tempat yang bebas daripada risiko di luar jangkaan seperti banjir, gegaran, kekotoran dan sebagainya.
2. Suhu hendaklah terkawal di dalam limit suhu peralatan rangkaian berkenaan.

3. Memasang *Uninterruptible Power Supply (UPS)* dengan minimum 15 minit masa beroperasi jika terputus bekalan elektrik dan menerima bekalan elektrik berkualiti (bekalan elektrik yang bebas daripada *voltage sag*, *voltage swell* dan *transient overvoltages*) bagi pusat data pula, *generator* sebagai alat bantuan *(backup)* hendaklah dipasang dan mempunyai kitaran udara yang baik.

7.2 Keselamatan peralatan tanpa wayar

Semua komputer yang disambungkan ke rangkaian UiTM secara tanpa wayar perlu menepati standard keselamatan yang ditetapkan oleh Jabatan Infostruktur. Data yang dihantar secara tanpa wayar perlu dienkripkan dan pengguna perlu menggunakan *certificate* yang ditetapkan oleh Jabatan Infostruktur.

7.3 Capaian Fizikal

Langkah-langkah sewajarnya perlu diambil untuk melindungi kabel rangkaian daripada di capai oleh orang yang tidak berkenaan.

1. Melindungi pengkabelan di dalam kawasan awam dengan cara memasang *conduit* atau lain-lain mekanisme perlindungan.
2. Pusat pendawaian diletakkan di dalam ruang atau bilik yang berkunci dan hanya boleh dicapai oleh staf yang dibenarkan sahaja; dan
3. Capaian Peralatan Rangkaian
    a. Peralatan hendaklah ditempatkan di lokasi yang selamat dan terkawal; dan
    b. Peralatan rangkaian hanya boleh dicapai oleh staf yang dibenarkan sahaja.

7.4 Capaian Logikal

Kata laluan diperlukan untuk mencapai sistem rangkaian. Capaian hanya boleh dibuat oleh staf yang dibenarkan sahaja.

1. Komposisi kata laluan mestilah konsisten dengan dasar yang telah ditetapkan.
2. Maklumat capaian ke *router* hendaklah direkodkan - Nama pegawai yang melaksanakan capaian, tarikh semasa capaian dilakukan, masa dilakukan dan aktiviti yang dilakukan. Maklumat mestilah disimpan selama 90 hari.
3. Rangkaian hanya menerima trafik daripada alamat IP dalaman yang berdaftar sahaja.
4. Semua perubahan konfigurasi suis rangkaian hendaklah dilogkan termasuk nama pengguna yang membuat perubahan, pengesahan, tarikh dan masa. Maklumat mestilah disimpan selama 90 hari.
5. Perubahan konfigurasi perisian mestilah direkodkan – pegawai yang membuat perubahan, pegawai yang membenarkan perubahan dibuat dan tarikh.
6. Perubahan konfigurasi hendaklah dikendalikan secara berpusat oleh Unit Rangkaian, Jabatan Infostruktur.
7. Semua aktiviti di dalam rangkaian hendaklah direkodkan.

7.5 Konfigurasi Peralatan

Peralatan dikonfigurasi dengan betul dengan mengambil langkah-langkah berikut:

1. *enable* perkhidmatan yang diperlukan sahaja;
2. capaian untuk konfigurasi dihadkan melalui nod atau alamat IP yang dibenarkan sahaja;
3. *disable broadcast*;
4. menggunakan kata laluan yang selamat; dan

5. dilaksanakan oleh staf yang terlatih dan dibenarkan sahaja.

7.6 Penyelenggaraan Peralatan

1. Peralatan hendaklah dipasang, dioperasi dan diselenggarakan mengikut spesifikasi pengilang.
2. Dibaiki dan diselenggara hanya oleh staf yang terlatih dan dibenarkan sahaja.
3. Mempunyai rekod penyelenggaraan.

7.7 Kebolehcapaian Pengguna (*User Accessibility*)

7.7.1 Rangkaian Setempat (*Local Area Network*)

1. Hanya staf dan pelajar UiTM dibenarkan membuat penyambungan ke dalam rangkaian UiTM.
2. Hanya komputer kepunyaan staf dan pelajar UiTM yang dibenarkan untuk disambungkan ke rangkaian UiTM.
3. Pihak ketiga perlu mendapatkan kebenaran daripada Pengarah Jabatan Infostruktur/PTJ/Kampus Negeri sebelum membuat capaian ke rangkaian UiTM.
4. Hanya pengguna yang disahkan sahaja dibenarkan membuat capaian kepada sistem pengkomputeran UiTM.
5. Perisian pengintip (*sniffer*) atau penganalisis rangkaian (*network analyser*) tidak boleh digunakan pada sebarang komputer.

7.7.2 Capaian Yang Tidak Digalakkan

Kurangkan penggunaan protokol rangkaian seperti NetBEUI atau IPX, sebaliknya gunakan TCP/IP dan WINS Server.

8.0 *FIREWALL*

1. Semua trafik daripada dalam ke luar UiTM dan sebaliknya mestilah melalui *firewall*.
2. Hanya trafik yang dibenarkan sahaja boleh melepasinya berasaskan kepada Dasar Keselamatan Rangkaian.
3. Rekabentuk *firewall* hendaklah mengambil kira perkara-perkara berikut:
   a. keperluan audit dan arkib;
   b. kebolehsediaan;
   c. kerahsiaan; dan
   d. melindungi maklumat/UiTM.

9.0 Rangkaian Tanpa Wayar

1. ***Access Point***

   Semua jenis *wireless access point* yang bersambung ke rangkaian UiTM atau tidak bersambung ke rangkaian UiTM perlu mendapat kelulusan pemasangan daripada Pengarah Jabatan Infostruktur/PTJ/Kampus Negeri.

2. **Enkripsi dan Authentikasi**

   Semua komputer yang disambungkan ke rangkaian UiTM secara tanpa wayar perlu menepati standard keselamatan yang ditetapkan oleh Jabatan Infostruktur. Data yang dihantar secara tanpa wayar perlu dienkripkan dan pengguna perlu menggunakan *certificate* yang ditetapkan oleh Jabatan Infostruktur.

3. **SSID**

   SSID yang digunakan di UiTM Shah Alam ialah “uitmsalam” manakala di kampus cawangan adalah berdasarkan SSID yang telah disahkan oleh Bahagian ICT Kampus Cawangan.

10.0 Pembukaan *Port* dan *Service* (Untuk Aplikasi)

1. Unit Rangkaian, Jabatan Infostruktur bertanggungjawab sepenuhnya mengawal selia capaian melalui port yang dibuka ke semua sistem dalam rangkaian UiTM.
2. Unit Rangkaian, Jabatan Infostruktur berhak menutup port yang memudaratkan keselamatan rangkaian UiTM.
3. Kelulusan daripada Pengarah Jabatan Infostruktur perlu diperolehi jika pengguna ingin membuka port tertentu yang dalam sistem rangkaian UiTM untuk aplikasi tertentu.
4. Pentadbir sistem aplikasi bertanggungjawab ke atas keselamatan sistem. Penggunaan port yang dibuka bagi tujuan web server, FTP, telnet dan servis yang berkaitan aplikasi adalah tanggungjawab pentadbir sistem.

10

PENGGUNAAN EMEL

1.0 TUJUAN

Seksyen ini menerangkan peraturan penggunaan *e-mel* UiTM.

