GARIS PANDUAN PENGGUNAAN ICT UiTM

PENTABIR SISTEM / PEGAWAI ICT

Kandungan

SINGKATAN

AP	Access Point
BPP	Bahagian Pengambilan Pelajar
CIO	Chief Information Officer (Ketua Pegawai Maklumat)
CITU	Pusat Pemikiran dan Kefahaman Islam
COINS	Corporate Information Superhighway
DBA	Database Administrator
DNS	Domain Name Server
FAIS	Financial Accounting Integrated System
FTMSK	Fakulti Teknologi Maklumat dan Sains Kuantitatif
FTP	File Transfer Protocol
HEA	Hal Ehwal Akademik
HEP	Hal Ehwal Pelajar
ICT	Information and Communication Technology (Teknologi Maklumat dan Komunikasi)
ILQaM	Institut Kepimpinan dan Pengurusan Kualiti
InED	Institut Perkembangan Pendidikan
InQKA	Institut Kualiti & Pengembangan Ilmu
IOS	Internetworking Operating System
IP	Internet Protocol
iSIS	Integrated Student Information System
JKKPA	Jabatan Komunikasi Korporat dan Perhubungan Antarabangsa
JPPK	Jawatankuasa Penilaian dan Penggunaan Komputer
LAN	Local Area Network
MAMPU	Malaysia Administrative Modernisation and Management Planning Unit (Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia)
MEDEC	Pusat Pembangunan Usahawan Malaysia
NC	Naib Canselor
OSS	Open Source Software

PENDAFTAR	Pendaftar UiTM
PNC	Penolong Naib Canselor
PPF	Pejabat Pengurusan Fisiliti
PPS	Pusat Perancangan Strategik
PSMB	Pusat Sistem Maklumat Bersepadu
PTAR	Perpustakaan Tun Abdul Razak
RMI	Research Management Institute
SIMS	Student Information Management System
SSID	Service Set Identifier
STARS	Staff Resource Information System
TNC	Timbalan Naib Canselor
UiLC	Pusat Perhubungan UiTM-Industri
UiTM	Universiti Teknologi MARA
UiTMNet	Sistem Rangkaian LAN dan WAN yang bersambung ke internet
UPENA	Pusat Penerbitan UiTM
UPPICT	Unit Penyelidikan dan Pembangunan ICT
VPN	Virtual Private Network
WAN	Wide Area Network

PENTAKRIFAN

akaun pengguna	kemudahan yang telah diperuntukkan kepada setiap pengguna yang sah dalam sesuatu sistem ICT. Setiap pengguna dikenalpasti melalui penggunaan identiti pengguna.
Capaian	dapat memperolehi perkhidmatan dari sistem-sistem UiTM yang diselenggara oleh PSMB.
CIO	pegawai kanan UiTM yang dilantik oleh MAMPU untuk menerajui kepimpinan ICT UiTM dan bertanggungjawab dalam menentukan strategi dan melaksanakan inisiatif ICT bagi mencapai misi dan objektif pembangunan dan penggunaan ICT UiTM.
Data	Kombinasi aksara (huruf, angka dan symbol) yang disimpan, dijana, diguna oleh sistem
Garis panduan	pernyataan umum yang bertujuan untuk memudahkan pengguna menggunakan sumber ICT.
Integriti	melindungi ketepatan dan keutuhan maklumat
Jabatan	Merujuk kepada semua bahagian, akademi, jabatan, fakulti, pusat, kampus cawangan, unit dan pusat tanggungjawab di UiTM;
kemudahan ICT	termasuk, tetapi tidak terhad kepada, sistem komputer peribadi, terminal, sistem komputer, alat-alat pinggiran komputer, peralatan komunikasi, rangkaian komunikasi, perisian komputer, dokumentasi bantuan, pembekalan, peralatan storan, kemudahan sokongan dan sumber tenaga. Kemudahan terhad kepada kemudahan yang dibeli, disewa, dipajak, dimiliki atau dipinjamkan kepada UiTM. Ia termasuk semua kemudahan yang disediakan oleh UiTM secara terpusat dan yang disediakan melalui Jabatan;
Kerahsiaan	menghadkan capaian maklumat kepada orang yang diberi kuasa pada masa dan keadaan yang dibenarkan
Maklumat	Kombinasi data yang memberi maksud tertentu
maklumat rahsia atau sulit	Maklumat yang tidak dibenarkan sesiapa pun mendapatkannya kecuali mereka yang dibenarkan.
media storan	semua bentuk media storan seperti thumb drives, disket, kartrij, CD, DVD, pita, cakera
pelajar	individu yang mendaftar dengan UiTM untuk mengikuti Program Pengajian yang ditawarkan setelah membayar yuran pengajian dan mendaftar kursus
Pembangunan sistem aplikasi	sistem aplikasi yang dibangunkan dengan menggunakan perisian pembangunan atau pun pakej sedia ada (*off-the-shelf*) untuk kegunaan tertentu dan seumpamanya (contoh: Sistem Perakaunan, Sistem Personel, Sistem Pengurusan Inventori).

Pemilik Proses	Jabatan/Bahagian/Fakulti/Unit yang bertanggungjawab terhadap proses sesuatu aplikasi. Contohnya Pejabat Bendahari adalah pemilik proses bagi aplikasi FAIS.
pengeboman mel	memenuhkan kotak mel seseorang pengguna dengan e-mel yang bersaiz besar atau banyak
pengguna	satu atau sekumpulan indvidu yang menggunakan kemudahan ICT UiTM
Pengguna luar	Pengguna dari kalangan masyarakat luar
Peningkatan sistem	mempertingkatkan keupayaan perkakasan, perisian, rangkaian, aplikasi dan/atau perkhidmatan ICT. Contoh adalah seperti peningkatan perkakasan dari segi konfigurasi dan kapasiti, pengemaskinian fungsi-fungsi di dalam sistem ICT sedia ada kepada tahap yang lebih baik, peningkatan saiz jalur lebar (*bandwidth*) serta peluasan rangkaian, pertambahan skop perkhidmatan sedia ada kepada yang lebih baik dan seumpamanya.
Pentadbir Operasi	Pengguna yang bertanggungjawab terhadap operasi sistem di jabatan masing-masing. Contohnya Pengemaskinian Rekod, Pendaftaran Pelajar, Pendaftaran Kursus dan sebagainya.
peralatan ICT	peralatan komputer dan periferal seperti komputer peribadi, stesen kerja, server, alat cetak, scanner, alat-alat perangkaian dan sebagainya
peralatan komunikasi	semua peralatan berkaitan komunikasi seperti pelayan rangkaian, gateway, bridge, router dan peralatan PABX;
perisian komputer	merangkumi semua jenis perisian sistem dan perisian aplikasi. Perisian sistem merangkumi sistem operasi, pangkalan data dan perisian bagi membangunkan sistem. Perisian aplikasi atau automasi pejabat adalah perisian yang digunakan untuk menyokong kerja-kerja harian.
perkakasan komputer	merangkumi semua jenis alat-alat input/output (contoh: pencetak, pengimbas), pemprosesan, storan data, peralatan rangkaian dan multimedia (contoh: persidangan video (*video conferencing)*) kecuali alat-alat seperti komponen alat ganti, barang pakai habis (*consumable item*), aksesori dan perabot komputer
Perkhidmatan ICT	merangkumi semua jenis perkhidmatan teknikal yang diperoleh daripada syarikat perunding swasta, kontraktor dan syarikat-syarikat lain yang berkaitan. Di antara contoh-contoh perkhidmatan teknikal ialah pembangunan sistem, pemasangan sistem, infrastruktur rangkaian, talian Internet, *web hosting*, kemasukan data, pemindahan data, migrasi sistem, pemulihan data, langganan maklumat atas talian dan seumpamanya.
Perluasan sistem *(system roll-out)*	memperkembangkan pelaksanaan projek ICT daripada lokasi sedia ada ke lokasi-lokasi lain atau dengan menambah bilangan pengguna di lokasi yang sama atau pun kedua-duanya sekali.

Pertambahan peralatan	menambahkan bilangan bagi mana-mana perkara di bawah kategori perkakasan, perisian dan/atau rangkaian bagi projek ICT sedia ada.
Projek baru	projek pengkomputeran yang melibatkan salah satu atau gabungan aktiviti-aktiviti perolehan perkakasan, perisian dan/atau perkhidmatan ICT untuk membangunkan projek ICT agensi.
Prosedur	tatacara standard dan garis panduan yang digunapakai dalam operasi ICT.
PTJ	PTJ atau Pusat Tanggung Jawab merangkumi semua Pusat, Bahagian, Fakulti, Jabatan, Akademi dan cawangan yang menerima Peruntukan kewangan.
Sebutharga rasmi	pembelian melebihi RM50,000.00 sehingga RM500,000.00
Sebutharga runcit	pembelian tidak melebihi RM 50,000.00
Spam	penghantaran e-mel yang tidak diperlukan kepada ramai penerima
SSID	Nama yang digunakan sebagai pengenalan bagi sistem rangkaian tanpa wayar.
staf	seseorang yang dilantik oleh UiTM untuk sesuatu jawatan sama ada secara tetap, sambilan, harian, sementara atau kontrak dan masih berkhidmat dengan UiTM.
Standard	sesuatu aktiviti, tindakan, peraturan atau tatacara piawai yang perlu dipatuhi oleh pengguna.
Tender	pembelian melebihi RM500,000.00
UiTMNet	sistem rangkaian berpusat di mana UiTM Shah Alam adalah laluan keluar dan masuk utama sistem UiTMNet secara menyeluruh
VPN	Sistem rangkaian persendirian yang terhubung melalui internet dengan menggunakan enkripsi dan mekanisme keselamatan lain bagi memastikan hanya pengguna yang dibenarkan dapat mengakses rangkaian ini

1 GARIS PANDUAN PENGURUSAN MAKLUMAT (DATA) UiTM

1.1 Tujuan

Garis panduan bertujuan untuk memastikan semua maklumat dan data yang terdapat di didalam sistem UiTM diurus, digunakan secara optima dan berintegriti supaya menyokong proses pengajaran, pembelajaran, pembudayaan ilmu, penyelidikan, perundingan, pentadbiran dan membantu pihak pengurusan UiTM membuat keputusan dengan cepat, tepat dan betul.

1.2 Objektif

Objektif ini adalah seperti berikut: -

(i) Memastikan sumber rujukan data dan maklumat ICT datang daripada satu sumber.

(ii) Mengelakkan berlakunya percanggahan data dan maklumat di UiTM

1.3 Skop

Garis panduan ini diguna pakai oleh UiTM merangkumi semua maklumat UiTM termasuk dan tidak terhad kepada maklumat pelajar, staf, kewangan, ruang dan sebagainya.

1.4 Penyataan

(i) Semua data yang terdapat pada mana-mana pangkalan data yang diguna pakai oleh Jabatan adalah hakmilik UiTM. Ia perlu digunakan secara optima selaras dengan keperluan perancangan strategik UiTM.

