



Dasar dan Peraturan ICT UKM

Versi 3.0
(Kuatkuasa 1 Jun 2010)



UNIVERSITI KEBANGSAAN MALAYSIA
National University of Malaysia

Dasar dan Peraturan ICT UKM (Versi 3.0)

Kandungan

Bab	Keterangan	Muka surat
Bab 1	Dasar Umum	2
1.1	Tujuan	2
1.2	Objektif	2
1.3	Skop	3
1.4	Definisi	3
1.5	Istilah	11
1.6	Am	12
1.7	Pelanggaran dan Tindakan Tatatertib	13
1.8	Pindaan dan Kemas kini	14
1.9	Pemakaian Dasar Teknologi Maklumat Peringkat Kebangsaan	14
Bab 2	Pengurusan ICT	16
2.1	Tujuan	16
2.2	Skop	16
2.3	Pusat Teknologi Maklumat	16
2.4	Majlis Teknologi Maklumat UKM	19
Bab 3	Perisian dan Perkakasan ICT	26
3.1	Tujuan	27
3.2	Skop	27
3.3	Perisian	27
3.4	Perkakasan ICT	30

Bab	Keterangan	Muka surat
Bab 4	Penggunaan Makmal Komputer	41
	4.1 Tujuan	42
	4.2 Skop	42
	4.3 Penggunaan Makmal	42
	4.4 Tempahan Makmal Komputer	43
	4.5 Rekod Penggunaan Komputer Makmal	43
	4.6 Budi Bicara Pentadbir Makmal Komputer	44
	4.7 Tindakan Penguatkuasaan dan Pematuhan	44
Bab 5	Pengurusan Rangkaian UKM	45
	5.1 Tujuan	46
	5.2 Skop	46
	5.3 Penyediaan Perkhidmatan Rangkaian UKM	46
	5.4 Konfigurasi Pengoperasian Rangkaian UKM	47
	5.5 Penyambungan Rangkaian UKM	47
	5.6 Penggunaan Kemudahan Rangkaian UKM	48
	5.7 Tindakan Penguatkuasaan dan Pematuhan	48
Bab 6	Penggunaan Intranet atau Internet	49
	6.1 Tujuan	50
	6.2 Skop	50
	6.3 Kemudahan E-Mel	50
	6.4 Pembangunan Laman Web	53
	6.5 Capaian Internet atau Intranet	55
	6.6 Tanggungjawab Pengguna	56
	6.7 Tindakan Penguatkuasaan dan Pematuhan	56
Bab 7	Akauntabiliti dan Kerahsiaan Maklumat	57
	7.1 Tujuan	58
	7.2 Skop	58

Bab	Keterangan	Muka surat
	7.3 Capaian Maklumat Rahsia Atau Sulit	58
	7.4 Pemantauan Data Dalam Rangkaian	60
	7.5 Pengurusan Maklumat Rahsia Atau Sulit	60
	7.6 Tindakan Penguatkuasaan dan Pematuhan	64
Bab 8	Keselamatan ICT	65
	8.1 Tujuan	66
	8.2 Skop	66
	8.3 Keselamatan Perisian Aplikasi	66
	8.4 Keselamatan <i>Server</i>	70
	8.5 Keselamatan Peralatan Rangkaian	74
	8.6 Keselamatan Rangkaian	77
	8.7 Keselamatan Akaun e-Mel	78
	8.8 Jejak Audit	80
	8.9 Pengurusan Insiden Keselamatan ICT	81
	8.10 Tindakan Penguatkuasaan dan Pematuhan	82
Bab 9	Penguatkuasaan dan Pematuhan	83
	9.1 Tujuan	84
	9.2 Skop	84
	9.3 Jenis Pelanggaran	84
	9.4 Jenis Pelanggaran dan Tindakan Terhadap Pelanggaran	85
Bab 10	e-Pembelajaran	91
	10.1 Tujuan	92
	10.2 Skop	92
	10.3 Takrif	92
	10.4 Umum	93

Bab	Keterangan	Muka surat
10.5	Tahap Pelaksanaan e-Pembelajaran	94
10.6	Peranan dan Tanggungjawab	95
10.7	Hak Cipta dan Harta Intelek	99
10.8	Lain-lain	99
Bab 11	Perihal Pemakaian Dasar, Pematuhan Dan Pertikaian Undang-Undang	100
11.1	Pemakaian Dasar Teknologi Maklumat UKM	101
11.2	Pemakaian Peruntukan Undang – Undang Malaysia	101
11.3	Pematuhan Kepada Undang – Undang	101
11.4	Pertikaian Undang-Undang	101

Lampiran			
Lampiran	Keterangan	Rujukan (Bab)	Muka surat
A	Struktur Majlis Teknologi Maklumat	2	103
B	Terma Rujukan Ketua Pegawai Maklumat (CIO)	2	104
C	Senarai Tugas Pegawai Keselamatan ICT (ICTSO)	2	106
D	Garis Panduan Pembangunan Laman Web	6	108