2.0 SKOP

Ia melibatkan penggunaan kemudahan *e-mel* UiTM dan bukan UiTM. Seksyen ini terbahagi kepada dua bahagian, iaitu Penggunaan Am untuk peraturan am penggunaan semua aplikasi *e-mel* bukan UiTM seperti yahoo mail, gmail dll. dan penggunaan *e-mel* rasmi UiTM.

3.0 PENYATAAN

E-Mail rasmi UiTM perlu menggunakan nama domain:
<nama>@<lokasi>.uitm.edu.my

4.0 PENGGUNA

Kemudahan *e-mel* disediakan seperti berikut:-

1. Semua staf UiTM melalui permohonan;
2. Semua Pelajar UiTM yang berdaftar
3. Jabatan atau persatuan rasmi UiTM melalui permohonan.

5.0 KESELAMATAN PENGGUNAAN E-MEL

5.1 Akaun *E-mel*

Pendedahan akan membolehkan pengguna lain menyalahgunakan kemudahan tanpa pengetahuan pemilik akaun.

1. Akaun *e-mel* bukan hak mutlak seseorang. Ia adalah kemudahan yang disediakan tertakluk kepada peraturan UiTM dan boleh ditarik balik jika penggunaannya melanggar peraturan.
2. Gunakan akaun *e-mel* milik pengguna. Pengguna tidak dibenarkan menggunakan akaun *e-mel* milik orang lain atau akaun yang dikongsi bersama untuk mengemukakan pendapat persendirian. Pengguna juga tidak digalakkan menggunakan akaun yang didaftarkan secara percuma untuk penghantaran *e-mel* rasmi.
3. Kata laluan tidak boleh didedahkan kepada pengguna lain.

5.2 Menyelenggara Kotak Mel (Mail Box)

1. Kandungan dan penyelenggaraan kotak mel adalah tanggungjawab pengguna.
2. Pengguna harus menghadkan jumlah *e-mel* yang disimpan di dalam kotak mel. Hapuskan *e-mel* yang difikirkan tidak perlu disimpan.
3. Pengguna hendaklah memastikan fail yang dihantar melalui lampiran bebas daripada virus
4. *e-mel* tidak boleh mengandungi maklumat rahsia yang boleh disalah guna.

5.3 Penggunaan Perisian Mel

1. Pengguna digalakkan mengguna perisian mel rasmi UiTM.
2. Pengguna yang tidak menggunakan perisian mel rasmi UiTM dinasihatkan sentiasa membuat *backup* terhadap data-data emel.

6.0 PENGGUNAAN AM

Pengguna *e-mel* perlu mematuhi perkara-perkara berikut:

1. Perisian-perisian berlesen dan mempunyai hakmilik terpelihara atau intelek tidak boleh disebarkan melalui e-mel individu atau organisasi;
2. Aktiviti *spamming* atau *mail-bombing* dan penyebaran e-mel dengan kandungan tidak beretika (seperti lucah, ugutan, perkauman dan gangguan) kepada individu, *mailing list* atau *discussion groups* sama ada di dalam rangkaian setempat (LAN) UiTM atau ke rangkaian luas (WAN) dan Internet oleh pengguna adalah tidak dibenarkan;
3. UiTM berhak memasang sebarang jenis perisian atau perkakasan penapisan *e-mel* dan virus (*email filter* dan *anti virus*) yang difikirkan sesuai dan boleh menggunakannya untuk mencegah, menapis menyekat atau menghapuskan mana-mana *e-mel* yang disyaki mengandungi virus atau berunsur *Spamming* daripada memasuki ke dalam server, stesen kerja atau rangkaian setempat (LAN) UiTM dan keluar daripada server, stesen kerja atau rangkaian setempat (LAN) UiTM.
4. UiTM tidak bertanggungjawab secara langsung atau tidak langsung terhadap pengguna yang menjadi penghantar (*sender*) atau penerima (*receiver*) kepada sebarang *e-mel* yang berunsur spamming atau penyebaran *e-mel* dengan kandungan tidak beretika (seperti lucah, ugutan,

perkauman dan gangguan) sama ada secara disedari/sengaja atau tidak disedari/sengaja olehnya.

5. UiTM tidak bertanggungjawab secara langsung atau tidak langsung terhadap sebarang kerosakan, kehilangan atau sebarang kesan lain kepada maklumat, aplikasi, data, kotak e-mel atau fail yang disimpan oleh pengguna didalam stesen kerja atau server akibat daripada penggunaan perkhidmatan *e-mel*.

6. Untuk keselamatan penggunaan, perkara berikut perlu diberi perhatian oleh pengguna:

   a. tukar kata laluan secara berkala (dicadangkan setiap 6 bulan) bagi mengelakkan akaun e-mel diceroboh;

   b. tidak berkongsi kata laluan dengan pengguna lain dan tidak melayan mana-mana permintaan untuk mendapat kata laluan;

   c. berhati-hati ketika menerima fail kepilan (attachments). Fail kepilan mungkin mengandungi '*letterbombs*' atau virus yang boleh merosakkan komputer dan rangkaian UiTM. Fail kepilan yang sering mengandungi virus ialah fail yang mempunyai "extension" '.exe', '.zip', 'pif', '.scr' dan sebagainya.

   d. *'log out'* setelah selesai sesi penggunaan *e-mel* bagi menyelamatkan akaun dari pencerobohan atau tutup 'browser' yang digunakan setelah sesi capaian *e-mel* selesai;

   e. tidak menjawab *e-mel* yang tidak berkenaan (seperti '*spam'*, ugutan atau ofensif) kerana dengan menjawab *e-mel* yang sedemikian, pengguna mendedahkan diri kepada aktiviti yang tidak bertanggungjawab. Pengguna bertanggungjawab melapor penerimaan *e-mel* sedemikian kepada pentadbir *e-mel* Jabatan Infostruktur/PTJ/Kampus Negeri.

6.0 PENGGUNAAN KHUSUS

1. Alamat *e-mel* yang diberikan oleh UiTM kepada pengguna individu atau jabatan/persatuan adalah muktamad dan ditentukan oleh UiTM. Pengguna tidak dibenarkan untuk memohon penukaran alamat e-mel.
2. Pengguna diberikan ruangan storan *e-mel* 1 GB sahaja.
3. Seseorang pengguna individu tidak dibenarkan untuk memohon dan memiliki lebih dari satu akaun atau alamat *e-mel* UiTM pada satu-satu masa.
4. Setiap alamat *e-mel* yang disediakan adalah untuk kegunaan individu atau jabatan/persatuan berkenaan sahaja. Ia tidak boleh digunakan oleh pihak lain sama ada dengan kebenaran atau tanpa kebenaran.
5. Pengguna dilarang menggunakan kemudahan *e-mel* untuk sebarang aktiviti yang tidak dibenarkan oleh peraturan dan undang-undang UiTM dan negara.
6. Semua pengguna yang diberi kemudahan *e-mel* UiTM tidak dibenarkan mengguna *e-mel* luar (seperti *hotmail, yahoo* dan lain-lain) untuk tujuan rasmi. Pentadbir Rangkaian berhak menghalang penggunaan *e-mel* tersebut jika didapati memudarat dan membebankan rangkaian UiTM;
7. Di dalam kes sistem tergendala (rosak), pihak pentadbir mel hanya bertanggungjawab untuk memulihkan kembali (*restore*) maklumat akaun pengguna dan bukannya kandungan/kotak *e-mel* (*mailbox*) pengguna;
8. Atas keperluan audit, keselamatan dan penggunaan, pentadbir *e-mel* berhak memeriksa dan melihat isi kandungan *e-mel* dan ruang storan pengguna-pengguna; dan
9. Pengguna bertanggungjawab sepenuhnya di atas penggunaan perisian *e-mel.*