(ii) Jabatan yang bertanggungjawab mengemaskini, menyelenggara dan menyimpan maklumat perlu mengambil tindakan sewajarnya untuk memastikan maklumat dan data di bawah tanggungjawab Jabatan tersebut sentiasa tepat dan terkini.

(iii) CIO mempunyai kuasa untuk menentukan penggunaan semua maklumat dan data tersebut adalah mengikut kepentingan UiTM.

(iv) PPS bertindak sebagai sumber maklumat UiTM. Semua permohonan maklumat elektronik UiTM mesti dimajukan kepada PPS.

2 GARIS PANDUAN PEROLEHAN KEMUDAHAN ICT UiTM

2.1 Tujuan

Garis panduan perolehan kemudahan ICT ini bertujuan untuk memberikan penjelasan prosedur pembelian kemudahan ICT kepada pengguna dan ketua Jabatan.

2.2 Objektif

(i) Memaklumkan kepada Jabatan prosedur perolehan secara tender perkakasan dan perisian yang diamalkan oleh UiTM

(ii) Memaklumkan kepada Jabatan prosedur perolehan secara sebutharga perkakasan dan perisian yang diamalkan oleh UiTM

(iii) Memaklumkan kepada Jabatan prosedur perolehan secara perolehan runcit perkakasan dan perisian yang diamalkan oleh UiTM.

2.3 Skop

Merangkumi perolehan seperti berikut :

(i) Perkakasan Komputer

(ii) Perisian Komputer

(iii) Perkhidmatan ICT

(iv) Aksesori ICT Yang lain

Perolehan ICT yang melibatkan

(i) pelanjutan, seperti langganan maklumat atas talian, talian Internet dan *web hosting,* dengan tiada perubahan kepada skop asal, tidak perlu mendapatkan kelulusan teknikal.

(ii) Perkhidmatan Perunding

Rujuk :

a. **Pekeliling Perbendaharaan Bil. 3 Tahun 1995** bertajuk **Peraturan Perolehan Perkhidmatan Perunding DAN**

b. **Pekeliling Perbendaharaan Bil. 6 Tahun 2006** bertajuk **Had Kuasa Agensi Bagi Melantik Perunding**

(iii) Perkhidmatan penyelenggaraan

tidak perlu mendapatkan kelulusan teknikal JTICT.

2.4 Nilai Perolehan

Nilai Perolehan	Kelulusan yang Diperlukan					Kaedah Perolehan
	JPPK	JPICT, KPT	MAMPU	UPPICT (Kelulusan Spesifikasi)	PTJ (Kelulusan Bajet)	
Tidak melebihi RM 50,000.00	√			√	√	Sebutharga runcit
Melebihi RM 50,000.00 tetapi tidak melebihi RM 500,000.00	√			√	√	Sebutharga rasmi
Melebihi RM 500,000.00 tetapi tidak melebihi RM 3 juta	√	√		√	√	Tender

Melebihi RM 500,000.00 tetapi tidak melebihi RM 3 juta **DAN** mempunyai item pembangunan sisem aplikasi bernilai RM 500,000.00 ke atas	√	√	√	√	√	Tender
Melebihi RM 3 juta	√	√	√	√	√	Tender

Rujuk pekeliling Surat Pekeliling Am Bilangan 1 tahun 2009 bertarikh 30 April 2009.

2.5 Pernyataan

Ketua PTJ perlu mematuhi peraturan perolehan yang dikeluarkan oleh Pejabat Bendahari melalui Pekeliling Bendahari bertarikh 1 Oktober 2009.

2.5.1 Perolehan Peralatan/Perkakasan/Perisian dan perkhidmatan ICT secara Tender (Pembelian melebihi RM3,000,000.00)

(i) Ketua PTJ perlu menyediakan kertas kerja dan mendapatkan kelulusan daripada JPPK untuk dikemukakan bagi kelulusan dari sekretariat perolehan ICT Kementerian Pengajian Tinggi dan diikuti kelulusan dari MAMPU.

(ii) Ketua PTJ perlu mendapatkan spesifikasi peralatan/perkakasan/perisian dan perkhidmatan ICT yang diluluskan oleh UPPICT.

(iii) Spesifikasi tersebut perlu ditandatangani oleh Pengerusi UPPICT untuk tujuan perolehan secara tender.

(iv) PTJ perlu mempunyai peruntukan untuk perolehan berkaitan.

2.5.2 Perolehan Peralatan/Perkakasan/Perisian dan perkhidmatan ICT secara Tender (Pembelian melebihi RM500,000.00 dan tidak lebih daripada RM1,000,000.00)

(i) Ketua PTJ perlu menyediakan kertas kerja dan mendapatkan kelulusan daripada JPPK untuk dikemukakan bagi kelulusan dari sekretariat perolehan ICT Kementerian Pengajian.

(ii) Ketua PTJ perlu mendapatkan kelulusan daripada MAMPU jika terdapat item Pembangunan Sistem Aplikasi bernilai RM500,000.00 atau lebih.

(iii) Ketua PTJ perlu mendapatkan spesifikasi peralatan/perkakasan/perisian dan perkhidmatan ICT yang diluluskan oleh UPPICT.

(iv) Spesifikasi tersebut perlu ditandatangani oleh Pengerusi UPPICT untuk tujuan perolehan secara tender.

(v) PTJ perlu mempunyai peruntukan untuk perolehan berkaitan.

2.5.3 Perolehan Peralatan/Perkakasan/Perisian dan perkhidmatan ICT secara Sebutharga RASMI (Pembelian melebihi RM50,000.00 dan tidak lebih daripada RM500,000.00 setahun).

(i) Ketua PTJ perlu menyediakan kertas kerja dan mendapatkan kelulusan daripada JPPK.

(ii) Ketua PTJ perlu mendapatkan spesifikasi peralatan/perkakasan/perisian dan perkhidmatan ICT yang diluluskan oleh UPPICT.

(iii) Spesifikasi tersebut perlu ditandatangani oleh Pengerusi UPPICT untuk tujuan perolehan secara sebutharga rasmi.

(iv) PTJ perlu mempunyai peruntukan untuk Perolehan Peralatan/Perkakasan.

(v) PTJ adalah dilarang memecah-mecahkan peruntukan semata-mata untuk membolehkan perolehan berkaitan dilaksanakan bagi mengelakkan perolehan secara tender.

2.5.4 Perolehan Peralatan/Perkakasan/Perisian dan perkhidmatan ICT secara Sebutharga RUNCIT (Pembelian tidak melebihi RM50,000.00 setahun)

(i) Ketua PTJ perlu menyediakan kertas kerja dan mendapatkan kelulusan daripada JPPK.

(ii) PTJ adalah dilarang memecah-mecahkan peruntukan semata-mata untuk membolehkan perolehan berkaitan dilaksanakan bagi mengelakan perolehan secara tender dan sebutharga.

2.5.5 Perolehan Perisian

(i) Ketua PTJ perlu mendapatkan kelulusan daripada JPPK dan UPPICT untuk pembelian sebarang jenis perisian.

(ii) Permohonan pembelian perisian standard boleh dimajukan ke PSMB untuk diuruskan.

(iii) Sebarang perolehan perisian umum yang terdapat dalam kontrak antara Kementerian Pengajian Tinggi dan pembekal perisian perlu dirujuk kepada PSMB

2.5.6 Perolehan Perkakasan Sistem Rangkaian Dan *Structured Cabling System (SCS)* Bagi Projek Pembangunan Melalui Tender atau Sebutharga.

(i) Jururunding bagi pihak Bahagian Pembangunan perlu mendapatkan kelulusan daripada Pengarah PSMB dari segi rekabentuk dan konfigurasi sistem rangkaian;

(ii) Jururunding bagi pihak Bahagian Pembangunan perlu mendapatkan kelulusan daripada Pengarah PSMB dari segi spesifikasi teknikal perkakasan/peralatan yang akan digunakan dalam projek yang dikendalikan oleh Jurunding berkenaan.

(iii) Kelulusan perolehan melalui JPPK.

(iv) Pengesahan spesifikasi teknikal oleh UPPICT.

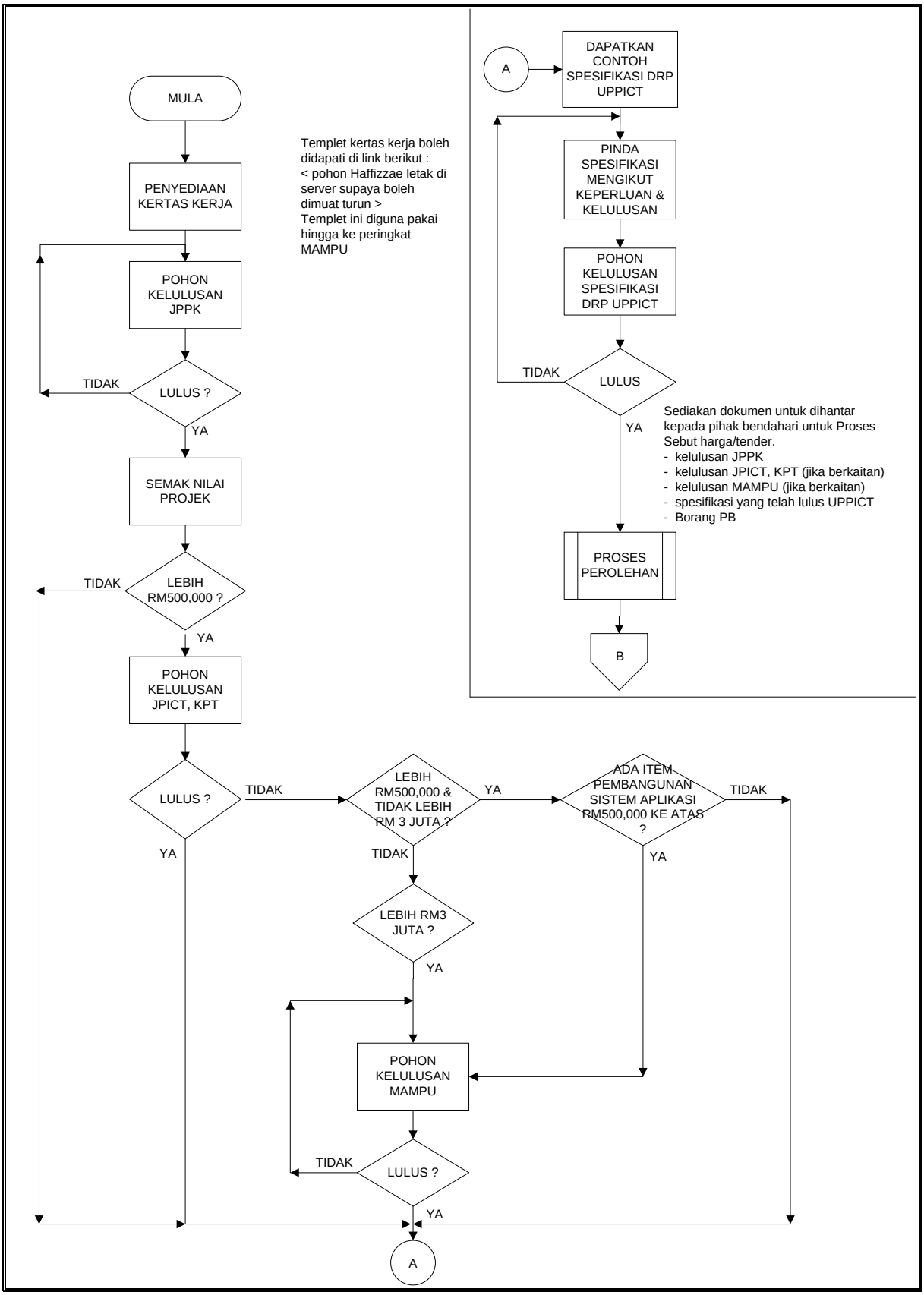
2.5.7 Perolehan *Structured Cabling System (SCS)* Melalui Tender, Sebutharga Rasmi atau Sebutharga Runcit.