UNIVERSITI KEBANGSAAN MALAYSIA
National University of Malaysia

Dasar dan Peraturan ICT Universiti Kebangsaan Malaysia

Bab 1: Dasar Umum ICT

Bab 1: Dasar Umum ICT

1.1 Tujuan

Satu dasar penggunaan sumber Teknologi Maklumat dan Komunikasi (ICT) di Universiti Kebangsaan Malaysia (UKM) yang merangkumi pembangunan, penyelenggaraan dan penggunaan infrastruktur, pembangunan perisian aplikasi, sokongan teknikal dan keselamatan ICT oleh warga UKM dan pihak-pihak lain yang berurusan dengan UKM. Mana-mana dasar terperinci seperti Akta, Statut, Arahan, Peraturan sedia ada untuk setiap sumber yang disenaraikan adalah mengatasi Dasar Umum ini.

1.2 Objektif

Penggunaan ICT oleh warga UKM dan pihak-pihak lain merupakan suatu peranan penting dalam mencapai wawasan dan misi UKM. Dasar ini bertujuan memastikan:

- i. warga UKM dan pihak-pihak lain dimaklumkan mengenai kewujudan dan peranan Dasar Teknologi Maklumat dan Komunikasi (ICT) Universiti Kebangsaan Malaysia;
- ii. kemudahan ICT digunakan secara bijaksana mengikut dasar yang ditetapkan;
- iii. tanggungjawab pengguna dan pihak-pihak lain dimaklumkan; dan
- iv. kerosakan, kemusnahan dan penyalahgunaan ICT dapat diminimumkan.

1.3 Skop

1.3.1 Sumber

Sumber ICT yang digunakan untuk pembangunan, penyelenggaraan dan penggunaan infrastruktur, pembangunan perisian aplikasi, sokongan teknikal dan keselamatan ICT adalah juga tertakluk kepada Dasar ini.

Sumber ICT yang diperolehi dan pembangunan perisian aplikasi hendaklah mengambilkira ciri-ciri IPv6 untuk mempertingkatkan prestasi, kestabilan dan ciri-ciri keselamatan.

1.3.2 Pengguna

Semua pengguna adalah tertakluk kepada dasar ini. Sesiapa yang tidak diberi kebenaran adalah dianggap sebagai penceroboh dan boleh diambil tindakan yang sesuai mengikut kesalahan yang dilakukan, sebagaimana yang disebut dalam Dasar ICT, UKM.

1.4 Definisi

Definisi berikut digunakan dalam Pernyataan Dasar yang berkaitan dengan penggunaan kemudahan ICT di UKM:

Penyataan	Definisi
Aktiviti Atau Kegiatan Yang Dijalankan	Arahan yang dilaksanakan (<i>run</i>) atau <i>keystrokes</i> yang ditaip semasa pengguna berinteraksi dengan sumber ICT yang disediakan oleh UKM
Akaun Pengguna	Ruang storan yang telah diperuntukkan kepada setiap pengguna yang sah dalam sesuatu sistem atau sumber ICT. Setiap pengguna dikenalpasti melalui penggunaan identifikasi pengguna (ID)

Penyataan	Definisi
Access Point (AP)	Peralatan yang membenarkan capaian wayarles untuk berhubung dengan rangkaian
Chief Information Officer (CIO)	Ketua Pegawai Maklumat yang bertanggungjawab ke atas perancangan, pengurusan, penyelarasan dan pemantauan program ICT di UKM
Chief Operating Officer (COO)	Ketua Pegawai Operasi yang bertanggungjawab ke atas semua pengoperasian di PPUKM termasuk ICT
Dynamic Host Configuration Protocol (DHCP)	Protokol atau prosedur yang digunakan oleh aplikasi rangkaian untuk mendapatkan maklumat konfigurasi secara automatik untuk beroperasi di dalam rangkaian
File Transfer Protocol (ftp)	Protokol atau prosedur rangkaian yang digunakan untuk pemindahan fail dalam rangkaian
Hypertext Transfer Protocol Secure (https)	Gabungan protokol atau prosedur pemindahan <i>hypertext</i> secara penggunaan http dalam lapisan yang selamat
Information And Communication Technology (ICT)	Merangkumi produk, peralatan dan perkhidmatan yang digunakan untuk menyimpan, mencapai, memanipulasi, menghantar dan menerima data dalam bentuk digital
Information And Communication Technology Security Officer (ICTSO)	Pegawai Keselamatan ICT yang bertanggungjawab ke atas keselamatan ICT di UKM