7.0 PERMOHONAN

Permohonan untuk mendapatkan kemudahan *e-mel* boleh dibuat oleh staf UiTM dengan cara mengisi Borang Permohonan *e-mel* Individu atau secara elektronik. Manakala Jabatan dan persatuan rasmi UiTM boleh memohon kemudahan *e-mel* dengan cara mengisi Borang Pemohonan *E-Mel* Jabatan & Persatuan iaitu yang boleh diperolehi di PTJ/Kampus Negeri atau melalui laman web rasmi UiTM. Borang yang telah lengkap diisi hendaklah dimajukan kepada PTJ/Kampus Negeri.

Permohonan yang telah diluluskan akan dikembalikan kepada pemohon dengan disertakan maklumat alamat *e-mel* dan kata laluan.

8.0 PENAMATAN KEMUDAHAN

UiTM boleh menamatkan kemudahan akaun *e-mel* yang telah diberikan kepada staf dan pelajar atas sebab-sebab berikut:-

1. Staf telah tamat atau ditamatkan perkhidmatan dengan UiTM secara rasmi;
2. Pelajar telah tamat atau ditamatkan pengajiannya di UiTM secara rasmi;
3. Jabatan atau Persatuan yang telah dibubar secara rasmi oleh pihak pengurusan UiTM;
4. Permintaan dari staf atau pelajar sendiri untuk menamatkan perkhidmatan tersebut; dan
5. Staf atau pelajar yang tidak bersetuju atau melanggar syarat-syarat di dalam Dasar Penggunaan *E-Mel*.

11

MEMBANGUN LAMAN WEB DAN TAPAK HOSTING

1.0 TUJUAN

Seksyen ini bertujuan menyelaras dan mengawasi pembangunan laman web yang dibangunkan oleh pengguna untuk tujuan laman web peribadi bersesuaian seperti mana yang dikehendaki oleh UiTM.

2.0 SKOP

Melibatkan semua pembangunan laman web persendirian yang dibangunkan oleh staf UiTM.

3.0 PENYATAAN

1. UiTM menggalakkan warga kampus membangunkan laman web, tetapi hanya laman web rasmi Jabatan/Bahagian/Fakulti/Kampus Negeri atau seumpamanya sahaja yang boleh dipautkan dalam laman web rasmi UiTM.

2. Pengguna atau pemilik laman web adalah bertanggungjawab sepenuhnya terhadap semua kandungan. Pihak UiTM tidak akan bertanggungjawab terhadap kandungan dan sebarang penyalahgunaan hakcipta yang dilakukan oleh pemilik laman web.

3. Jabatan Infostruktur berhak menentukan perisian pembangunan laman web bagi tujuan pengoptimumkan penggunaan dan keselamatan.

4. Keselamatan maklumat dan penyiaran adalah di bawah tanggungjawab individu (pembina laman web) atau PTJ/Kampus Negeri dan perlu mengambil kira aspek keselamatan daripada pencerobohan pihak luar.
5. Laman web peribadi hendaklah berbentuk ilmiah dan bagi tujuan akademik.
6. Laman web yang berunsur politik, perniagaan dan pengiklanan adalah tidak di benarkan sama sekali.
7. Pengiklanan komersial seperti *banner*, *Ads Adsense Google* atau mana-mana yang seumpamanya adalah tidak dibenarkan sama sekali diletakkan di dalam laman web individu.
8. Kandungan laman web tidak boleh mengandungi maklumat yang menyalahi undang-undang / peraturan UiTM, negeri dan negara. Ini termasuk (tetapi tidak terhad kepada) maklumat yang berbentuk politik, keganasan, lucah, hasutan dan yang boleh menimbul atau membawa kepada keganasan, keruntuhan akhlak dan kebencian.
9. Tidak memberi atau membenarkan dengan sengaja orang perseorangan atau individu lain mengendalikan laman web peribadi di atas identiti pemilik.
10. Pemilik laman web dilarang menggunakan laman web yang dibangunkan sebagai jalan keluar *(proxy)* kepada laman web lain yang berada di luar terutamanya yang menyebabkan kerosakan kepada pihak lain atau UiTM.
11. UiTM berhak menamatkan mana-mana laman web peribadi yang melanggar syarat-syarat yang dinyatakan tanpa sebarang notis.
12. Pemilik laman web perlu membuat salinan atau *backup* terhadap laman web mereka sendiri.

13. Jabatan Infostruktur tidak bertanggungjawab ke atas sebarang kerosakan atau kehilangan maklumat pada *server* sehingga menyebabkan berlakunya kegagalan capaian maklumat.

4.0 PENGGUNAAN HOS MAYA (*VIRTUAL HOSTING*)

1. Setiap pengguna diberikan maksima 500Mb – 1000Mb ruang storan di server induk dan bergantung kepada keperluan mengikut PTJ.
2. Setiap pengguna/pemilik bertanggungjawab terhadap penggunaan tapak yang dihoskan, khususnya terhadap maklumat yang disebarkan secara elektronik melalui laman web mereka dan mempunyai backup terhadap segala maklumat yang dihoskan.
3. Sebarang masalah yang berkaitan dengan tahap penghantaran dan penerimaan data bagi tapak hos hendaklah dirujuk kepada Jabatan Infostruktur/PTJ/Kampus Negeri untuk tindakan selanjutnya.
4. Pengguna/pemilik tapak tidak dibenarkan merosakkan sistem komputer atau data dengan apa jua cara seperti pengedaran virus komputer melalui tapak yang dihoskan.
5. Jika didapati bahawa sumber maklumat UiTM telah disalahgunakan atau tidak mengikut peraturan yang ditetapkan, Jabatan Infostruktur boleh menghadkan atau membatalkan akses kepada tapak hos tersebut dan seterusnya menamatkan perkhidmatannya.

12

PENGURUSAN SISTEM APLIKASI DAN PANGKALAN DATA

1.0 TUJUAN

Seksyen ini adalah untuk memastikan pengurusan sistem aplikasi dan pangkalan data adalah berdasarkan *Enterprise Architecture* dan selari dengan hala tuju strategik universiti bagi mengelakkan pertindanan serta memperjelaskan peranan dan tanggungjawab pihak pemilik sistem dan Jabatan Infostruktur seterusnya meningkatkan kebolehgunaan dan kebolehpercayaan serta integriti dan kebolehsediaan sistem aplikasi dan pangkalan data.

2.0 OBJEKTIF

1. Memastikan semua PTJ/Kampus Negeri menggunakan perisian pengajaran dan pembelajaran yang selaras di kampus negeri dan di kampus induk.
2. Penjimatan kos perisian.
3. Penyelarasan perolehan perisian secara berpusat.
4. Penyelarasan penyelenggaraan perisian secara berpusat.
5. Kemudahan pembelajaran dan pengajaran dengan versi yang terkini bagi perisian yang diselenggara secara kontrak.
6. Memastikan sistem aplikasi yang dibangunkan tidak menduplikasi sistem sedia ada.