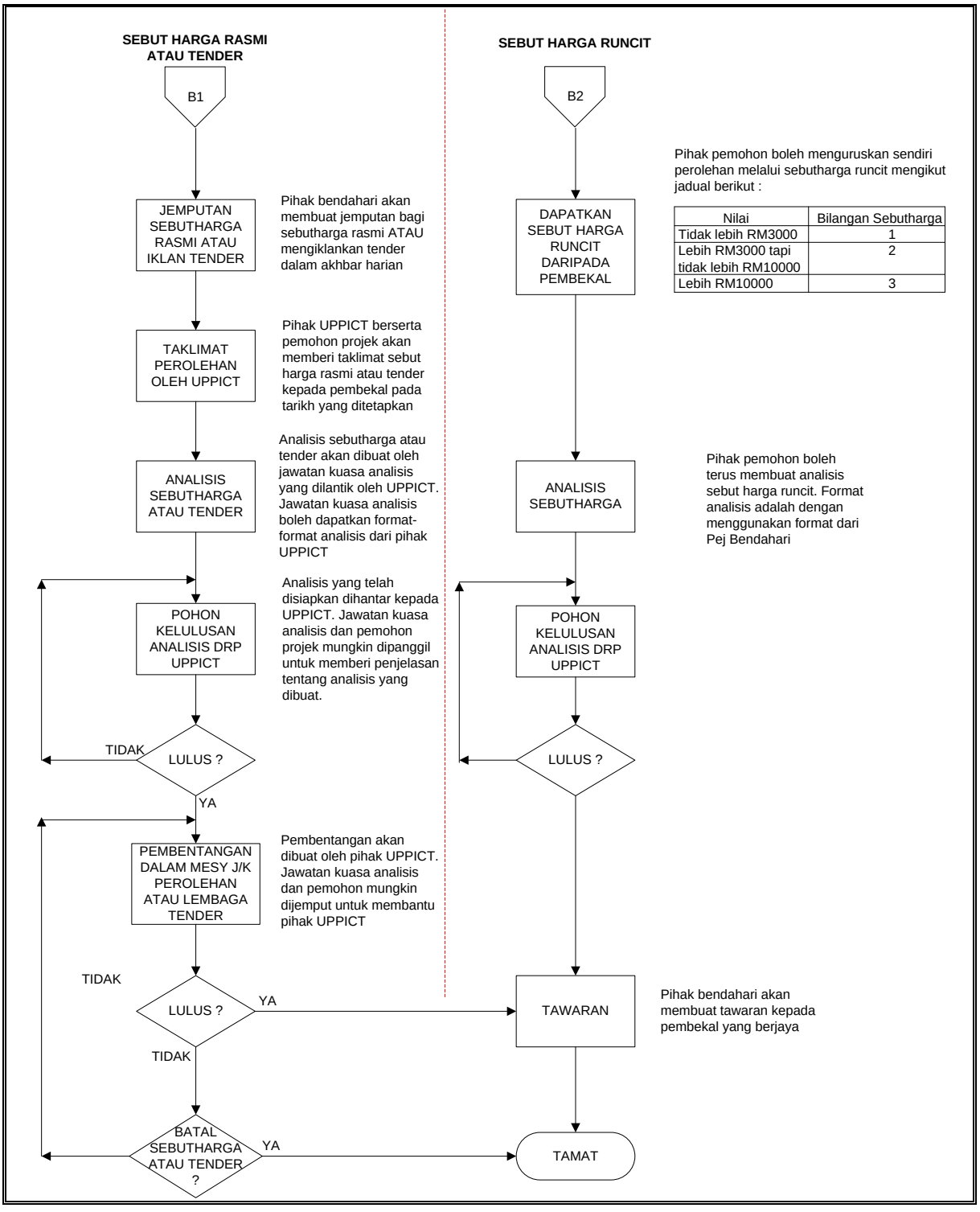
(i) Ketua PTJ perlu mendapatkan kelulusan daripada Pengarah PSMB.

(ii) Kelulusan perolehan melalui JPPK.

(iii) Pengesahan spesifikasi teknikal oleh UPPICT.

2.6 Carta alir Proses Perolehan ICT




SEBUT HARGA RASMI ATAU TENDER
B1
JEMPUTAN SEBUTHARGA RASMI ATAU IKLAN TENDER
Pihak bendahari akan membuat jemputan bagi sebutharga rasmi ATAU mengiklankan tender dalam akhbar harian
TAKLIMAT PEROLEHAN OLEH UPPICT
Pihak UPPICT berserta pemohon projek akan memberi taklimat sebut harga rasmi atau tender kepada pembekal pada tarikh yang ditetapkan
ANALISIS SEBUTHARGA ATAU TENDER
Analisis sebutharga atau tender akan dibuat oleh jawatan kuasa analisis yang dilantik oleh UPPICT. Jawatan kuasa analisis boleh dapatkan format-format analisis dari pihak UPPICT
POHON KELULUSAN ANALISIS DRP UPPICT
Analisis yang telah disiapkan dihantar kepada UPPICT. Jawatan kuasa analisis dan pemohon projek mungkin dipanggil untuk memberi penjelasan tentang analisis yang dibuat.
TIDAK
LULUS ?
YA
PEMBENTANGAN DALAM MESY J/K PEROLEHAN ATAU LEMBAGA TENDER
Pembentangan akan dibuat oleh pihak UPPICT. Jawatan kuasa analisis dan pemohon mungkin dijemput untuk membantu pihak UPPICT
TIDAK
LULUS ?
YA
TIDAK
BATAL SEBUTHARGA ATAU TENDER ?
YA
SEBUT HARGA RUNCIT
B2
DAPATKAN SEBUT HARGA RUNCIT DARIPADA PEMBEKAL
Pihak pemohon boleh menguruskan sendiri perolehan melalui sebutharga runcit mengikut jadual berikut :
Nilai
Bilangan Sebutharga
Tidak lebih RM3000
1
Lebih RM3000 tapi tidak lebih RM10000
2
Lebih RM10000
3
ANALISIS SEBUTHARGA
Pihak pemohon boleh terus membuat analisis sebut harga runcit. Format analisis adalah dengan menggunakan format dari Pej Bendahari
POHON KELULUSAN ANALISIS DRP UPPICT
LULUS ?
TAWARAN
Pihak bendahari akan membuat tawaran kepada pembekal yang berjaya
TAMAT

3 GARIS PANDUAN PENGGUNAAN DAN PEMBANGUNAN SISTEM APLIKASI, PERISIAN DAN LAIN-LAIN BAHAN BERBENTUK DIGITAL

3.1 Tujuan

Garis panduan ini menyatakan tanggungjawab dan peranan pengguna dan pihak UiTM di dalam mengguna pakai sistem aplikasi, perisian dan lain-lain bahan berbentuk digital.

3.2 Objektif

(i) Memastikan semua fakulti menggunakan perisian pengajaran dan pembelajaran yang selaras di kampus cawangan dan di kampus induk.

(ii) Penjimatan kos perisian.

(iii) Penyelarasan perolehan perisian secara berpusat.

(iv) Penyelarasan penyelenggaraan perisian secara berpusat.

(v) Kemudahan pembelajaran dan pengajaran dengan versi yang terkini bagi perisian yang di selenggara secara kontrak.

(vi) Memastikan sistem aplikasi yang dibangunkan tidak menduplikasi sistem sedia ada.

3.3 Skop

Merangkumi semua pembangunan sistem aplikasi, perisian yang dimiliki, diguna atau berada di dalam simpanan pengguna, bagi tujuan penggunaan hal-hal berkaitan UiTM, tidak kira di mana perisian itu berada.

3.4 Penyataan

3.4.1 Perjanjian Lesen Perisian (Software Licence Agreements)

(i) Semua pengguna tidak dibenarkan melanggar mana-mana perjanjian lesen perisian atau lesen perkakasan yang telah ditetapkan oleh pembangun (developer) bagi perisian tersebut.

(ii) Semua pengguna tidak dibenarkan membuat salinan (copy) sama ada dalam bentuk media (CD/DVD/Thumb Drive) ataupun apa jua kaedah yang bertujuan memindah, menyalin, menyebarkan dan membuat instalasi mana-mana perisian yang diberikan oleh PSMB melebihi jumlah lesen yang ditetapkan.

(iii) PSMB tidak akan bertanggungjawab terhadap sebarang penyalahgunaan perisian, termasuk penggunaan tanpa lesen yang dilakukan oleh pengguna.

(iv) Setiap pengguna secara peribadi bertanggungjawab untuk membaca, memahami dan mematuhi peraturan penggunaan dan syarat-syarat pelesenan bagi setiap perisian yang digunakan.

(v) Setiap pengguna tidak dibenarkan memuat turun dan membuat instalasi perisian yang boleh mendatangkan kemudaratan dan kerosakan kepada komputer serta gangguan kepada UiTMNet.

(vi) Setiap pengguna tidak dibenarkan memuat turun dan membuat instalasi perisian-perisian yang tidak relevan dengan keperluan akademik, pentadbiran dan kaji selidik di UiTM.

3.4.2 Hakmilik

(i) 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.

(ii) 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.

(iii) Bagi perisian yang dibangunkan, maklumat tentang semua pengarang/pencipta mestilah dikekalkan.

(iv) Semua perisian hakmilik UiTM tidak dibenarkan dijual, disewa, dilesenkan semula, dipinjam, disebar atau diberi kepada sesiapa atau entiti tanpa kebenaran bertulis CIO.

3.4.3 Kelulusan Penggunaan

(i) Semua jenis perisian yang diguna pakai oleh Jabatan perlu mendapat kelulusan daripada pihak pembekal atau pembangun perisian dan diguna mengikut syarat-syarat yang ditetapkan oleh pihak pembekal atau pembangun.

3.4.4 Penggunaan Perisian yang digunakan Untuk Tujuan Pengajaran dan Pembelajaran

(i) Fakulti/Cawangan bertanggungjawab sepenuhnya terhadap semua keperluan perisian yang diguna pakai untuk tujuan pengajaran dan pembelajaran di Fakulti dan cawangan masing-masing.