Penyataan	Definisi
Insiden Keselamatan ICT	Musibah yang mengakibatkan perkhidmatan ICT terjejas atau tidak berfungsi sebagaimana dirujuk di dalam Bab 8
Internet Protocol (IP)	Protokol atau prosedur yang digunakan sebagai komunikasi data di dalam rangkaian
Jejak Audit Atau Audit Trail	Satu jejak audit adalah urutan kronologi rekod audit yang digunakan untuk mengenalpasti akauntabiliti pengguna sekiranya berlaku sebarang masalah
Kakitangan	Seseorang yang dilantik oleh UKM atau badan-badan lain di bawah UKM untuk menjawat jawatan sama ada sebagai kakitangan akademik atau kakitangan bukan akademik sama ada secara tetap, sementara atau kontrak dan masih berkhidmat
Kemudahan ICT	Termasuk, tetapi tidak terhad kepada sistem komputer peribadi, terminal, sistem komputer, alat komunikasi peribadi, 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 UKM. Ia termasuk semua kemudahan yang disediakan oleh UKM secara terpusat dan yang disediakan melalui PTJ
Kios	Kemudahan komputer yang disediakan untuk mengakses maklumat dan capaian SMU oleh warga UKM di PTJ dan lokasi yang ditetapkan
Maklumat Peribadi	Data atau maklumat tentang seseorang individu, termasuk nama, tarikh lahir dan

Penyataan	Definisi
	<p>sebagainya; yang mana data ini boleh digunakan untuk mengenali seseorang individu</p> <p>Contoh: nombor kad pengenalan, nombor kakitangan dan sebagainya</p>
<p>Maklumat Rahsia Atau Sulit</p>	<p>Teks, grafik, audio, animasi dalam pelbagai format sama ada yang boleh dicerna seperti teks ataupun dalam format binari yang terdapat dalam akaun pengguna.</p> <p>Maklumat ini juga boleh dicapai semasa dalam medium penghantaran (transmisi) seperti data e-mel dalam talian atau dalam simpanan fail sementara</p>
<p>Makmal Komputer</p>	<p>Adalah kemudahan yang disediakan oleh UKM bagi menyokong aktiviti pentadbiran, pengajaran dan pembelajaran, pembangunan dan penyelidikan dan perkhidmatan. Penggunaan makmal komputer merangkumi aktiviti yang dilakukan di dalam makmal atau secara atas talian terus ke makmal.</p>
<p>MAMPU</p>	<p>Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, Jabatan Perdana Menteri</p>
<p>Open System Interconnection (OSI)</p>	<p>Piawaian rekabentuk rangkaian (1977 oleh <i>International Organization for Standardization</i>)</p>
<p>Patches</p>	<p>Merupakan tampalan perisian (<i>small piece of software</i>) yang direkabentuk bagi mengemaskini atau menyelesaikan masalah sedia ada dan mengemaskini pengaturcaraan komputer dan data yang disokong oleh komputer berkenaan. Ia merangkumi ciri keselamatan terkini untuk mengatasi pepijat dan meningkatkan prestasi kebolegunaan</p>

Penyataan	Definisi
Pelayan	Komputer berkeupayaan tinggi yang memberikan perkhidmatan kepada komputer lain Contoh: capaian ke fail data, aplikasi dan sebagainya
Personal Digital Assistant (PDA)	Berfungsi sebagai alat komunikasi mudah alih peribadi yang dilengkapi dengan kemudahan e-mel, internet, diari, penyimpanan data (<i>data storage</i>), perisian aplikasi contohnya: MS Word, Excel dan sebagainya
Pelajar	Seseorang yang mendaftar sesuatu program akademik (sama ada sepenuh masa atau separuh masa) di UKM dan statusnya masih aktif
Pemilik Maklumat / Pemilik Sistem	UKM sebagai organisasi yang memiliki semua sistem aplikasi yang dibangunkan secara dalaman atau perisian yang diperolehi serta maklumat yang dihasilkan melalui sistem aplikasi
Pembangun Sistem	Pasukan Pembangun Sistem yang bertanggungjawab membangun dan menyelenggara sistem aplikasi
Pemberi Maklumat	Pejabat yang bertanggungjawab memberikan maklumat setelah disahkan oleh Urus Setia Sistem Aplikasi
Pengguna	Seseorang atau kumpulan orang yang dibenarkan menggunakan kemudahan ICT UKM
Pentadbir Makmal Komputer	Individu yang diberikan tanggungjawab terhadap pengurusan makmal komputer di PTJ

Penyataan	Definisi
Pentadbir Pangkalan Data	Pegawai yang diberikan tanggungjawab terhadap pengurusan pangkalan data
Pentadbir Sistem	Pegawai yang bertanggungjawab mengurus, mengawal, memantau dan menyelenggara operasi dan keselamatan <i>server</i> dan data yang disimpan
Pentadbir Rangkaian	Pegawai yang bertanggungjawab mengurus, mengawal, memantau dan menyelenggara operasi dan keselamatan rangkaian UKM
Penasihat Sistem	Individu yang dilantik untuk memberi nasihat teknikal pembangunan SMU
Perisian	Kod atur cara (<i>program code</i>) yang diperolehi; atau sistem aplikasi yang dibangunkan secara dalaman. Perisian merangkumi perisian aplikasi dan perisian sistem
Perisian Aplikasi	Kumpulan atur cara komputer yang dibina bagi menyelesaikan masalah khusus atau melaksanakan tugas tertentu Contoh: Microsoft Office, Sistem Maklumat Universiti
Perisian Sistem	Kumpulan atur cara dan kemudahan (<i>utility</i>) yang membolehkan komputer berfungsi dan beroperasi
Perkakasan ICT	Peralatan dan komponen ICT Contoh: komputer, <i>notebook</i> , pencetak, pengimbas, <i>LCD Projector</i> dan sebagainya
Perunding Rangkaian UKM	Individu yang dilantik sebagai perunding untuk merangka keperluan teknologi terkini, memberi khidmat nasihat pembangunan rangkaian dan menjalankan pengujian terhadap sistem rangkaian yang dibangunkan