3.0 SKOP

Merangkumi semua pembangunan sistem aplikasi, perisian yang dimiliki, diguna atau berada di dalam simpanan staf, bagi tujuan staf dan hal-hal berkaitanUiTM, tidak kira di mana perisian itu berada.

4.0 PENYATAAN

4.1 Perjanjian Lesen Perisian (*Software Licence Agreements*)

1. Semua staf tidak dibenarkan melanggar mana-mana perjanjian lesen perisian atau lesen perkakasan yang telah ditetapkan oleh pembangun (*developer*) bagi perisian tersebut.
2. Semua staf tidak dibenarkan membuat salinan (*copy*) sama ada dalam bentuk media (CD/DVD/Thumb Drive) atau pun apa jua kaedah yang bertujuan memindah, menyalin, menyebarkan dan membuat instalasi mana-mana perisian yang diberikan oleh Jabatan Infostruktur/PTJ/Kampus Negeri melebihi jumlah lesen yang ditetapkan.
3. Jabatan Infostruktur/PTJ/Kampus Negeri tidak akan bertanggungjawab terhadap sebarang penyalahgunaan perisian, termasuk penggunaan perisian tanpa lesen yang dilakukan oleh staf.
4. Setiap staf secara peribadi bertanggungjawab untuk membaca, memahami dan mematuhi peraturan penggunaan dan syarat-syarat perlesenan bagi setiap perisian yang digunakan.
5. Setiap staf tidak dibenarkan memuat turun dan membuat instalasi perisian yang boleh mendatangkan kemudaratan dan kerosakan kepada komputer serta gangguan kepada rangkaian UiTM.
6. Setiap staf tidak dibenarkan memuat turun dan membuat instalasi perisian-perisian yang tidak relevan dengan keperluan akademik, pentadbiran dan kaji selidik di UiTM.

4.2. Hak milik

1. Semua perisian yang diperolehi untuk atau bagi pihak UiTM atau semua perisian yang dibangunkan oleh staf atau pelajar UiTM untuk tujuan pengajaran, pembelajaran, penyelidikan, perundingan atau pentadbiran adalah menjadi hak milik UiTM.
2. Bagi perisian yang dibangunkan secara *Joint Venture (JV)* di antara UiTM dengan pembekal, kontraktor atau syarikat ICT di mana UiTM membayar kos pembangunan perisian tersebut kepada pembekal, kontraktor atau syarikat berkenaan, maka perisian ini dianggap sebagai hak milik UiTM. Semua kod sumber (*source code*) bagi perisian tersebut adalah menjadi hak milik UiTM.
3. Bagi perisian yang dibangunkan, maklumat tentang semua pengarang/pencipta mestilah dikekalkan.
4. Semua perisian hakmilik UiTM tidak dibenarkan dijual, disewa, dilesenkan semula, dipinjam, disebar atau diberi kepada sesiapa atau entiti tanpa kebenaran bertulis CIO.

5.0 KELULUSAN PENGGUNAAN

Semua jenis perisian yang diguna pakai oleh Jabatan Infostruktur/PTJ/Kampus Negeri perlu mendapat kelulusan daripada pihak pembekal atau pembangun perisian dan diguna mengikut syarat-syarat yang ditetapkan oleh pihak pembekal atau pembangun.

6.0 PENGGUNAAN PERISIAN YANG DIGUNAKAN UNTUK TUJUAN PENGAJARAN DAN PEMBELAJARAN

1. PTJ/Kampus Negeri bertanggungjawab sepenuhnya terhadap semua keperluan perisian yang digunapakai untuk tujuan pengajaran dan pembelajaran di PTJ dan kampus negeri masing-masing.

2. Penggunaan perisian bagi subjek yang sama di seluruh UiTM perlu menggunakan perisian dari modul dan versi yang sama.

7.0 PEMBANGUNAN PERISIAN APLIKASI YANG MEMPUNYAI PERTINDANAN FUNGSI SISTEM SEDIA ADA

1. Pembangunan aplikasi yang mempunyai pertindanan fungsi sistem sedia ada seperti STARS, FAIS, iSIS dan sebagainya adalah TIDAK DIBENARKAN.
2. Sebarang keperluan pembangunan perisian yang melibatkan perubahan proses perlu dirujuk kepada pemilik proses. Pemilik proses perlu meneliti keperluan dan majukan kepada pihak Jabatan Infostruktur untuk tindakan.

8.0 PEMBANGUNAN SISTEM APLIKASI

Sebarang sistem aplikasi yang perlu dibangunkan hendaklah dirujuk dan dibincang terlebih dahulu dengan Jabatan Infostruktur (Rujuk Pekeliling Naib Canselor Bil 7/2006 bertarikh 29 Mac 2006).

8.1. Katalog Sistem Aplikasi

UiTM akan menyimpan daftar terkini sistem aplikasi yang digunakan secara rasmi di seluruh universiti.

8.2. Pemilikan Sistem Aplikasi

Setiap sistem aplikasi mesti mempunyai pemilik yang bertanggungjawab terhadap proses kerja sistem berkenaan.

8.3. Permohonan Sistem Aplikasi atau Perubahan

Permohonan atau cadangan sistem aplikasi baru atau perubahan terhadap sistem aplikasi sedia ada mesti dimajukan kepada Jabatan Infostruktur/PTJ/Kampus

Negeri dan mematuhi prosedur yang telah ditetapkan oleh Jabatan Infostruktur, UiTM. Kelulusan dan pendekatan pembangunan projek sistem aplikasi adalah tertakluk kepada hasil kajian yang akan dilakukan.

8.4. Pembangunan Sistem

Pembangunan sistem aplikasi, sama ada oleh pihak PTJ/Kampus Negeri mesti mematuhi *Enterprise Architecture Blueprint* UiTM dan mematuhi prosedur yang telah ditetapkan.

8.5. Penyerahan Sistem Aplikasi daripada Pihak Ketiga

Sistem Aplikasi (yang dibangunkan oleh pihak ketiga) yang ingin diserahkan kepada pihak PTJ/Kampus Negeri untuk diselenggara mestilah lengkap dengan dokumen berikut:

1. Spesifikasi Keperluan Pengguna (SRS)
2. Definisi RekaBentuk Sistem (SDD)
3. Manual Operasi
4. Manual Pengguna

8.6. Cadangan Penggunaan Sistem Aplikasi daripada Pihak Ketiga

Cadangan penggunaan sistem aplikasi daripada pihak ketiga mesti dimajukan kepada pihak Jabatan Infostruktur/PTJ/Kampus Negeri dan mematuhi prosedur yang telah ditetapkan. Kelulusan penggunaan sistem aplikasi adalah tertakluk kepada hasil kajian yang akan dilakukan.

8.7. *Retirement* Sistem Aplikasi

Sistem Aplikasi yang tidak digunakan lagi mesti diarkibkan dan dikeluarkan daripada persekitaran ICT universiti. Arahan menamatkan penggunaan sistem aplikasi mesti diberikan oleh pemilik proses sistem berkenaan.

8.8. Kawalan Akses Sistem

Kawalan akses kepada system mesti ditentukan oleh pemilik proses sistem berkenaan dan mematuhi DKICT Universiti.