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

3.4.5 Pembangunan Perisian Aplikasi yang mempunyai pertindanan fungsi sistem sedia ada

(i) Pembangunan aplikasi yang mempunyai pertindanan fungsi sistem sedia ada seperti STARS, FAIS, iSIS dan sebagainya adalah TIDAK DIBENARKAN.

(ii) Sebarang keperluan pembangunan perisian yang melibatkan perubahan proses perlu dirujuk kepada pemilik proses. Pemilik proses perlu meneliti keperluan dan majukan kepada pihak PSMB untuk tindakan.

3.4.6 Pembangunan Sistem Aplikasi

(i) Sebarang sistem aplikasi yang perlu dibangunkan hendaklah dirujuk dan dibincang terlebih dahulu dengan Pusat Sistem Maklumat Bersepadu (Rujuk Pekeliling Naib Canselor Bil 7/2006 bertarikh 29 Mac 2006) –Kepil pekeliling dalam apendix

4 GARIS PANDUAN PENGGUNAAN RANGKAIAN DAN PENYAMBUNGAN UiTMNet

4.1 Tujuan

Garis panduan ini menghuraikan penggunaan perkhidmatan UiTMNet dan panduan penyambungan infrastruktur UiTMNet

4.2 Skop

Merangkumi LAN dan WAN yang bersambung ke Internet yang dipanggil UiTMNet.

4.3 Penyataan

4.3.1 Perkhidmatan UiTMNet

Merangkumi semua sumber rangkaian, termasuk (tetapi tidak terhad kepada) peralatan rangkaian seperti *switches* dan *routers*, perisian rangkaian seperti *e-mail, browsers,* dan *ftp*, konsep konfigurasi rangkaian seperti penggunaan alamat IP, dan teknologi yang diguna seperti teknologi Gigabit Ethernet dan protokol TCP/IP.

4.3.2 Penyambungan Rangkaian

Penyambungan adalah termasuk rangkaian setempat (LAN) dan rangkaian luas (WAN) sama ada berwayar atau tanpa wayar.

4.4 Garis panduan Penggunaan Sistem UiTMNet

Pihak UiTM berhak menarik balik kemudahan penggunaan UiTMNet jika pengguna didapati melanggar mana-mana peraturan yang ditetapkan seperti berikut:

(i) Kemudahan rangkaian hanya boleh diguna untuk tujuan yang berkaitan dengan urusan UiTM. Kegunaan peribadi, terutama yang berunsur komersial tidak dibenarkan;

(ii) Pengguna tidak boleh mengguna UiTMNet untuk aktiviti-aktiviti yang bertentangan dengan undang-undang atau peraturan-peraturan UiTM, negeri dan negara. Ini termasuk tetapi tidak terhad kepada menghantar dan menerima maklumat yang berunsur subversif dan menghantar dan menyebar maklumat yang rahsia atau sulit mengenai UiTM tanpa kebenaran CIO.

(iii) Pengguna tidak dibenarkan dalam apa bentuk sekali pun mengganggu lain-lain pengguna UiTMNet, Internet dan sebarang rangkaian yang lain termasuk tetapi tidak terhad kepada menghantar maklumat rambang secara mel elektronik atau mesej atas talian.

(iv) Pengguna tidak boleh memberi kemudahan rangkaian termasuk tetapi tidak terhad kepada kemudahan nod rangkaian dan kad tanpa wayar untuk diguna oleh orang lain walaupun kepada pelajar atau staf UiTM tanpa mendapat kelulusan pentadbir rangkaian;

(v) Pengguna bertanggungjawab sepenuhnya terhadap semua aktiviti termasuk tetapi tidak terhad kepada stesen kerja, komputer peribadi atau PDA yang melibatkan atau melalui UiTMNet termasuk akses ke Internet dan rangkaian-rangkaian yang lain;

(vi) Komputer yang menjadi sumber ancaman atau penyebar virus akan disekat capaiannya ke UiTMNet sehingga komputer tersebut disahkan bebas dari ancaman virus tersebut;

(vii) Penggunaan alamat IP di bawah domain UiTM sama ada setempat atau global adalah mengikut peraturan yang ditetapkan oleh PSMB, dan berada di bawah kawalan PSMB.

(viii) Semua penggunaan domain perlu dirujuk dan didaftarkan di PSMB;

4.5 Garis panduan Penyambungan Rangkaian

(i) Sebarang pemasangan rangkaian sama ada dihubungkan dengan UiTM atau tidak, perlu dilakukan dengan mengisi borang permohonan sistem rangkaian;

(ii) Pembelian peralatan rangkaian dan penyambungan ke UiTMNet perlu mendapat kelulusan dari PSMB. Konfigurasi penyambungan hendaklah dibuat oleh pembekal di bawah pengawasan dan kawalan pentadbir rangkaian PSMB;

(iii) PSMB berhak memutuskan penyambungan rangkaian ke UiTMNet yang tidak mendapat kebenaran dari Pengarah PSMB

(iv) Semua kampus-kampus cawangan UiTM perlu dihubungkan melalui teknologi VPN yang telah diselaraskan ke UiTM Shah Alam.

(v) Penyewaan dan pemasangan talian ISDN, ADSL, leased-line dan dial-up adalah dilarang sama sekali kecuali setelah mendapat kelulusan daripada JPPK.

4.6 Garis Panduan Penyediaan Infrastruktur Rangkaian Bangunan Baru

(i) Keperluan infrastruktur rangkaian mesti ditentukan bersama oleh pengguna, PSMB, Pejabat Pengurusan Fasiliti dan Bahagian Pembangunan bagi setiap bangunan baru yang akan dibina

(ii) Kos pemasangan infrastruktur rangkaian perlu dimasukkan dalam kos peruntukan pembinaan bangunan.

(Rujuk Pekeliling NC Bil 28/2006 bertarikh 3 Oktober 2006)

4.7 Garis panduan Pemberian Alamat IP

Bagi tujuan keselamatan dan kawalan perkhidmatan rangkaian, pemberian alamat IP adalah tertakluk kepada syarat-syarat yang ditetapkan oleh PSMB seperti berikut:

(i) Semua Server rasmi yang memberi perkhidmatan capaian dari luar UiTM boleh mempunyai alamat IP global. Permohonan perlu dibuat kepada PSMB dengan mengisi borang yang ditetapkan.

(ii) Sistem pemberian alamat IP di UiTM adalah menggunakan teknologi DHCP (*Distributed Host Configuration Protocol*) di mana pengguna akan mendapat alamat IP secara automatik.

(iii) Keperluan bagi alamat IP statik untuk server dan peralatan komunikasi yang berkaitan perlu dimohon kepada Bahagian Rangkaian PSMB.

(iv) Penggunaan DHCP server tanpa kebenaran Pengarah PSMB adalah tidak dibenarkan. Bahagian Rangkaian berhak memutuskan penyambungan rangkaian DHCP server daripada UiTMNet.

(v) Kampus cawangan yang tidak mempunyai DHCP server perlu mendapatkan alamat IP statik daripada Bahagian IT Kampus cawangan masing-masing.

(vi) Semua server untuk kegunaan dalaman UiTM akan diberi alamat IP dalaman. Permohonan mendapat IP perlu dibuat kepada PSMB dengan mengisi borang.

(vii) Semua peralatan rangkaian akan diberi alamat IP dalaman kecuali yang dibenarkan mengguna alamat IP global oleh PSMB;

5 GARIS PANDUAN PENGGUNAAN KOMPUTER/PENCETAK/ PENGIMBAS/ LAIN-LAIN PERIFERAL ICT

5.1 Tujuan

Garis panduan ini menyatakan tanggungjawab dan peranan pengguna dan pihak UiTM di dalam mengguna pakai komputer / pencetak / pengimbas / lain-lain periferal ICT.

5.2 Skop

Skop garis panduan melibatkan semua perkakasan yang dimiliki atau diguna atau berada di dalam simpanan pengguna bagi tujuan penggunaan hal-hal berkaitan UiTM, tidak kira di mana perkakasan itu berada.

5.3 Pernyataan

5.3.1 Hakmilik

(i) Semua perkakasan yang diperolehi untuk atau bagi pihak UiTM atau semua perkakasan yang dicipta/dipasang oleh staf atau pelajar UiTM untuk tujuan pengajaran, pembelajaran, penyelidikan atau pentadbiran adalah menjadi hakmilik UiTM.

(ii) Bagi perkakasan yang dicipta, maklumat tentang semua pencipta mestilah dikekalkan.

(iii) Perkakasan tersebut tidak dibenarkan dijual, disewa, dipaten, dipinjam, disebar atau diberi kepada sesiapa atau entiti tanpa kebenaran JPPK.

5.3.2 Tanggungjawab Pengguna

(i) Pengguna bertanggungjawab sepenuhnya terhadap keselamatan perkakasan seperti komputer, pencetak atau pengimbas yang diperuntukkan kepadanya.

(ii) Pengguna tidak berhak mengganggu dengan apa cara sekalipun perkakasan yang bukan berada di bawah kawalannya. Ini termasuk mengguna atau mengambil tanpa kebenaran, perkakasan atau komponen-komponennya.

(iii) Sebarang penggunaan secara perkongsian adalah menjadi tanggungjawab bersama pengguna-pengguna terbabit. Sebarang perkongsian perlu mempunyai syarat dan peraturan yang dipersetujui bersama.

5.4 Garis panduan Baik Pulih Dan Penyelenggaraan Komputer

(i) Servis baikpulih di kampus induk akan diuruskan secara terus oleh PSMB, manakala di kampus-kampus cawangan pula akan diuruskan oleh Bahagian ICT masing-masing.

(ii) Hanya peralatan yang berdaftar dengan Bahagian Pengurusan Harta Benda, Pejabat Bendahari UiTM, iaitu mempunyai **Kod Tanda Harta Rasmi UiTM** sahaja akan diservis.

(iii) Bagi kerosakan perkakasan yang dibekalkan oleh PSMB, Jabatan dikehendaki membuat aduan kepada PSMB dengan mengisi borang penyelenggaraan komputer. Urusan pembaikan dan penyelenggaraan akan diurus sepenuhnya oleh PSMB;

(iv) Bagi kerosakan perkakasan yang dibeli menggunakan bajet Jabatan, Jabatan diminta membuat aduan kepada PSMB untuk tujuan pemeriksaan dan pengesahan kerosakan. Jabatan perlu menanggung kos pembaikan rosakan sepenuhnya sekiranya perkakasan tersebut sudah tamat jaminannya manakala bagi perkakasan yang belum tamat jaminan, Jabatan dikehendaki menghubungi pembekal perkakasan tersebut untuk dibaiki; dan

(v) PSMB menyediakan perkhidmatan penyelenggaraan pencegahan untuk semua Jabatan (tidak termasuk komputer di makmal) dua (2) kali setahun iaitu dalam bulan Jun dan Disember. Perkhidmatan ini adalah dilaksanakan secara "Outsourcing" oleh syarikat yang dilantik oleh UiTM sahaja dan mengesahkan urusan ini pengguna boleh menghubungi PSMB bagi mengenal pasti syarikat yang dilantik. Syarikat yang dilantik tidak boleh, tanpa kebenaran atau pengesahan PSMB membawa keluar sebarang peralatan berkaitan bagi mengawal kadar kecurian.