Penyataan	Definisi
Pihak-Pihak Lain	Pihak-pihak yang bertanggungjawab menyediakan, mengurus, membekal, menyelenggara perkhidmatan di UKM
Postmaster	Pegawai yang diberikan tanggungjawab memantau dan menyelenggara sistem e-mel UKM
Pusat Tanggungjawab (PTJ)	Semua jabatan, fakulti, pusat dan institut di UKM
Pusat Teknologi Maklumat (PTM)	Merangkumi PTM UKM dan PTM PPUKM
Rangkaian UKM	Infrastruktur rangkaian ICT UKM yang terdiri daripada rangkaian tulang belakang (<i>backbone</i>), rangkaian kawasan setempat (<i>LAN</i>) dan rangkaian wayarles (<i>WIFI</i>)
Service Set Identifier (SSID)	Nama yang digunakan untuk mengenalpasti perkhidmatan wayarles (AP)
Sistem Maklumat Universiti (SMU)	Sistem yang mengandungi semua aplikasi berkaitan dengan fungsi utama UKM
Sumber Rangkaian	Peralatan dan komponen yang digunakan dalam sistem rangkaian seperti access point, <i>switch</i> , <i>hub</i> , <i>router</i> dan sebagainya
Transmission Control Protocol (TCP)	Protokol atau prosedur aras empat (4) dalam <i>Open System Interconnection (OSI)</i> yang digunakan sebagai kawalan penghantaran data
Tuan Punya Maklumat	Individu yang boleh dikenal pasti melalui maklumat peribadi sedia ada
Urus Setia Sistem Aplikasi	Pusat Tanggungjawab (PTJ) yang bertanggungjawab menggerakkan

Penyataan	Definisi
	pelaksanaan sesuatu sistem aplikasi dan menentukan sebarang perubahan ke atas sistem aplikasi tersebut serta bertanggungjawab ke atas pengwujudan, pengemaskinian dan kesahihan maklumat
Universiti Kebangsaan Malaysia (UKM)	Termasuk fakulti, institut, pusat, jabatan, kolej kediaman dan badan-badan lain di bawah pengurusan dan pengawalan Universiti Kebangsaan Malaysia termasuk anak-anak syarikat di bawahnya
UKM Computer Response Team (UKMCERT)	Pasukan yang bertanggungjawab memantau dan mengambil tindakan ke atas insiden keselamatan ICT di UKM
Warga UKM	Kakitangan dan pelajar UKM yang berdaftar

1.5 Istilah

Bahasa Inggeris	Bahasa Melayu
Access Point	Titik Akses
Attachment	Fail lampiran
Audit Trail	Jejak Audit
Back Up	Penyalinan
E-Mail	e-Mel
Information And Communication Technology (ICT)	Teknologi Maklumat Dan Komunikasi
Keystrokes	Ketukan Kekunci
Mail Box	Peti Mel
Online	Atas Talian
Recovery	Pemulihan
Server	Pelayan
Sniffer	Pengintip
Source Code	Kod Sumber
Wired	Berwayar

Bahasa Inggeris	Bahasa Melayu
Stakeholder	Pihak Berkepentingan

1.6 Am

- i. UKM bertanggungjawab menyediakan kemudahan ICT untuk kegunaan kakitangan akademik, pentadbiran, sokongan dan pelajar bagi menyokong fungsinya;
- ii. Semua kemudahan dan perkhidmatan ICT yang disediakan oleh UKM adalah hak milik UKM. Pengguna diberi keistimewaan untuk menggunakan kemudahan tersebut berdasarkan keperluan tugas dan bukannya hak yang diberikan kepadanya. UKM berhak menarik balik kebenaran dan atau kemudahan yang diberikan pada bila-bila masa tanpa notis;
- iii. Kemudahan ICT yang disediakan oleh UKM hanya boleh digunakan untuk tujuan yang berkaitan dengan fungsi UKM. Penggunaan selain daripada itu seperti untuk tujuan peribadi, komersil dan politik adalah tidak dibenarkan;
- iv. Pengguna yang menggunakan peralatan ICT peribadi yang dibenarkan di dalam kampus juga tertakluk kepada dasar ini. Sebarang penggunaan adalah tertakluk kepada undang-undang negara dan dasar UKM. UKM tidak akan bertanggungjawab terhadap sebarang penyalahgunaan yang dilakukan oleh pengguna;
- v. Setiap pengguna mesti mematuhi Dasar ICT yang ditetapkan selaras dengan hasrat UKM mewujudkan pengguna yang beretika dan menghormati pengguna yang lain;
- vi. UKM bertanggungjawab memastikan pelaksanaan Dasar ICT dan syarat yang berkaitan dengan pengguna dan kod etika diamalkan selaras dengan kemudahan di bawah kawalannya;
- vii. Ketua PTJ bertanggungjawab memastikan Dasar ICT diamalkan selaras dengan kemudahan di bawah kawalan dan pengurusannya; dan

- viii. Dasar ini adalah tertakluk kepada perubahan dan pindaan dari semasa ke semasa mengikut keperluan. UKM berhak meminda, membatalkan, menghadkan dan menambah mana-mana Dasar ICT mengikut kesesuaian dan keperluan semasa.