8.9. Kandungan Sistem dan Kualiti Data

Pemilik dan pengguna sistem aplikasi bertanggungjawab terhadap kualiti data bagi sistem yang digunakan.

8.10. Penyelenggaraan, sokongan & latihan

1. Sistem yang diselenggara mesti diuji sebelum digunakan. Pengguna mesti dimaklumkan dan diberi latihan yang sesuai.
2. Dokumentasi sistem mesti dikemaskini.
3. Persetujuan sokongan dan selenggaraan mesti didokumenkan di dalam *Service Level Agreement* (SLA)/*Organization Level Agreement* (OLA).

9. PANGKALAN DATA

9.1. Standard

Pemilik pangkalan data bertanggungjawab menyediakan, mengesahkan dan memelihara semua proses dan prosedur yang didokumenkan untuk menyokong standard yang ditetapkan dalam dokumen Standard Pengurusan Pangkalan Data. Semua dokumentasi mesti dikaji dan disahkan oleh pengurusan pihak PTJ/Kampus Negeri.

9.2. Pemilihan Perisian Pangkalan Data

Pemilihan perisian pangkalan data (DBMS) adalah berdasarkan kepada standard yang dinyatakan dalam Standard Pengurusan Pangkalan Data.

9.3. Pangkalan Data Berpusat

1. Pentadbir pangkalan data perlu dilantik untuk mengurus pengkalan data.
2. Semua pangkalan data berpusat dan pemilik sistem dilantik sebagai pentadbir pangkalan data yang bertanggungjawab mesti dilaporkan di Pejabat CIO.

9.4. Keselamatan Pangkalan Data

Dasar keselamatan dan standard mestilah selaras dengan dasar dan standard yang ditakrifkan dalam DKICT.

Semua pengendalian pangkalan data mesti mematuhi Garis Panduan Pengkelasan dan Pengendalian Data & Maklumat.

9.5. Pengurusan *Backup & Recovery*

Operasi *Backup & Recovery* Pangkalan Data mesti mematuhi prosedur yang telah ditetapkan.

.

13

PENGURUSAN PERKHIDMATAN SERVER (PELAYAN)

1.0 TUJUAN

Seksyen ini menerangkan peraturan dan perkara yang perlu dipatuhi untuk pengoperasian server untuk memastikan server tersebut diselenggara dan dipasang dengan sedemikian rupa untuk mengelakkan daripada ia dicerobohi atau dicapai oleh individu yang tidak sepatutnya.

2.0 HAK MILIK

Semua server yang diperoleh mengikut tatacara perolehan atau sumbangan daripada mana-mana pihak adalah menjadi hak milik UiTM sepenuhnya.

3.0 TANGGUNGJAWAB

Semua PTJ/Kampus Negeri yang membuat pembelian server adalah bertanggungjawab sepenuhnya kepada server tersebut. Tanggungjawab ini boleh dipecahkan kepada:

1. Pemilik

Pemilik adalah PTJ/Kampus Negeri yang membuat perolehan kepada sesuatu server. Pemilik adalah bertanggungjawab bagi memastikan server di bawah pengawasannya berada di dalam keadaan baik. Setiap PTJ/Kampus Negeri dinasihatkan agar melantik seorang staf yang mempunyai kemahiran teknikal yang berkaitan bagi menguruskan server yang dimilikinya. Pengurusan server oleh PTJ/Kampus Negeri adalah tertakluk kepada Dasar

Keselamatan Universiti Teknologi MARA serta undang-undang yang dikuatkuasakan dari semasa ke semasa.

2. Pentadbir Sistem

Pentadbir Sistem bertanggungjawab memastikan server diurus dan ditadbir dengan betul serta memenuhi keperluan pemilik server dan dasar yang dilaksanakan. Pentadbir adalah bertanggungjawab sepenuhnya ke atas keselamatan data dan sistem di dalam server.

4.0 PENYATAAN

Setiap PTJ/Kampus Negeri atau penyedia server perlu mematuhi peraturan-peraturan berikut:

1. Pentadbir sistem perlu memastikan keselamatan server daripada pencerobohan. Ini termasuk tetapi tidak terhad kepada membuat pemeriksaan ke atas proses tersembunyi (hidden processes), *daemons*, mengemaskini perisian seperti e-mel dan laman web, dan mengenal pasti pengguna-pengguna. Jabatan atau penyedia server boleh menyedia *firewall* khusus untuk tujuan ini;
2. Pentadbir sistem perlu mengenal pasti tahap capaian pengguna dan penggunaan server secara jelas. Ini akan menghasilkan capaian yang lebih terkawal;
3. Server yang melibatkan penyimpanan maklumat yang penting dan kritikal perlu mempunyai *backup* yang lengkap untuk mengelak kehilangan maklumat dan mengurangkan masa *downtime.* Urusan operasi *backup* adalah di bawah tanggung jawab Unit Pusat Data/Pusat Pemulihan Bencana dan Pentadbir sistem;

4. Server yang digunakan untuk projek pelajar perlu mendapat kelulusan daripada penyelia projek / Dekan. Alamat IP dalaman statik digunakan untuk server ini. Alamat IP global boleh diberi kepada projek yang memerlukan capaian Internet;
5. Semua Pentadbir sistem yang dipertanggungjawabkan 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 Sistem dan Pusat Data/Pusat Pemulihan Bencana; dan
c. Pentadbir Sistem di Jabatan bertanggungjawab memastikan server tidak disalah guna untuk tujuan yang bukan sepatutnya.

5.0 PENGURUSAN KATA LALUAN SERVER

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

Dalam apa jua keadaan dan sebab, kata laluan bagi peralatan ICT UiTM hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; walaubagaimanapun, bagi kata laluan untuk server, ianya akan disimpan di dalam peti besi dan hanya boleh dicapai oleh tiga orang yang disenaraikan apabila diperlukan.

Tiga orang yang disenaraikan adalah;

a. Pengarah Jabatan Infostruktur
b. Ketua Bahagian Pengurusan Sistem, Jabatan Infostruktur

c. Ketua Unit Pusat Data/Pusat Pemulihan Bencana

6.0 PERMOHONAN PENEMPATAN SERVER DI PUSAT DATA/PUSAT PEMULIHAN BENCANA UNIVERSITI

Setiap server yang ingin diletakkan di Pusat Data/Pusat Pemulihan Bencana perlu mendapat kelulusan Ketua Unit Pusat Data/Pusat Pemulihan Bencana dengan mengisi borang yang disediakan oleh Unit Pusat Data. Pembekal / Pegawai TanggungJawab diminta menyediakan beberapa perkara iaitu:

1. Railing Kit
2. Power Cord (C13 atau C19)
3. KVM Conventer
4. Salinan Borang Harta Benda KEW312
5. Pegawai yang dihubungi jika berlaku kecemasan

7.0 PELANGGARAN PRINSIP UTAMA

Sebarang pelanggaran prinsip utama yang berlaku boleh mengakibatkan salah satu daripada perkara-perkara berikut bergantung kepada tahap masalah tersebut:

1. Bagi masalah keselamatan, server akan ditutup sementara sehingga tahap keselamatan server ditingkatkan ke tahap yang sewajarnya.
2. Penyambungan server ke rangkaian akan ditutup.
3. Penutupan operasi server.
4. Peringatan kepada pentadbir atau pemilik akan dikeluarkan jika didapati server digunakan untuk aktiviti yang bukan berkaitan urusan rasmi Universiti.