5.5 Garis Panduan Peminjaman Komputer Peribadi, Komputer Riba Dan Perkakasan Komputer

(i) Pinjaman adalah untuk staf UiTM sahaja.

(ii) Semua peminjam perlu mengisi borang pinjaman dan urusan pengambilan peralatan boleh dibuat di PSMB.

(iii) Peminjam bertanggungjawab sepenuhnya terhadap keselamatan peralatan yang dipinjam.

(iv) Peminjam perlu membuat laporan bertulis dengan segera kepada Pengarah PSMB sekiranya berlaku kerosakan atau kehilangan peralatan yang dipinjam.

(v) Peminjam perlu memulangkan peralatan yang dipinjam dalam keadaan baik, berfungsi dan dalam set lengkap pada tarikh dan masa pemulangan yang ditetapkan. Peminjam perlu menandatangani borang pinjaman peralatan ICT yang telah diisi sebagai bukti pemulangan peralatan yang dipinjam.

(vi) Peminjam perlu mengganti atau membayar kos peralatan sekiranya berlaku kerosakan atau kehilangan ke atas peralatan yang dipinjam.

(vii) Tempoh pinjaman maksima ialah tujuh (7) hari bekerja. Sekiranya lebih, peminjam perlu mengemuka permohonan secara bertulis kepada Pengarah PSMB.

6 GARIS PANDUAN PENGGUNAAN SERVER

6.1 Tujuan

Garis panduan 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.

6.2 Objektif

(i) Memelihara keselamatan dan integriti server

(ii) Menjaga keselamatan fizikal server

(iii) Mengelak daripada dicerobohi oleh pengguna yang tidak bertanggungjawab

6.3 Skop

Server merangkumi semua sistem server (perkakasan dan perisian) yang dibangun atau disediakan oleh pengguna-pengguna yang dibenarkan. Ini termasuk server aplikasi, server rangkaian dan server kegunaan setempat dan sebagainya.

6.4 Penyataan

Setiap Jabatan atau penyedia server perlu mematuhi peraturan-peraturan berikut:

(i) Pentadbir server 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 penyedia server boleh menyedia 'firewall' khusus untuk tujuan ini;

(ii) Pentadbir server perlu mengenal pasti tahap capaian pengguna dan penggunaan server secara jelas. Ini akan menghasilkan capaian yang lebih terkawal;

(iii) 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 Pentadbir server;

(iv) Server yang digunakan untuk tujuan penyelidikan yang menggunakan rangkaian secara intensif (high bandwidth usage) perlu ditempatkan dalam rangkaian persendirian yang dipisahkan daripada UiTMNet melalui penggunaan 'switch / router' untuk mengelak gangguan kepada rangkaian utama. Sebarang ujian yang memerlukan penggunaan UiTMNet secara terus perlu mendapat kelulusan daripada Pengarah PSMB;

(v) 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;

(vi) Semua Pentadbir server perlu mematuhi peraturan berikut :

(a) pertukaran alamat IP tidak dibenarkan sama sekali tanpa kebenaran pentadbir alamat IP;

(b) login dan kata laluan untuk 'root' dan 'super-user' adalah di bawah kawalan dan tanggungjawab pentadbir server sepenuhnya; dan

(c) pentadbir server di Jabatan bertanggungjawab memastikan server tidak disalah guna untuk tujuan yang bukan sepatutnya.

6.5 Permohonan Penempatan Server di PSMB

Setiap server yang ingin diletakkan di server farm perlu mendapat kelulusan Pengarah PSMB dengan mengisi borang yang disediakan.

7 GARIS PANDUAN CAPAIAN TEKNOLOGI MAKLUMAT

7.1 Tujuan

Garis panduan ini 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.

7.2 Objektif

(i) Memelihara keselamatan dan integriti sumber ICT UiTM

(ii) Memastikan perkongsian sumber yang saksama

7.3 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 UiTMNet. Capaian boleh diberikan kepada pelajar, staf dan sesiapa yang berkenaan untuk tujuan pengajaran, pembelajaran, penyelidikan, perundingan dan pentadbiran.

7.4 Pernyataan

(i) 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.

(ii) Pengguna yang menggunakan sumber-sumber ICT UiTM mestilah mematuhi Garis panduan 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 UiTMNet dengan tujuan untuk mendapat capaian kepada sumber-sumber ICT UiTM perlu mendapat kebenaran/kelulusan bertulis daripada Pengarah PSMB. Kebenaran/kelulusan ini adalah bergantung kepada tahap piawai dan keselamatan untuk alat/peranti elektronik/komputer tersebut yang telah ditetapkan oleh UPPICT;

(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.

8 GARIS PANDUAN AKAUNTABILITI DAN INTEGRITI ICT UiTM

8.1 Tujuan

Garis panduan ini menyatakan tanggungjawab pihak yang terlibat dengan penggunaan kemudahan ICT di UiTM seperti berikut:

(i) Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap sumber ICT UiTM;

(ii) Melindungi kepentingan pengguna ICT apabila berlaku kejadian perlanggaran atau pencabulan Garis panduan-Garis panduan keselamatan ICT yang lain;

(iii) Memelihara akauntabliti dan intergriti sumber-sumber ICT UiTM.

8.2 Skop

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

(i) Perkhidmatan-perkhidmatan ICT;

(ii) Penyelenggaraan dan penyeliaan perkhidmatan-perkhidmatan ICT;

(iii) Penggunaan perkhidmatan-perkhidmatan ICT.

8.3 Penyataan

8.3.1 Tanggungjawab UiTM

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

(i) 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;

(ii) Menyediakan perkhidmatan ICT;

(iii) Menyelenggara dan membaik pulih peralatan ICT yang dinyatakan dalam perkara 9.3(i) dan 9.3(ii)

(iv) Menyelenggara dan mengkonfigurasikan ciri-ciri keselamatan perkhidmatan ICT supaya selamat diguna pakai oleh pengguna;

(v) Mengikuti perkembangan semasa keselamatan ICT dan mengambil langkah bersesuaian untuk meningkatkan kekebalan keselamatan peralatan dan perkhidmatan ICT;

(vi) Pentadbir sistem maklumat / pangkalan data bertanggungjawab membuat penyalinan (backup) data dan maklumat pengguna yang terdapat pada komputer-komputer server yang diselenggarakan;

(vii) Menyedia dan mengambil langkah-langkah keselamatan lain seperti penyediaan pendinding keselamatan (firewall), peralatan pemantauan, dan lain-lain peralatan dan perkhidmatan keselamatan yang difikirkan perlu;

(viii) 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

(ix) Melaksanakan Garis panduan penyiasatan sebagaimana yang disediakan oleh MAMPU untuk menangani insiden-insiden pencabulan keselamatan.

8.3.2 Bukan Tanggungjawab UiTM

Sekiranya berlaku kesilapan mekanikal ke atas peralatan ICT yang disediakan oleh PSMB yang menyebabkan keselamatan, integriti dan kandungan maklumat atau data yang dilindungi terjejas, dan kesilapan ini berlaku di luar jangkaan dan keperluan teknikal PSMB, maka PSMB 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 PSMB.

8.3.3 Tanggungjawab Pengguna dan Jabatan

(i) Mematuhi peraturan-peraturan yang telah ditetapkan oleh UPPICT

(ii) 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.

(iii) Tidak memberi atau membenarkan dengan sengaja orang perseorangan atau individu lain menggunakan kemudahan dan perkhidmatan ICT yang disediakan oleh UiTM di atas identiti beliau.

(iv) 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.

(v) Jabatan perlu memastikan data dan maklumat dibawah pengurusannya sentiasa tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;

(vi) Jabatan perlu Bertanggungjawab membuat salinan (backup) data, fail dan program kepunyaan sendiri yang dimiliki dan disimpan di komputer atau server masing-masing.

9 GARIS PANDUAN KERAHSIAAN MAKLUMAT UiTM

9.1 Tujuan

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

9.2 Objektif

(i) Memelihara kerahsiaan data dan maklumat UiTM

(ii) Memelihara integriti data dan maklumat UiTM

(iii) Memelihara keberadaan data dan maklumat UiTM

9.3 Pernyataan

9.3.1 Capaian Maklumat Sulit

(i) Pentadbir operasi sesuatu sistem atau sumber IT 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.

(ii) Jika pengguna disyaki melanggar *Garis panduan 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 *Garis panduan 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 JPPK.

(iii) 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 CIO boleh mencapai maklumat atau data sulit atau rahsia pengguna seperti e-mel atau fail-fail yang tersimpan dalam akaunnya.

(iv) 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 *Garis panduan Capaian Teknologi Maklumat*.

(v) Pengguna ditegah menyimpan data atau maklumat sensitif, rahsia atau sulit di dalam akaunnya.

(vi) Sebarang permohonan untuk mendapatkan data perlu mendapat kelulusan pemilik data terlebih dahulu.

9.3.2 Pemantauan Data dalam Rangkaian

(i) 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 *Garis panduan Keselamatan Operasi ICT*.

(ii) Sama seperti kes capaian maklumat di atas sekiranya pentadbir operasi mengesyaki pengguna melanggar *Garis panduan Keselamatan Operasi ICT*, maka pentadbir operasi mempunyai mandat tanpa mendapat kebenaran Setiausaha JPPK untuk memantau dan merekodkan data-data dalam 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 Jawatankuasa Penyiasat ICT UiTM.

(iii) 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.

10 GARIS PANDUAN KESELAMATAN OPERASI ICT

10.1 Tujuan

Tujuan garis panduan adalah untuk memastikan pengawalan dan pengurusan keselamatan ke atas perkakasan, perisian, aplikasi dan operasi komputer di UiTM. Ia mengandungi peraturan-peraturan yang perlu dipatuhi dalam menggunakan aset ICT. Tujuan utama garis panduan ini ialah untuk menerangkan kepada semua pengguna di UiTM mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT UiTM.

10.2 Objektif

(i) Menjamin semua aset ICT (kemudahan komputer, perisian, data, rangkaian dan peralatan) adalah dilindungi secukupnya daripada kehilangan, disalah guna atau penyelewengan;

(ii) Meminimumkan kerosakan ke atas aset ICT yang telah dikenal pasti;

(iii) Menjamin urusan ICT yang lancar serta berterusan; dan

(iv) Melindungi kepentingan mereka yang bergantung pada teknologi maklumat, daripada kesan kegagalan atau kelemahan ICT dari segi kerahsiaan, integriti, kebolehsediaan dan tidak boleh dipertikaikan.

10.3 Skop

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

10.4 Keselamatan Sistem Pengkomputeran

10.4.1 Kawalan Capaian Fizikal

(i) Kawalan terhadap individu/staf yang masuk ke Bilik Komputer dan juga kawalan akses kepada semua sistem pengkomputeran, dan

(ii) Mewujudkan mekanisme kawalan capaian fizikal untuk staf/individu mencapai sistem pengkomputeran berkenaan.

10.4.2 Kawalan Capaian Logikal

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

(i) Identiti Pengguna

(ii) 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.