1.7 Pelanggaran dan Tindakan Tatatertib

- i. Pelanggaran dasar ini boleh mengakibatkan tindakan tatatertib diambil terhadap kakitangan dan pelajar. Mereka boleh dihalang atau digantung daripada menggunakan atau mendapatkan kemudahan ICT yang disediakan.
- ii. Pelajar yang melanggar dasar ini boleh dikenakan tindakan tatatertib di bawah Kaedah-kaedah UKM (Tatatertib Pelajar-pelajar) 1999 [P.U.(A)209/1999].
- iii. Kakitangan berstatus tetap Universiti boleh dikenakan tindakan tatatertib di bawah Akta Badan-badan Berkanun (Tatatertib dan Surcaj) 2000 (Akta 605) atau mana-mana peruntukan undang-undang yang berkaitan:
- a. Perlembagaan UKM Tahun 2009 S.6 dan S.12
 - b. Akta Rahsia Rasmi 1972 (Akta 88) S.8
 - c. Akta Komunikasi dan Multimedia 1998 (Akta 588)
 - d. Akta Jenayah Komputer 1997 (Akta 563)
 - S.3 *Unauthorized Access to Computer Material*
 - S.4 *Unauthorized Access With Intent To Commit Or Facilitate Commission Of Further Offence*
 - S.5 Pengubahsuaian Tanpa Kuasa (*Unauthorized Modification Of The Contents Of Any Computer*)
 - S.6 *Wrongfull Communication*
 - S.7 Persubahatan dan Percubaan
- iv. Kakitangan berstatus kontrak, sementara dan sambilan pula boleh dikenakan tindakan sewajarnya termasuklah ditamatkan perkhidmatan.

1.8 Pindaan Dan Kemas Kini

Dasar ini adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial.

1.9 Pemakaian Dasar Teknologi Maklumat Peringkat Kebangsaan

Dasar ini tidak terhad kepada kandungan dokumen ini, malah ianya hendaklah dibaca bersama dengan dasar / garis panduan ICT peringkat kebangsaan yang dikuatkuasakan seperti berikut:

- i. Akta Universiti dan Kolej Universiti 1971 (Akta 30) Pindaan 2009 [A1342];
- ii. Surat Arahan MAMPU (MAMPU.BDPICT – 7/22(23) bertarikh 4 Januari 2010) – Garis Panduan Transisi Protokol Internet Versi 6 (IPV6) Sektor Awam;
- iii. Surat Pekeliling Am Bil. 1 Tahun 2008 : Garis Panduan Mengenai Tatacara Memohon Kelulusan Teknikal Projek ICT Agensi Kerajaan yang dikeluarkan oleh MAMPU;
- iv. Akta 680 - Akta Aktiviti Kerajaan Elektronik 2007;
- v. Arahan Teknologi Maklumat (2007) yang dikeluarkan oleh MAMPU;
- vi. Pekeliling Am Bil.4 Tahun 2006 : Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;
- vii. Pekeliling Am Bil.6 Tahun 2005 : Garis Panduan Melaksanakan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
- viii. Pekeliling Am Bil.1 Tahun 2003 : Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi Kerajaan;

- ix. Garis Panduan Pengurusan Keselamatan ICT Sektor Awam Malaysia (MyMIS) yang dikeluarkan oleh MAMPU;
- x. Pekeliling Am Bil.1 Tahun 2001: Mekanisme Pelaporan Insiden Keselamatan ICT (ICT) yang dikeluarkan oleh MAMPU;
- xi. Pekeliling Am Bil. 3 Tahun 2000: Dasar Keselamatan ICT Kerajaan yang dikeluarkan oleh MAMPU;
- xii. Pekeliling Am Bil.1 Tahun 2000: Garis Panduan Malaysian Civil Service Link (MCSL) dan Laman Web Kerajaan yang dikeluarkan oleh MAMPU;
- xiii. Pekeliling Am Bil. 6 Tahun 1999: Garis Panduan Pelaksanaan Perkongsian Pintar Antara Agensi-agensi Kerajaan Dalam Bidang Teknologi Maklumat yang dikeluarkan oleh MAMPU;
- xiv. Pekeliling Am Bil. 2 Tahun 1999: Penubuhan Jawatankuasa IT dan Internet Kerajaan (JITIK) yang dikeluarkan oleh MAMPU; dan
- xv. Undang-undang Siber (Cyber Law) yang diperkenalkan oleh kerajaan yang terdiri daripada akta berikut:
 - Akta Tandatangan Digital 1997 (Akta 562)
 - Akta Hakcipta 1997
 - Akta Jenayah Komputer 1997 (Akta 563)
 - Akta Tele-perubatan 1997
 - Akta Komunikasi dan Multimedia 1998 (Akta 588)
 - Akta Suruhanjaya Komunikasi dan Multimedia Malaysia 1998