14

PENGURUSAN AKSES KE PUSAT DATA/PUSAT PEMULIHAN BENCANA UTAMA UITM

1.0 PENGENALAN

Ia adalah untuk memastikan keselamatan dan kerahsiaan maklumat serta data-data Universiti dengan menghadkan akses ke Pusat Data/Pusat Pemulihan Bencana.

2.0 KEBENARAN DAN PENERIMAAN

Akses ke Pusat Data/Pusat Pemulihan Bencana perlu mendapat kebenaran daripada Ketua Unit Pusat Data/Pusat Pemulihan Bencana, atau Ketua Bahagian Pengurusan Sistem, Jabatan Infostruktur atau Pengarah Jabatan Infostruktur.

3.0 PENYATAAN

Akses ke Pusat Data/Pusat Pemulihan Bencana universiti terhad kepada staf operasi Unit Pusat Data/Pusat Pemulihan Bencana/Pusat Pemulihan Bencana dan staf tertentu sahaja (Mempunyai keperluan akses ke Pusat Data/Pusat Pemulihan Bencana secara kerap dan telahpun mendapat kebenaran dari Ketua Unit Pusat Data/Pusat Pemulihan Bencana/ Ketua Bahagian Pengurusan Sistem/ Pengarah Jabatan Infostruktur.

1. Pihak ketiga yang memerlukan akses ke Pusat Data/Pusat Pemulihan Bencana untuk melaksanakan kerja –kerja penyelenggaraaan perlulah diiringi oleh Staf Operasi Pusat Data/Pusat Pemulihan Bencana.
2. Lawatan dari mana-mana agensi luar/Pelajar ke Pusat Data/Pusat Pemulihan Bencana perlulah terlebih dahulu membuat permohonan rasmi melalui surat dengan menyatakan tujuan lawatan kepada Ketua Unit Pusat Data/Pusat Pemulihan Bencana/ Ketua Bahagian Pengurusan Sistem/ Pengarah Jabatan Infostruktur.
3. Dalam keadaan kecemasan, kebenaran akses ke Pusat Data/Pusat Pemulihan Bencana oleh staf akan diberikan dan dikoordinasikan oleh Ketua Unit Pusat Data/Pusat Pemulihan Bencana bertanggungjawab tanpa mengira waktu dan masa. Apabila terdapat keperluan untuk membuka pintu Pusat Data/Pusat Pemulihan Bencana yang disebabkan oleh kecemasan, Ketua Unit Pusat Data/Pusat Pemulihan Bencana yang bertanggungjawab perlu:-
    a. Mengesahkan situasi kecemasan yang berlaku
    b. Mengesahkan dan mengenalpasti individu yang memohon akses dan kaitan dalam menyelesaikan masalah kecemasan tersebut (e.g. *police responding to a bomb threat, firefighters responding to a fire alarm, HVAC personnel responding to a temperature alarm,* etc.);
    c. Merekodkan maklumat (tarikh, masa, nama , sebab dan sebagainya)
    d. Makluman berkaitan dengan insiden perlulah dilaporkan kepada Ketua Polis bantuan UiTM dan Pengarah Jabatan Infostruktur.

15

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1.0 TUJUAN

Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pengguna apabila berlaku gangguan atau bencana.

2.0 GANGGUAN/ BENCANA

Gangguan atau bencana adalah akibat dari kejadian yang menyebabkan kegagalan penyampaian perkhidmatan Kerajaan. Gangguan atau bencana yang berlaku di Malaysia adalah akibat dari kejadian-kejadian seperti berikut:

1. Bencana alam seperti banjir, gempa bumi, tanah runtuh, kemarau, kebakaran hutan, ribut petir, ribut tropika, luruan ribut, tsunami dan wabak penyakit;
2. Gangguan yang tidak dirancang atau disengajakan seperti kebakaran,keganasan, sabotaj, kecurian, vandalisme dan tunjuk perasaan;
3. Gangguan kepada perkhidmatan dan utiliti seperti bekalan elektrik, air, gas, komunikasi dan pengangkutan awam; dan
4. Gangguan akibat serangan siber seperti pencerobohan, virus, *Distributed Denial of Service* (DDoS), kegagalan sistem ICT termasuk aplikasi, rangkaian dan perkakasan.

3.0 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN (PKP)

3.1. Pelan ini mestilah **diluluskan dan disahkan** oleh Jawatankuasa Pengurusan Insiden dan Risiko UiTM dan Lembaga Pengurusan Insiden dan Risiko UiTM.

3.2. Perkara yang perlu dipatuhi dan diberi perhatian oleh PTJ dan Pentadbir Sistem yang dipertanggungjawabkan berkenaan pelaksanaan PKP adalah seperti berikut :

1. Mewujudkan atau menurunkuasa kepada jawatankuasa berkaitan untuk menguruskan pelan kesinambungan perkhidmatan
2. Mengenalpasti *core business* dan proses-proses kritikal di Universiti serta menyediakan senarai keutamaan proses yang mengambil kira keperluan perkhidmatan universiti.
3. Melaksanakan penilaian risiko bagi menentukan tahap keselamatan dalam menyediakan strategi perlaksanaan PKP.
4. Mendapatkan sokongan padu dan komitmen daripada Lembaga Pengarah Universiti.
5. Mewujudkan Pusat Pemulihan Bencana sebagai lokasi alternatif untuk kesinambungan perkhidmatan Universiti apabila berlaku bencana.
6. Melantik Ketua Pegawai Maklumat (CIO) atau Penolong sebagai peneraju PKP.
7. Melantik Koordinator PKP dan pasukan PKP bagi melaksanakan PKP Universiti.
8. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;

9. Keperluan keselamatan maklumat dibangunkan untuk mengurus dan selenggara proses formal untuk mengawal pelaksanaan perubahan;
10. Memastikan kawalan keselamatan ke atas pusat data diberi keutamaan bagi menjamin keselamatan data.
11. Peraturan untuk menangani gangguan ke atas penyediaan perkhidmatan dengan mengenal pasti keadaan tersebut, kebarangkalian berlaku dan kesan sekiranya berlaku;
12. Merancang dan melaksana peraturan kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;
13. Hanya satu rangka pelan kesinambungan perkhidmatan yang menyeluruh dibangunkan, didokumentasikan, dipersetujui oleh pengurusan dan diselenggarakan untuk seluruh Universiti;
14. Mendokumentasikan proses dan prosedur yang telah dipersetujui;
15. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; dan
16. Membuat penduaan (backup) untuk data-data kritikal Universiti.

4.0 PEMBANGUNAN PELAN PENGURUSAN KESINAMBUNGAN PERKHIDMATAN (PKP)

4.1. Pelan PKP yang dibangunkan hendaklah mengandungi perkara-perkara berikut:

1. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;
2. Senarai personel ICT Universiti yang terlibat dan pembekal (*vendor*) berserta nombor yang boleh dihubungi (faksimili, telefon bimbit, telefon pejabat dan e-mel). Senarai kedua juga hendaklah

disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani insiden;

3. Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;
4. Alternatif sumber pemprosesan dan lokasi untuk menggantika nsumber yang telah lumpuh; dan
5. Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh.

4.2. Salinan pelan PKP perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan PKP universiti dikategorikan sebagai dokumen terperingkat.