(iii) 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 atau tamatkan perkhidmatan.

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

(iii) 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, dsbnya;

(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.

(iv) Had Cubaan Capaian

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

10.5 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 :

(i) capaian maklumat yang kritikal;

(ii) capaian perkhidmatan rangkaian; dan

(iii) capaian fungsi-fungsi ‘superuser.

(iv) 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 :

(a) meneliti dan melaporkan sebarang aktiviti yang diragui dengan segera;

(b) meneliti jejak audit secara berjadual;

(c) meneliti dan melaporkan sebarang masalah berkaitan keselamatan dan sesuatu kejadian yang di luar kebiasaan;

(d) menyimpan maklumat jejak audit untuk jangka masa tertentu untuk keperluan operasi; dan

(e) mengawal maklumat jejak audit daripada dihapus dan diubahsuai.

10.6 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 :

(i) prosedur backup dan restore didokumenkan;

(ii) menyimpan 3 generasi backup;

(iii) menyimpan salinan media backup di tempat lain yang selamat yang telah dikenal pasti oleh pihak pengurusan PSMB

(iv) media backup dan prosedur restore diuji dua (2) kali setahun.

Penyelenggaraan

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

(i) Melaksanakan Patches bagi mengatasi kelemahan sistem.

(ii) Dapatkan patches yang terkini daripada agensi keselamatan berdaftar seperti MyCERT (Malaysian Computer Emergency Response Team) di alamat web http://www.mycert.org.my/.

(iii) Melakukan peningkatan (upgrades) perisian dan firmware

(iv) Wujudkan prosedur pengemaskinian sistem pengoperasian daripada serangan dan ancaman.

10.7 Keselamatan Sistem Aplikasi

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

10.7.1 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 :

(i) Pengurusan ID pengguna secara berpusat;

(ii) Profil capaian berpandukan peranan dan keperluan capaian;

(iii) kawalan capaian yang konsisten berdasarkan had capaian pengguna.

(iv) kawalan aplikasi yang menentukan akauntabiliti tertentu kepada setiap pengguna untuk setiap transaksi;

10.7.2 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 :

(i) Sistem pengurusan pangkalan data yang memastikan integriti dalam pengemaskinian dan capaian maklumat. Kawalan perlu dilaksanakan untuk pangkalan data yang dikongsi bersama;

(ii) Kawalan capaian kepada maklumat ditentukan oleh Pentadbir Pangkalan Data;

(iii) Mekanisme kawalan capaian kepada sumber maklumat fizikal dan

(iv) 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'

10.7.3 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:

(i) gunakan data 'dummy' atau 'historical' untuk tujuan pengujian

(ii) hapuskan maklumat yang digunakan semasa pengujian sistem (terutamanya apabila menggunakan data historical)

(iii) Menghadkan capaian kepada staf yang dibenarkan semasa ujian dilaksanakan.

10.7.4 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 :

(i) wujudkan program jaminan kualiti untuk semua perisian yang dibangunkan secara dalaman atau luaran.

(ii) pastikan semua perisian didokumenkan, diuji, disahkan fungsinya, tahan lasak (robustness) dan menepati spesifikasi.

10.7.5 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. (jelaskan prosedurnya)

10.7.6 Penyimpanan Kod Sumber (Source Code)

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

(i) mewujudkan prosedur untuk menyelenggara versi terkini perisian dan

(ii) mewujudkan perjanjian untuk keadaan di mana berlakunya kerosakan atau bencana dan kod sumber tidak ada.

10.7.7 Perisian Tidak Berlesen

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

10.7.8 Kod Jahat (Malicious Code)

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

(i) melaksanakan prosedur untuk menguruskan 'malicious code';

(ii) Mematuhi garis panduan berkaitan memuat turun, penerimaan dan penggunaan perisian percuma (freeware dan shareware);

(iii) menyebarkan arahan dan maklumat untuk mengesan 'malicious code' kepada semua pengguna; dan

(iv) mendapatkan bantuan sekiranya disyaki dijangkiti virus dan lain-lain.

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

(i) menyimpan semua salinan utama untuk semua perisian, data dan maklumat untuk tujuan 'restore'; dan

(ii) memastikan semua data di'backup' secara berkala.

Bagi masalah serangan virus, ikuti langkah-langkah berikut :

(i) gunakan perisian anti virus yang telah diluluskan;

(ii) scan virus secara berkala.

(iii) tidak melaksana (run) atau membuka fail kepilan (attachment) daripada e-mel yang meragukan.

10.7.9 Keselamatan Penggunaan E-mel

10.7.9.1 Akaun E-mel

(i) Akaun e-mel bukan hak mutlak seseorang. Ia adalah kemudahan yang disediakan tertakluk kepada peraturan UiTM dan boleh ditarik balik jika penggunaannya melanggar peraturan.

(ii) 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.

(iii) Kata laluan tidak boleh didedahkan kepada pengguna lain. Pendedahan akan membolehkan pengguna lain menyalahgunakan kemudahan tanpa pengetahuan pemilik akaun.

10.7.9.2 Menyelenggara Kotak Mel (Mail Box)

(i) Kandungan dan penyelenggaraan kotak mel adalah tanggungjawab pengguna.

(ii) Pengguna harus menghadkan jumlah e-mel yang disimpan di dalam kotak mel. Hapuskan e-mel yang difikirkan tidak perlu disimpan.

(iii) Pengguna hendaklah memastikan fail yang dihantar melalui lampiran (attachment) bebas daripada virus

(iv) E-mel tidak boleh mengandungi maklumat rahsia yang boleh disalah guna.

10.7.9.3 Penggunaan Perisian Mel

(i) Pengguna digalakkan mengguna perisian mel rasmi lotus notes UiTM

(ii) Pengguna yang tidak menggunakan perisian mel rasmi UiTM dinasihatkan sentiasa membuat 'backup' terhadap data-data e-mel.

11 GARIS PANDUAN KESELAMATAN RANGKAIAN

11.1 Tujuan

Garis panduan ini bertujuan untuk menerangkan pelaksanaan keselamatan UiTMNet bagi tujuan komunikasi dan perkongsian maklumat/sumber termasuk capaian ke Internet termasuk rangkaian tanpa wayar.

11.2 Objektif

(i) Keselamatan UiTMNet lebih terjamin

(ii) Pengguna dimaklumkan tentang kewujudan Garis panduan keselamatan sistem rangkaian.

(iii) Mengelakkan ancaman 'hacker'

(iv) Mengelakkan berlaku tindanan saluran dan menyebabkan gangguan sistem rangkaian wireless

(v) Memastikan keselamatan UiTMNet

(vi) Sistem wireless dapat berfungsi dengan baik

11.3 Skop

Skop Garis panduan ini merangkumi semua jenis peralatan komunikasi data berwayar atau tanpa wayar yang bersambung ke UiTMNet dan mampu menghantar packet data.

11.3.1 Rekabentuk Keselamatan Rangkaian

Melibatkan rekabentuk keselamatan rangkaian yang mengambilkira perkara-perkara berikut:

(i) Matlamat, objektif dan skop keselamatan (sama ada meliputi end-to-end security, inter-network security atau keselamatan pada tahap sistem dalaman sahaja).

(ii) Aset-aset yang perlu dilindungi termasuk jenis-jenis maklumat dan tahap keselamatan yang diperlukan.

(iii) Menggunakan konsep VLAN dan sistem rangkaian berhiraki

(iv) Potensi ancaman dan serangan (vulnerabilities) serta mewujudkan sistem pencegahan, garis panduan dan prosedur untuk melindungi maklumat.

11.3.2 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 Detection System (IDS) bagi mengesan sebarang cubaan menceroboh atau aktiviti yang luar biasa. IDS seharusnya boleh mengesan aktiviti seperti ping, scanning, denial of service attack dan meneka kata frasa yang rapuh;

11.4 Keselamatan Peralatan Rangkaian

11.4.1 Keselamatan Fizikal

(i) Peralatan rangkaian ditempatkan di tempat yang bebas daripada risiko di luar jangkaan seperti banjir, gegaran, kekotoran dan sebagainya.

(ii) Suhu hendaklah terkawal di dalam limit suhu peralatan rangkaian berkenaan.

(iii) 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;

(iv) Kitaran udara yang baik.

11.4.2 Keselamatan peralatan tanpa wayar

(i) Semua komputer yang disambungkan ke UiTMNet secara wireless perlu menepati standard keselamatan yang ditetapkan oleh PSMB. Data yang dihantar secara wireless perlu dienkripkan dan pengguna perlu menggunakan *certificate* yang ditetapkan oleh PSMB.

11.4.3 Capaian Fizikal

(i) Capaian Pengkabelan Rangkaian

(a) langkah-langkah sewajarnya perlu diambil untuk melindungi kabel rangkaian daripada di capai oleh orang yang tidak berkenaan;

(b) melindungi pengkabelan di dalam kawasan awam dengan cara memasang 'conduit' atau lain-lain mekanisme perlindungan; dan

(c) pusat pendawaian diletakkan di dalam ruang atau bilik yang berkunci dan hanya boleh dicapai oleh staf yang dibenarkan sahaja.

(ii) 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.

11.4.4 Capaian Logikal

Kata laluan diperlukan untuk mencapai Sistem Rangkaian. Capaian hanya boleh dibuat oleh staf yang dibenarkan sahaja.

(i) Komposisi kata laluan mestilah konsisten dengan garis panduan yang telah ditetapkan.

(ii) 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.

(iii) Rangkaian hanya menerima trafik daripada alamat IP dalaman yang berdaftar sahaja.

(iv) Semua perubahan konfigurasi suis rangkaian hendaklah dilogkan termasuk nama pengguna yang membuat perubahan, pengesahan, tarikh dan masa. Maklumat mestilah disimpan selama 90 hari.

(v) Perubahan konfigurasi perisian mestilah direkodkan – pegawai yang membuat perubahan, pegawai yang membenarkan perubahan dibuat dan tarikh.

(vi) Perubahan konfigurasi hendaklah dikendalikan secara berpusat oleh Bahagian Rangkaian, PSMB.

(vii) Semua aktiviti di dalam rangkaian hendaklah direkodkan;

11.5 Konfigurasi Peralatan

Peralatan dikonfigurasi dengan betul dengan mengambil langkah-langkah berikut:

(i) 'enable' perkhidmatan yang diperlukan sahaja;

(ii) capaian untuk konfigurasi dihadkan melalui nod atau alamat IP yang dibenarkan sahaja;

(iii) 'disable' broadcast;

(iv) menggunakan kata laluan yang selamat; dan

(v) dilaksanakan oleh staf yang terlatih dan dibenarkan sahaja.

11.6 Penyelenggaraan Peralatan

(i) Peralatan hendaklah dipasang, dioperasi dan diselenggarakan mengikut spesifikasi pengilang.

(ii) Dibaiki dan diselenggara hanya oleh staf yang terlatih dan dibenarkan sahaja.

(iii) Mempunyai rekod penyelenggaraan.

11.7 Kebolehcapaian Pengguna (User Accessibility)

11.7.1 Rangkaian Setempat (Local Area Network)

(i) Hanya staf dan pelajar UiTM dibenarkan membuat penyambungan ke UiTMNet.