UNIVERSITI KEBANGSAAN MALAYSIA
National University of Malaysia

Dasar dan Peraturan ICT Universiti Kebangsaan Malaysia

Bab 2: Pengurusan ICT

Bab 2: Pengurusan ICT

2.1 Tujuan

- i. Menerangkan terma rujukan Majlis Teknologi Maklumat yang bertanggungjawab menetapkan Dasar Teknologi Maklumat dan Komunikasi (ICT) dan memantau keberkesanan pelaksanaan ICT di UKM; dan
- ii. Menerangkan skop dan fungsi Pusat Teknologi Maklumat (termasuk Pusat Teknologi Maklumat PPUKM) di dalam melaksanakan pengurusan dan pembangunan ICT di UKM

2.2 Skop

Merangkumi pengurusan dan pembangunan ICT di UKM

2.3 Pusat Teknologi Maklumat

2.3.1 Fungsi dan Peranan Pusat Teknologi Maklumat

i. Perancangan ICT

- a. Perancangan hendaklah memenuhi fungsi dan keperluan UKM dalam pengajaran, pembelajaran, penyelidikan, perundingan, pentadbiran dan pengurusan; dan
- b. Perancangan hendaklah selaras dengan agenda ICT Negara dan mematuhi Dasar, Peraturan dan Garis Panduan yang ditentukan oleh Kerajaan Malaysia.

ii. Perolehan ICT

- a. Semua perolehan hendaklah mematuhi Prosedur Perolehan UKM dan Kerajaan kecuali bagi kes tertentu dengan mendapat perakuan atau kelulusan khas Bendahari UKM;
- b. Perolehan hendaklah memenuhi teknologi terkini dengan mendapat perakuan spesifikasi oleh PTM; dan
- c. Semua perisian aplikasi hendaklah mempunyai lesen yang sah ;

iii. Instalasi dan Penyelenggaraan

- a. Pemasangan perkakasan dan atau perisian dibekalkan oleh PTM adalah di bawah penyeliaan PTM kecuali yang diperolehi oleh PTJ; dan
- b. PTJ hendaklah memastikan peralatan ICT di bawah kawalannya diselenggara sewajarnya.

iv. Pengurusan Kesenambungan Perkhidmatan (*Business Continuity Management*)

PTM membangunkan Pelan Kesenambungan Perkhidmatan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan ICT. Ini bertujuan memastikan tiada gangguan kepada proses dalam penyediaan perkhidmatan UKM. Pelan ini hendaklah diluluskan oleh Majlis Teknologi Maklumat dan perkara berikut perlu diberi perhatian:

- a. Mengenalpasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;

-
- b. Melaksanakan prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang ditetapkan;
 - c. Mendokumentasikan proses dan prosedur yang telah dipersetujui;
 - d. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;
 - e. Membuat *back up* dan menguji dan mengemaskini pelan setahun sekali;
 - f. Memastikan Pusat Pemulihan Bencana (*Disaster Recovery Centre*) berada dalam keadaan tersedia; dan
 - g. Pelan Kesyinambungan Perkhidmatan hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan persekitaran atau fungsi perkhidmatan untuk memastikan ia sentiasa kekal berkesan.
- v. Naik taraf atau Pelupusan Perkakasan ICT**
- a. Semua naik taraf perkakasan dan perisian aplikasi (selain daripada yang dibangunkan secara dalaman) hendaklah mendapat kelulusan PTM; dan
 - b. Perkakasan ICT yang tidak berkeupayaan dan atau tidak sesuai untuk dinaiktaraf atau diperbaiki boleh dicadang untuk pelupusan mengikut Prosedur Pelupusan (rujuk Pekeliling Bendahari Bil.15/2008 dan Pekeliling Bendahari Bil.8/2009).

2.3.2 Pembangunan Sumber Manusia

- i. Merancang keperluan sumber manusia yang secukupnya bagi menyokong perkhidmatan ICT di UKM;
- ii. Merancang dan melaksana pelan pembangunan sumber manusia bagi meningkatkan pengetahuan dan kemahiran teknikal; dan
- iii. Merancang dan melaksana peningkatan pengetahuan dan kemahiran asas ICT serta penggunaan aplikasi ICT untuk pengguna.