4.3. Pastikan salinan pelan PKP sentiasa dikemaskini dan dilindungi daripada gangguan/bencana yang bakal memusnahkan pelan tersebut.

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

4.5. Laksanakan pelan PKP mengikut Garis Panduan Pelaksanaan PKP seperti yang telah digariskan dalam Surat Arahan Ketua Pengarah MAMPU : Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam (Tarikh : 22 Januari 2010).

4.6. Pelan PKP (termasuk pelan simulasi) hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan.

4.7. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan.

16

PENGUATKUASAAN DAN PEMATUHAN

1.0 Pematuhan Dan Keperluan Perundangan

1.1. Pematuhan Dasar

Setiap pengguna di anggap mengetahui, membaca, memahami dan mematuhi DKICT UiTM. Penggunaan kemudahan ICT universiti selain daripada maksud dan tujuan yang telah ditetapkan merupakan satu penyalahgunaan. Prinsip "*res ipsa loquiotor*" atau *ignorance of law is not an excuse* adalah terpakai di dalam penguatkuasaan Dasar ICT UiTM.

1.2. Perlanggaran Dasar

1. Mana-mana pihak yang gagal untuk mematuhi peruntukan dasar ini sama ada dengan niat sengaja atau pun tidak, boleh dikenakan tindakan penguatkuasaan bagi tujuan pematuhan.

2. Kemudahan ICT yang disediakan oleh UiTM merupakan kemudahan bukan hak peribadi yang diberikan kepada pengguna. Sebarang pelanggaran dasar dan peraturan oleh pengguna akan dikenakan tindakan berdasarkan kepada jenis pelanggaran mengikut undang-undang semasa yang berkuatkuasa jika disabit kesalahan.

3. Pelanggaran dasar ini boleh mengakibatkan tindakan tatatertib diambil terhadap pengguna. Mereka boleh dihalang atau digantung daripada menggunakan atau mendapatkan kemudahan ICT yang disediakan.

4. Sebarang aduan tentang pelanggaran DKICT hendaklah dibuat secara bertulis kepada Pengarah Jabatan Infostruktur selaku ICTSO universiti. Jabatan Infostruktur boleh melantik satu Jawatankuasa Penyiasat untuk meneliti laporan dan menentukan sama ada siasatan terperinci perlu dilakukan. ICTSO akan melantik sekurang-kurangnya dua orang penyiasat teknikal untuk meneliti laporan dan menjalankan siasatan serta membuat keputusan sama ada siasatan terperinci perlu dilaksanakan sebelum sesuatu tindakan diambil.

5. Tindakan adalah tertakluk dan mematuhi kepada undang-undang yang berkaitan dan telah dirujuk ke Pejabat Undang-undang UiTM.

2.0 Keperluan Perundangan

Tindakan boleh diambil jika berkaitan, berdasarkan akta dan perundangan negara semasa, antaranya (dan tidak terhad kepada):

1. Akta Badan-badan Berkanun (Tatatertib dan Surcaj) 2000 (Akta 605)
2. Akta 174 (Akta Institusi-institusi Pelajaran (Tatatertib) 1976)
3. Akta Universiti Teknologi MARA 1976 (Akta 173)
4. Akta Rahsia Rasmi 1972 (Akta 88) Seksyen 8
5. Akta Komunikasi dan Multimedia 1998 (Akta 588)
6. Akta Jenayah Komputer 1997 (Akta 563)
7. *Personal Data Protection Act 2010 (Act 709)*
8. Akta Tandatangan Digital 1997 (Akta 562)
9. Akta Mesin Cetak dan Penerbitan 1984 (Akta301)
10. Akta Hak Cipta (Pindaan) 2012 (Akta A1420)
11. Akta Hak Cipta 1987 (Akta 332)

GLOSARI

Pernyataan	**Definisi**
UiTM	Universiti Teknologi MARA
CIO	Ketua Pegawai Maklumat (*Chief Information Officer*) Ketua Pegawai maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
JPPIT	Jawatankuasa Pembangunan Projek IT UiTM
PTJ	Pusat Tanggungjawab bermaksud jabatan, fakulti, pejabat, pusat, kampus kota, kampus negeri di UiTM
Pengurus ICT	Ketua-ketua jabatan
Pentadbir ICT	Staf PTM/PTMK yang bertanggungjawab.
Pentadbir Sistem	Pegawai yang bertanggungjawab untuk membangun, mengurus, mengawal, memantau dan menyelenggara operasan keselamatan kemudahan ICT.
Pelajar	Seseorang yang mendaftar sesuatu program akademik (sama ada sepenuh masa atau separuh masa) di UiTM dan statusnya masih aktif.
Pengguna	Staf, pelajar UiTM dan pihak ketiga yang menggunakan perkhidmatan ICT di UiTM
PTM	Pegawai Teknologi Maklumat
PTMK	Pegawai Teknologi Maklumat Kanan
PPTM	Penolong Pegawai Teknologi Maklumat
Pihak Ketiga	Pihak yang membekalkan perkhidmatan kepada UiTM. Pembekal, pakar runding dan lain-lain yang terlibat secara langsung dengan pengurusan Universiti

Akaun Pengguna	Akaun Pengguna merupakan satu kaedah bagi membenarkan seseorang pengguna untuk membuat capaian terhadap sesuatu sistem. Kebiasaanya akaun pengguna melibatkan penggunaan kata nama dan kata laluan.
MAMPU	Unit Permodenan Tadbiran dan Perancangan Pengurusan Malaysia, Jabatan Perdana Menteri
LAN	*Local Area Network* Rangkaian komputer yang merangkumi rangkaian kawasan setempat. LAN dalam skop UiTM adalah rangkaian UiTM di Shah Alam, kampus negeri dan kampus kota UiTM.
WAN	*Wide Area Network* Rangkaian komputer jarak jauh dan teknologi yang biasanya digunakan untuk menyambungkan komputer yang berada pada lokasi yang berbeza (negeri, negara dan benua). WAN dalam skop UiTM adalah sambungan kepada rangkaian Internet.
MAN	*Metropolitan Area Network* Rangkaian computer yang meliputi suatu kawasan geografi yang agak luas berbanding dengan rangkaian yang diliputi oleh LAN. MAN dalam skop UiTM adalah rangkaian yang merangkumi UiTM Kampus Negeri/ UiTM Kampus PFI, dan UiTM kampus kota/satelit
PFI	*Private Funding Initiative* Konsep kampus yang dibangunkan menerusi pembiayaan pihak swasta. Pihak swasta yang di kenalpasti yang akan membiayai kos pembiayaan dan penyelenggaraan buat kampus di negeri-negeri yang telah dikenalpasti.