(ii) Hanya komputer kepunyaan staf dan pelajar UiTM yang dibenarkan untuk disambungkan ke UiTMNet.

(iii) Pengguna luar (selain staf dan pelajar) perlu mendapatkan kebenaran daripada Pengarah PSMB sebelum membuat capaian ke UiTMNet.

(iv) Hanya pengguna yang disahkan sahaja dibenarkan membuat capaian kepada sistem pengkomputeran UiTM.

(v) Perisian pengintip (sniffer) atau penganalisis rangkaian (network analyser) tidak boleh digunakan pada sebarang komputer.

11.8 Sambungan Dengan Lain-Lain Rangkaian

11.8.1 Capaian Yang Tidak Digalakkan

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

11.8.2 'Firewall'

(i) Semua trafik daripada dalam ke luar UiTM dan sebaliknya mestilah melalui 'firewall'.

(ii) Hanya trafik yang dibenarkan sahaja boleh melepasinya berasaskan kepada Garis panduan Keselamatan Rangkaian.

(iii) Rekabentuk 'firewall' hendaklah mengambilkira perkara-perkara berikut:

(a) keperluan audit dan arkib;

(b) kebolehsediaan;

(c) kerahsiaan; dan

(d) melindungi maklumat/UiTM.

11.8.3 Rangkaian Tanpa Wayar

(i) Access Point

Semua jenis wireless access point yang bersambung ke UiTMNet atau tidak bersambung ke UiTMNet perlu mendapat kelulusan pemasangan daripada Pengarah PSMB.

(ii) Enkripsi dan Authentikasi

Semua komputer yang disambungkan ke UiTMNet secara wireless perlu menepati standard keselamatan yang ditetapkan oleh PSMB. Data yang dihantar secara wireless perlu dienkripkan dan pengguna perlu menggunakan *certificate* yang ditetapkan oleh PSMB.

(iii) SSID

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

11.8.4 Pembukaan Port dan Service (Untuk Aplikasi)

(i) Bahagian Rangkaian, PSMB bertanggungjawab sepenuhnya mengawal selia capaian melalui port yang dibuka ke semua sistem dalam UiTMNet.

(ii) Bahagian Rangkaian, PSMB berhak menutup port yang memudaratkan keselamatan UiTMNet.

(iii) Kelulusan daripada Pengarah PSMB perlu diperolehi jika pengguna ingin membuka port tertentu yang dalam sistem UiTMNet untuk aplikasi tertentu.

(iv) 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.

12 GARIS PANDUAN MEMBANGUN LAMAN WEB DAN TAPAK HOSTING

12.1 Tujuan

Garis panduan ini bertujuan menyelaras dan mengawasi pembangunan laman web yang dibangunkan oleh pengguna untuk tujuan laman web peribadi bersesuaian sepertimana yang dikehendaki oleh UiTM.

12.2 Skop

Skop garis panduan ini melibatkan semua pembangunan laman web persendirian yang dibangunkan oleh staf UiTM.

12.3 Pernyataan Garis Panduan

(i) UiTM menggalakkan warga kampus membangunkan laman web, tetapi hanya laman web rasmi Jabatan/Bahagian/Fakulti/Cawangan atau seumpamanya sahaja yang boleh dipautkan dalam laman web rasmi UiTM.

(ii) 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.

(iii) PSMB berhak menentukan perisian pembangunan laman web bagi tujuan pengoptimumkan penggunaan dan keselamatan.

(iv) Keselamatan maklumat dan penyiaran adalah di bawah tanggungjawab individu (pembina laman web) dan perlu mengambil kira aspek keselamatan daripada pencerobohan pihak luar.

(v) **Laman web peribadi hendaklah berbentuk ilmiah dan bagi tujuan akademik**.

(vi) **Laman web yang berunsur politik, perniagaan dan pengiklanan adalah tidak di benarkan sama sekali.**

(vii) Pengiklanan komersial seperti *banner*, *Ads Adsense Google* atau mana-mana yang seumpamanya adalah tidak dibenarkan sama sekali diletakkan di dalam laman web individu.

(viii) 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.

(ix) Tidak memberi atau membenarkan dengan sengaja orang perseorangan atau individu lain mengendalikan laman web peribadi di atas identiti pemilik.

(x) 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.

(xi) UiTM berhak menamatkan mana-mana laman web peribadi yang melanggar syarat-syarat yang dinyatakan tanpa sebarang notis.

(xii) Pemilik laman web perlu membuat salinan atau *backup* terhadap laman web mereka sendiri.

(xiii) PSMB tidak bertanggungjawab ke atas sebarang kerosakan atau kehilangan maklumat pada *server* sehingga menyebabkan berlakunya kegagalan capaian maklumat.

12.3.1 Garis Panduan Penggunaan Hos Maya (Virtual Hosting)

(i) Setiap pengguna diberikan maksima 500Mb – 1000Mb ruang storan di server induk.

(ii) 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.

(iii) Sebarang masalah yang berkaitan dengan tahap penghantaran dan penerimaan data bagi tapak hos hendaklah dirujuk kepada PSMB untuk tindakan selanjutnya.

(iv) Pengguna/pemilik tapak tidak dibenarkan merosakkan sistem komputer atau data dengan apa jua cara seperti pengedaran virus komputer melalui tapak yang dihoskan.

(v) Jika didapati bahawa sumber maklumat UiTM telah disalahgunakan atau tidak mengikut peraturan yang ditetapkan, PSMB boleh menghadkan atau membatalkan akses kepada tapak hos tersebut dan seterusnya menamatkan perkhidmatannya.

13 GARIS PANDUAN PENGGUNAAN E-MEL

13.1 Tujuan Garis Tujuan Garis Panduan

(i) Garis panduan ini bertujuan menerangkan tatacara dan peraturan berkaitan penggunaan kemudahan emel yang disediakan kepada staf UiTM.

(ii) Emel adalah merupakan aplikasi yang membolehkan pengguna berkomunikasi antara satu sama lain dalam bentuk mesej elektronik.

(iii) Emel membolehkan dua atau lebih pengguna berkomunikasi antara satu sama lain dengan lebih mudah dan lebih pantas walaupun semua pengguna adalah terpisah secara fizikal.

13.2 Tanggung jawab dan Hak UiTM

(i) UiTM adalah bertanggungjawab menyediakan kemudahan emel kepada semua staf UiTM pada sepanjang tempoh perkhidmatan staf berkenaan.

(ii) Kemudahan emel yang disediakan kepada staf UiTM adalah merupakan hak mutlak UiTM.

(iii) UiTM adalah berhak untuk menarik balik kemudahan emel yang disediakan kepada staf UiTM pada bila-bila masa, sekiranya berlaku sebarang penyalahgunaan atau perlanggaran polisi oleh staf berkenaan atau atas sebab-sebab tertentu.

(iv) Kemudahan emel yang disediakan kepada staf UiTM akan ditamatkan atas sebab-sebab berikut :

a. Staf UiTM menamatkan perkhidmatan secara rasmi dengan UiTM (bersara, berhenti, tamat kontrak, dsb).

b. Staf UiTM menyalahguna atau melanggar sebarang polisi penggunaan kemudahan emel UiTM.

c. Staf UiTM memohon menamatkan kemudahan emel yang disediakan atas sebab-sebab tertentu.

13.3 Tanggung jawab Staf UiTM

(i) Staf UiTM adalah diwajibkan menggunakan kemudahan emel UiTM dalam semua urusan rasmi universiti.

(ii) Staf UiTM adalah tertakluk kepada polisi penggunaan kemudahan emel UiTM pada sepanjang tempoh menggunakan kemudahan berkenaan.

(iii) Staf UiTM adalah bertanggungjawab sepenuhnya bagi semua emel yang dihantar dan diterima melalui emel masing-masing.

(iv) Staf UiTM adalah tidak dibenarkan pada bila-bila masa, menggunakan akaun pengguna lain untuk menghantar dan menerima emel, sama ada dengan kebenaran atau tanpa kebenaran pemilik akaun berkenaan.

13.4 Pengguna

Kemudahan e-mel disediakan seperti berikut:-

(i) Semua staf UiTM melalui permohonan;

(ii) Semua Pelajar UiTM yang berdaftar

(iii) Jabatan atau persatuan rasmi UiTM melalui permohonan.

13.5 Pembukaan Akaun Pengguna

(i) Pembukaan akaun pengguna adalah berdasarkan kepada rekod lapor diri staf UiTM.

(ii) Staf UiTM adalah tidak dibenarkan pada bila-bila masa, memohon atau memiliki lebih daripada satu akaun pengguna.

(iii) Pembukaan akaun pengguna adalah mengikut format seperti berikut :

a. Nama pengguna :
<Nama Penuh>/<Jabatan >/UiTM
Contoh : Ahmad bin Ali/Pendaftar/UiTM
atau
<Nama Penuh>/<Kampus>/UiTM
Contoh : Ahmad bin Ali/Perak/UiTM

b. Alamat emel :
<namapenuh>@<kampus>.uitm.edu.my
Contoh : ahmadali@salam.uitm.edu.my

(iv) Alamat emel alternatif akan diberikan sekiranya berlaku pertindihan dengan akaun sedia ada

a. Kata laluan :
8 aksara (kombinasi huruf dan nombor)

(v) Pengguna akan dikehendaki menukar kata laluan masing-masing pada *login* kali pertama

(vi) Setiap akaun pengguna yang diberikan kepada staf UiTM adalah muktamad.

(vii) Staf UiTM adalah tidak dibenarkan pada bila-bila masa, menukar akaun pengguna selain daripada yang telah ditetapkan oleh UiTM.

13.6 Kapasiti Storan Emel

(i) Kapasiti storan emel yang diperuntukkan kepada staf UiTM adalah seperti berikut :

i.	Staf Pengurusan Tertinggi	-	1 GB
ii.	Staf Akademik	-	1 GB
iii.	Staf Pengurusan dan Profesional	-	1 GB
iv.	Staf Sokongan I & II	-	300 MB
v.	Staf kontrak/harian	-	300 MB
vi.	Lain-lain	-	300 MB

(ii) UiTM adalah berhak untuk menaiktaraf (*upgrade*) atau menuruntaraf (*downgrade*) kapasiti emel staf UiTM pada bila-bila masa dan atas sebab-sebab tertentu.

(iii) Kemudahan emel yang disediakan kepada staf UiTM adalah merupakan kemudahan komunikasi, serta bukan merupakan kemudahan storan emel, teks, imej, dokumen atau kepilan (*attachment*).

(iv) Staf UiTM adalah bertanggungjawab sepenuhnya dalam mengemaskini dan memadam emel masing-masing dari masa ke semasa bagi memastikan jumlah saiz emel, teks, imej, dokumen atau kepilan (*attachment*) tidak melebihi had kapasiti storan yang telah diperuntukkan.