2.4 Majlis Teknologi Maklumat UKM

2.4.1 Fungsi dan Peranan Majlis Teknologi Maklumat UKM

- i. menetapkan dasar dan dasar teknologi maklumat UKM;
- ii. memantau keberkesanan penggunaan teknologi maklumat;
- iii. menilai pencapaian penggunaan serta perancangan pelaksanaan teknologi maklumat di UKM
- iv. Pengerusi Majlis ialah Naib Canselor;
- v. Majlis dianggotai oleh:
 - Timbalan-Timbalan Naib Canselor;
 - Pendaftar;
 - Bendahari;
 - Ketua Pustakawan;
 - Penasihat Undang-undang Universiti atau wakil dari Fakulti Undang-undang yang dinamakan oleh Naib Canselor dengan syor daripada Dekan Fakulti Undang-undang;
 - COO PPUKM;

- Pengerusi Mesyuarat Jawatankuasa Infrastruktur dan Operasi;
 - Pengerusi Mesyuarat Jawatankuasa e-Pembelajaran;
 - Pengerusi Mesyuarat Jawatankuasa Tapak Web;
 - Pengerusi Mesyuarat Jawatankuasa Penyelarasan Maklumat;
 - Wakil MIMOS;
 - Wakil MAMPU;
 - Wakil MDEC;
 - Ahli lain yang akan dinamakan oleh Naib Canselor;
 - Pengarah Pusat Teknologi Maklumat (PTM) sebagai setiausaha;
- vi. Majlis Teknologi Maklumat perlu mengadakan mesyuarat empat (4) kali dalam tempoh 12 bulan;
- vii. Majlis Teknologi Maklumat dibantu oleh lima (5) Jawatankuasa Kerja iaitu:
- Jawatankuasa Infrastruktur dan Operasi yang dipengerusikan oleh Pengarah PTM yang juga CIO UKM;
 - Jawatankuasa e-Pembelajaran yang dipengerusikan oleh Timbalan Pengarah (e-Pembelajaran) Pusat Pembangunan Akademik;
 - Jawatankuasa Tapak Web yang dipengerusikan oleh Pengurus UNIKWeb;
 - Jawatankuasa Penyelarasan Maklumat yang dipengerusikan oleh Pengarah Pusat Perancangan dan Komunikasi Korporat; dan
 - Jawatankuasa Keselamatan ICT yang dipengerusikan oleh CIO atau mana-mana pihak yang dinamakan oleh Pengerusi Majlis Teknologi Maklumat dengan syor dari CIO.

- viii. Struktur Organisasi Majlis Teknologi Maklumat adalah seperti di **Lampiran A**.

2.4.2 Jawatankuasa Keselamatan ICT

- i. Jawatankuasa ini berperanan untuk merancang pelaksanaan, pemantauan dan penguatkuasaan serta mengemaskini Dasar ICT UKM;
- ii. Jawatankuasa ini dipengerusikan oleh Pengarah PTM yang juga CIO dan Pegawai Keselamatan ICT (ICTSO) sebagai setiausaha dan keahlian lain adalah dilantik oleh CIO; dan
- iii. Terma rujukan Jawatankuasa Keselamatan ICT adalah seperti berikut:
 - a. Membangun, menilai dan mengkaji semula Dasar ICT UKM dari semasa ke semasa;
 - b. Menyebar dan menguatkuasakan Dasar kepada Warga UKM dan memantau pematuhannya;
 - c. Menerima aduan insiden keselamatan ICT dan menjalankan siasatan teknikal ke atas sebarang pelanggaran Dasar;
 - d. Menyediakan laporan insiden keselamatan ICT berdasarkan laporan daripada UKMCERT dan mengemukakan kepada Jawatankuasa Tatatertib Kakitangan bagi kakitangan dan Pihak Berkuasa Tatatertib Pelajar bagi pelajar;
 - e. Memantau dan menambahbaik kaedah pelaksanaan keselamatan ICT di UKM;
- iv. Jawatankuasa perlu mengadakan mesyuarat empat (4) kali dalam tempoh 12 bulan; dan
- v. Jawatankuasa boleh mengadakan mesyuarat pada bila-bila masa jika pada pandangan Jawatankuasa adalah perlu dan mustahak bagi tujuan membincangkan langkah-langkah

keselamatan ICT semasa dan atau membincangkan apa-apa perkara yang perlu dibincangkan dengan segera bagi kepentingan keselamatan ICT di UKM.

2.4.3 CIO

i. Pelantikan CIO

Pelantikan CIO adalah memenuhi keperluan Pekeliling Ketua Setiausaha Negara bertarikh 22 Mac 2000.

Kompetensi Teras CIO

Kompetensi teras CIO (rujuk Buku Panduan CIO Sektor Awam Versi 1.0 oleh MAMPU) terbahagi kepada dua jenis iaitu Kompetensi Pengurusan dan Kompetensi Teknologi:

a. Kompetensi Pengurusan

- Dasar dan Organisasi
- Kepimpinan atau Pengurusan
- Hubungan Strategik
- Pengurusan Perubahan
- Pengurusan Potfolio/Program/Projek
- Perancangan Kapasiti dan Bajet
- Pengurusan Sumber Manusia

b. Kompetensi Teknologi

- Perancangan Strategik ICT (ISP)
- *Enterprise Architecture* (EA)
- Penilaian Prestasi ICT
- *E-Government/Electronic Business / Electronic Commerce*
- Keselamatan ICT atau Jaminan Maklumat
- Teknologi Penyampaian Maklumat
- Pusat Kecemerlangan

ii. Terma Rujukan CIO

Menentukan strategi dan melaksanakan pembangunan dan penggunaan ICT serta Penasihat ICT kepada pengurusan UKM. Peranan CIO seperti di **Lampiran B**.