Kod Sumber Sistem Aplikasi	Merujuk kepada sebarang pernyataan yang ditulis dalam bahasa pengaturcaraan komputer yang difahami manusia dan terdapat dalam beberapa fail computer tetapi kod sumber yang sama boleh dicetak di dalam buku atau dirakam dalam pita.
Kemudahan ICT	Merujuk kepada perkakasan, peralatan dan perkhidmatan yang berkaitan teknologi maklumat dan telkomunikasi yang disediakan oleh UiTM bagi tujuan pengurusan, pentadbiran, penyelidikan, pengajaran dan pembelajaran serta operasi pengguna.
Server	Bermaksud computer yang mempunyai keupayaan tinggi yang member perkhidmatan berpusat.
Rahsia Besar	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Negara Malaysia, hendaklah diperingkatkan **Rahsia Besar**.
Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan Negara, menyebabkan kerosakan besar kepada kepentingan atau mertabat negara Malaysia atau member keuntungan besar kepada sesebuah kuasa asing hendaklah diperingkatkan **Rahsia**.
Sulit	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan Negara tetapi memudaratkan kepentingan atau mertabat negara Malaysia atau kegiatan kerajaan atau orang perseorangan atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran

	atau akan menguntungkan sesebuah kuasa asing hendaklah diperingkatkan **Sulit**.
Terhad	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan **Rahsia Besar, Rahsia** atau **Sulit** tetapi berkehendakkan hendaklah diperingkatkan **Terhad**.
Insiden Keselamatan	Musibah (*adverse event*) yang berlaku ke atas system maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
Dokumen	Semua himpunan atau kumpulan bahan atau dokumen yang disimpan dalam bentuk media cetak, salinan lembut (*soft copy*), elektronik, dalam talian, kertas lutsinar, risalah atau slaid.
Media storan	Perkakasan yang berkaitan dengan penyimpanan data dan maklumat seperti disket, kartrij, cakera padatm cakera mudah alih, pita, cakera keras dan pemacu pena.
Aset ICT	Data, maklumat, perkakasan, perisian, aplikasi, dokumentasi dan sumber manusia serta premis berkaitan dengan ICT yang berada di bawah tanggungjawab UiTM
Akaun Pengguna	Akaun e-mel, e-community dan rangkaian
Kawasan Terperingkat	Kawasan-kawasan premis atau sebahagian dari premis di mana perkara-perkara terperingkat disimpan atau diuruskan atau di mana kerja terperingkat dijalankan.
Peralatan Perlindungan	Peralatan yang berfungsi untuk pengawalan, pencegahan dan pengurusan tampalan seperti *firewall, router, proxy dan antivirus.*
Enkripsi	Bermaksud menjadikan teks biasa (plain text) kepada kod yang tidak dapat difahami dan kod yang tidak difahami ini

	akan menjadi versi teks cipher. Bagi mendapatkan semula teks biasa tersebut, penyahsulitan digunakan.
Kriptografi	Bermaksud adalah satu sains penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak yang tertentu sahaja.
Internet	Internet adalah sistem rangkaian komunikasi global. Ia merangkumi infrastruktur perkakasan dan perisian yang menyediakan sambungan rangkaian global di antara komputer.Internet dalam skop UiTM adalah servis rangkaian yang membolehkan pengguna mengakses sumber maklumat di seluruh dunia secara atas talian.
Intranet	Merujuk kepada jaringan rangkaian dalaman yang menghubungkan komputer di dalam sesebuah organisasi dan hanya boleh dicapai oleh staf atau mana-mana pihak yang dibenarkan. Intranet dalam skop UiTM adalah servis rangkaian yang membolehkan pengguna mengakses sumber maklumat di dalam kampus UiTM secara atas talian.
VPN	Virtual Private Network - Rangkaian Persendirian Maya Servis rangkaian yang menggunakan infrastruktur telekomunikasi awam seperti Internet bagi membolehkan pengguna yang berada di luar kampus mendapat capaian Metro-E dan menggunakan rangkaian tersebut dalam keadaan selamat.
Public IP	Alamat IP yang dikhaskan untuk kegunaan rangkaian luar seperti WAN (internet).
Private IP	Alamat IP yang dikhaskan untuk rangkaian dalaman seperti LAN dan MAN dan tidak di sebarkan ke internet.
Antivirus	Perisian yang mengimbas virus pada media storan seperti

	disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar Jalur. Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di anatara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*), penipuan (*hoaxes*).
GCERT	*Government Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan IT Kerajaan. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi

	masing-masing dan agensi di bawah kawalannya.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	Hab (*hub*) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu *port* kepada semua *port* yang lain.
ICT	*Information and Communication Technology* (Teknologi Maklumat dan Komunikasi).
ICTSO	*ICT Security Officer.* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan. 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 computer yang memantau rangkaian dan/atau aktivti 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.
Logout	*Log-out* computer iaitu keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse*, *worm*, *spyware* dan sebagainya.
MODEM	*MOdulator DEModulator*
	Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Perisian Aplikasi	Ia merujuk kepada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam 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.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya pengasingan rangkaian dapat dilakukan. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif peribadi dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.
Kesinambungan	Merujuk kepada perkhidmatan dan pelaksanaan fungsi

Perkhidmatan	kritikal serta proses-proses utama yang berterusan walaupun berlaku gangguan dan fungsi-fungsi normal segera dibaik pulih dalam tempoh masa yang ditetapkan.
Penilaian Risiko	Penilaian risiko atau *risk assessment* merujuk kepada penilaian ke atas kebarangkalian menghadapi gangguan dan kesan dari kerosakan atau kehilangan aset.
Pasukan PKP	Merupakan pasukan yang dipertanggungjawabkan ke atas projek Pengurusan Kesinambungan Perkhidmatan di agensi. Ahli Pasukan PKP terdiri daripada wakil Bahagian, Unit atau Cawangan di agensi dan diketuai oleh Koordinator PKP.
Simulasi	Simulasi adalah proses menguji pelan pelaksanaan PKP agensi untuk mengenal pasti isu dan kekurangan dalam dokumentasi.
Pelan Kesinambungan Perkhidmatan (PKP)	Pelan Kesinambungan Perkhidmatan(PKP) merujuk kepada pelan atau perancangan pengurusan kesinambungan perkhidmatan. Perancangan ini yang meliputi segala sumber, proses, peranan dan tanggungjawab semua pihak terlibat yang diperlukan sebelum, semasa dan selepas sesuatu gangguan kepada system penyampaian perkhidmatan perlu didokumenkan, diuji dan dikaji semula secara berkala dan dilaksanakan apabila berlaku gangguan. Di samping itu, tindakan dilaksanakan untuk segera membaik pulih pelaksanaan fungsi-fungsi normal university dalam tempoh yang ditetapkan.
Pusat Pemulihan Bencana	Pusat pemulihan bencana atau *disaster recovery centre* merupakan lokasi alternatif bagi lokasi asal untuk

membolehkan agensi meneruskan operasi ICT yang menyokong fungsi kritikal agensi apabila berlaku gangguan atau bencana.

Pelan Pemulihan Bencana	Pelan Pemulihan Bencana atau *Disaster Recovery Plan* merujuk kepada dokumen pelan yang menetapkan sumber, tindakan, tanggungjawab dan data yang diperlukan untuk mengurus proses pemulihan selepas berlaku gangguan dalam perkhidmatan agensi. Pelan ini direka bentuk untuk membantu agensi mengembalikan semula proses perkhidmatan dalam tempoh ditetapkan untuk pemulihan bencana.
Pelan Simulasi	Dokumen perancangan yang digunakan bagi proses simulasi atau menguji tindakan-tindakan yang perlu dilaksanakan oleh Pasukan PKP apabila pelan (kesinambungan perkhidmatan/pemulihan bencana/pengurusan krisis) diaktifkan. Pelaksanaannya mungkin melibatkan Pasukan PKP atau semua warga univerisiti dan dilaksanakan dalam keadaan atau situasi yang seakan-akan gangguan atau bencana sebenar.