(v) Staf UiTM adalah disarankan mencetak emel, serta memuatturun (*download*) teks, imej, dokumen atau kepilan (*attachment*) ke storan lain bagi memastikan jumlah saiz emel tidak melebihi had kapasiti storan yang telah diperuntukkan

(vi) UiTM adalah tidak bertanggungjawab atas sebarang kehilangan emel, teks, imej, dokumen atau kepilan (*attachment*) yang berlaku disebabkan oleh ketidakpatuhan atau kecuaian staf UiTM.

13.6.1 Pengurusan dan Keselamatan Akaun Pengguna

(i) Staf UiTM adalah bertanggungjawab sepenuhnya dalam memastikan keselamatan akaun pengguna dan kata laluan masing-masing.

(ii) Staf UiTM adalah bertanggungjawab memaklumkan kepada UiTM sekiranya mengesyaki berlaku penyalahgunaan atau pemecahan akaun pengguna masing-masing.

(iii) Staf UiTM adalah disarankan menggunakan kata laluan yang baik dan mempunyai ciri-ciri keselamatan seperti berikut :

a. Saiz minima 8 aksara dengan menggunakan kombinasi huruf dan nombor
b. Ditukar setiap 6 bulan, atau lebih kerap
c. Tidak pernah digunakan terlebih dahulu
d. Dihafal dan tidak disalin atau dicatat pada lokasi yang mudah dicapai oleh individu lain

13.6.2 Larangan Penyalahgunaan

(i) Staf UiTM adalah dilarang menggunakan kemudahan emel UiTM bagi tujuan menyedia, menyebar, menyimpan, memuatnaik (*upload*) atau memuatturun (*download*) sebarang emel, teks, imej, dokumen atau kepilan (*attachment*) yang mengandungi :

a. Unsur hiburan, lagu, audio, video atau permainan elektronik
b. Unsur komersial, iklan peribadi atau *spamming*
c. Unsur lucah, seksual atau gangguan seksual
d. Unsur politik, hasutan, fitnah atau penentangan
e. Unsur perjudian, perlanggaran undang-undang, jenayah berat atau aktiviti pengganas
f. Perisian tanpa lesen
g. Sebarang unsur lain yang boleh menjatuhkan nama baik UiTM.

(ii) Sebarang emel, teks, imej, dokumen atau kepilan (*attachment*) yang dihantar atau diterima menggunakan kemudahan emel UiTM, boleh dijadikan sebagai bahan bukti sekiranya berlaku sebarang penyalahgunaan atau perlanggaran polisi oleh staf UiTM.

(iii) UiTM berhak membuka mana-mana emel staf UiTM sekiranya berlaku sebarang penyalahgunaan kemudahan emel UiTM atau perlanggaran polisi oleh staf berkenaan.

(iv) Staf UiTM yang dibuktikan menyalahguna kemudahan emel UiTM akan diberi amaran dan boleh ditamatkan kemudahan berkenaan.

Senarai Rujukan

1. Akta Tandatangan Digital 1997
2. Akta Hakcipta (amendment) 1997
3. Akta Jenayah Komputer 1997
4. Akta Tele-medicine 1997
5. Akta Komunikasi dan Multimedia 1998
6. Akta Suruhanjaya komunikasi dan Multimedia Malaysia 1998
7. Pekeliling Am Bilangan 2 Tahun 1999, Jawatankuasa IT dan Internet Kerajaan.
8. Pekeliling Am Bilangan 6 Tahun 1999, Perlaksanaan Perkongsian Pintar Antara Agensi-Agensi Kerajaan Dalam Bidang Teknologi Maklumat
9. Pekeliling Am Bilangan 3 Tahun 2000, Rangka Garis panduan Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan
10. Pekeliling Am Bilangan 1 Tahun 2000, Garis Panduan Malaysian Civil Link (MCSL) dan Laman Web Agensi Kerajaan
11. Pekeliling Am Bil.1 Tahun 2001, Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT).
12. Surat Pekeliling Am Bil. 2 Tahun 2000, Peranan Jawatankuasa-Jawatankuasa dibawah Jawatankuasa IT dan Internet Kerajaan.
13. Pekeliling Am Bil. 2 Tahun 2002, Penggunaan dan Pemakaian Data Dictionary Sektor Awam Sebagai Standard di Agensi-Agensi Kerajaan
14. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 (Garis Panduan Mengenai Tatacara Penggunaan Internet dan mel elektronik di agensi-agensi kerajaan).
15. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003, Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan, MAMPU, 2003.
16. Surat Pekeliling Am Bilangan 4 Tahun 2004, Garis Panduan Mengenai Tatacara Memohon Kelulusan Teknikal Projek ICT Agensi Kerajaan (Tambahan Pertama Kepada SPA Bil. 2 Tahun 2000)
17. Surat Arahan Pematuhan Akta Keselamatan dan Kesihatan Pekerja 1994 dan Perlaksanaan Arahan, Peraturan, Prosedur dan Peruntukan Undang-Undang Berkaitan Keselamatan Perlindungan di Jabatan-Jabatan Kerajaan, 20 Ogos 2004.
18. Surat Pekeliling Am Bil. 2 Tahun 1995, Pengurusan Penyelenggaraan – Pewujudan Sistem Penyelenggaraan yang Dirancang
19. Standards, Policies and Guideline – Portal Guideline ver 1.0, MAMPU, August 2004.
20. Standards, Policies and Guidelines - Malaysian Government Interoperability Framework (MyGIF)

21. Standards, Policies and Guidelines - Channels Framework
22. ICT Strategic Plan (ISP) Guideline - MAMPU
23. Garis panduan Keselamatan ICT MAMPU
24. Garis panduan ICT UiTM Utara Malaysia
25. Garis panduan ICT UiTM Pendidikan Sultan Idris
26. Regulations for the Use of IT Facilities at the University of Liverpool
27. Macquarie University ICT Policy
28. The University of Sydney Policy on the Use of Information and Communications Technology (ICT) Resources: http://www.usyd.edu.au/ICTRPolicy/
29. http://www.ict.ox.ac.uk/oxford/rules/
30. http://www.harvard.edu/
31. http://www.cam.ac.uk/cs/
32. Undang-Undang lain yang berkaitan, Pekeliling Am MAMPU dari masa ke semasa.

Appendix I: Peraturan Am Penggunaan Makmal

Peraturan-peraturan berikut adalah peraturan umum penggunaan makmal komputer yang perlu dipatuhi oleh semua pengguna:-

(i) Pengguna mesti membuat tempahan mengikut syarat-syarat yang ditetapkan oleh pentadbir makmal

(ii) Pengguna tidak dibenarkan menganggu atau membuat perkara-perkara termasuk tetapi tidak terhad kepada:

(a) 'chatting' kecuali menggunakan yahoo massager;

(b) makan dan minum;

(c) menghisap rokok;

(d) membuat bising termasuk tetapi tidak terhad kepada berbual, berbincang, memasang dan mendengar muzik;

(e) menukar kedudukan komputer dan peranti;

(f) menukar konfigurasi komputer;

(g) menambah atau membuang sebarang perisian;

(h) menyimpan dan memindah turun maklumat atau data ke dalam komputer tanpa mendapat kebenaran penyelia makmal;

(i) membawa keluar sebarang peralatan dari makmal;

(j) mencuri peranti;

(k) mengganggu pengguna lain dengan apa cara sekalipun, termasuk menimbulkan rasa aib, marah dan tidak selesa; berkelakuan tidak senonoh dan mengaibkan;

(l) Pengguna perlu mendapatkan kebenaran pentadbir makmal untuk memasang perisian dalam komputer;

(m) Pengguna perlu mematuhi sebarang arahan tambahan dari pentadbir makmal yang bertugas; dan

(n) Pengguna perlu berpakaian mengikut sahsiah rupa diri pelajar sebagaimana yang berkuatkuasa.

Appendix II: Peraturan Tempahan Makmal Komputer

Semua penggunaan komputer di dalam makmal (sama ada yang disambung ke UiTMNet atau tidak) mesti direkodkan ke dalam buku log atau system yang berkuatkuasa. Rekod tersebut seharusnya mempunyai sekurang-kurangnya maklumat berikut: -

(i) Tarikh

(ii) Nama Pengguna

(iii) Nombor Kad Pelajar/No. Staf/No. Pengenalan

(iv) Masa mula penggunaan

(v) Masa tamat penggunaan

Buku log ini (sama ada berbentuk digital atau manual) perlu disimpan dengan baik sekurang-kurangnya untuk tempoh empat (4) tahun bagi tujuan rujukan jika diperlukan.

Appendix III: Peraturan Keselamatan Penggunaan E-Mail

Bagi tujuan keselamatan penggunaan, perkara berikut perlu diberikan perhatian oleh pengguna:

(i) Tukar kata laluan secara berkala (dicadangkan setiap 3 bulan) bagi mengelakan akaun e-mel dicerobohi;

(ii) Tidak berkongsi kata laluan dengan pengguna lain dan tidak melayan dengan mana-mana permintaan untuk mendapatkan kata laluan

(iii) Berhati-hati ketika menerima kepilan (attachments) Fail kepilan mungkin mengandungi 'letterboms' atau virus yang boleh merosakkan komputer dan UiTMNet. Fail kepilan yang sering mengandungi virus ialah fail yang mempunyai 'extension', '. exe', '.zip', 'pif', '.scr' dan sebagainya.

(iv) 'log out' setelah selesai sesi penggunaan e-mel bagi menyelamatkan akaun dari pencerobohan atau tutup 'browser' yang digunakan setelah sesi capaian e-mel selesai.

(v) Tidak menjawab e-mel yang tidak berkenaan (seperti 'spam', ugutan atau ofensif) kerana dengan menjawab e-mel yang sedemikian, pengguna mendedahkan diri aktiviti yang tidak bertanggungjawab. Pengguna bertanggungjawab melapor penerimaan e-mel sedemikian kepada pentadbir mel PSMB.

Appendix VI: Kategori Kesalahan Terhadap Pelanggaran Garis panduan ICT UiTM Teknologi MARA

JADUAL A: CONTOH KATEGORI PELANGGARAN DASAR PENGGUNAAN ICT UITM

Pelanggaran Penggunaan Kemudahan ICT UiTM	Kategori
Hacking into, meddling with, or damaging any other computer or service. eg trying to "break into" or "crash" another computer on the Internet.	*Major*
Using another person's identity or authorisation codes. eg, using someone else's username or password.	*Major*
Possessing, accessing or using any unauthorised hacker tools, whether hardware or software based. eg "packet sniffers" and "password crackers".	*Major*
Harassing any person. eg sending obscene messages, language, pictures or other materials; issuing threats of bodily harm; contacting a person repeatedly without legitimate reason; disrupting another person's lawful pursuits; and invading another person's privacy.	*Major*
Menggunakan access accounts atau passwords secara tidak sah	*Major*
Mencuri mana-mana atau apa-apa perkakasan, peranti komputer UiTM	Major
Menggunakan perisian tanpa lesen yang sah	Major
Menghalang pelajar lain daripada menggunakan kemudahan ICT UiTM di makmal komputer contohnya menggunakan kemudahan internet bukan untuk tujuan akedamik.	Minor
Bermain games internet dan chatting tanpa faedah.	Minor