2.4.4 ICTSO

i. Pelantikan ICTSO

Pelantikan ICTSO adalah memenuhi keperluan Pekeliling Am Bil.3/2000 (Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan). Senarai tugas ICTSO seperti di **Lampiran C**.

ii. Terma Rujukan ICTSO

- a. Menentukan semua warga UKM memahami keperluan standard piawaian, garis panduan, prosedur dan langkah keselamatan di bawah Dasar Keselamatan ICT Kerajaan;
- b. Menentukan semua warga UKM mematuhi standard, garis panduan, prosedur dan langkah keselamatan di bawah Dasar Keselamatan ICT Kerajaan. Tindakan sewajarnya hendaklah diambil apabila berlaku sebarang pelanggaran keselamatan;
- c. Menjalankan penilaian risiko dan program keselamatan berpandukan kepada standard, garis panduan, prosedur dan langkah keselamatan ICT;
- d. Mengadakan Pelan Rancangan Pematuhan yang bertujuan untuk mengurus risiko yang timbul akibat daripada ketidakpatuhan kepada standard, garis panduan, prosedur dan langkah keselamatan ICT;
- e. Menggerakkan tindakan penyiasatan dalaman terhadap sebarang pelanggaran terhadap Dasar ini selepas menerima aduan berkaitan perkara tersebut;
- f. Melaporkan kepada Bahagian Keselamatan ICT, MAMPU sebarang insiden pelanggaran keselamatan seperti kejadian-kejadian berikut:

- Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;
- Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;
- Kata laluan atau mekanisma kawalan sistem akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; dan
- Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar.

2.4.5 UKMCERT

i. Penubuhan UKMCERT

Penubuhan UKMCERT UKM adalah memenuhi keperluan GCERT dan Arahan Teknologi Maklumat 2007 untuk memastikan tahap keselamatan ICT adalah terjamin setiap masa.

ii. Terma Rujukan UKMCERT

- a. Menerima dan mengambil tindakan ke atas insiden keselamatan yang dilaporkan;
- b. Menyediakan laporan tindakan insiden keselamatan kepada Jawatankuasa Keselamatan ICT dan GCERT;
- c. Menyebarkan maklumat bagi membantu pengukuhan keselamatan ICT di UKM dari semasa ke semasa;
- d. Menyediakan khidmat nasihat kepada pelanggan dalam mengesan, mengenalpasti dan menangani sesuatu insiden keselamatan ICT;

- e. Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden;
- f. Merekod dan menjalankan siasatan awal insiden yang diterima;
- g. Menangani tindak balas insiden keselamatan ICT dan mengambil tindakan baik pulih;
- h. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden dapat dielakkan;
- i. Meningkatkan pengetahuan dan kesedaran keselamatan ICT melalui program kesedaran keselamatan ICT. Setiap pengguna perlu diberikan program kesedaran, latihan ICT dalam melaksanakan tugas dan tanggungjawab mereka; dan
- j. Menjalankan program menangani insiden dianggap penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT.



Dasar dan Peraturan ICT Universiti Kebangsaan Malaysia

Bab 3: Perisian dan Perkakasan ICT

Bab 3: Perisian dan Perkakasan ICT

3.1 Tujuan

Menentukan tanggungjawab pengguna dan pihak UKM mengenai perkara yang berhubung dengan perisian dan perkakasan ICT.

3.2 Skop

- i. semua perisian yang diperolehi atau yang dibangunkan oleh UKM yang berada dalam simpanan pengguna; dan
- ii. semua perkakasan hakmilik UKM atau digunakan atau berada dalam simpanan pengguna.

3.3 Perisian

3.3.1 Perisian Aplikasi

i. Perisian Yang Diperolehi

a. Perolehan Perisian

- Semua perolehan perisian hendaklah mengikut Prosedur Perolehan UKM dan spesifikasi perisian diluluskan oleh PTM;
- Semua perolehan perisian untuk kegunaan UKM hendaklah versi terkini dan pelesenan akademik seperti *academic edition (AE)*, *academic license* atau *education edition*;
- Penggunaan perisian adalah tertakluk kepada terma dan syarat penggunaan yang ditetapkan oleh pihak UKM, pembekal atau pembangun;

- UKM tidak akan bertanggungjawab terhadap sebarang perolehan dan penggunaan perisian tanpa lesen oleh pengguna;
- UKM bertanggungjawab melaksanakan peningkatan dan naik taraf perisian bagi memastikan versi yang terkini digunapakai; dan
- UKM bertanggungjawab menyediakan perkhidmatan penyelenggaraan bagi perisian yang memerlukan kepakaran khusus mengikut tempoh yang sesuai.

b. Penyediaan Maklumat Perisian Aplikasi

Maklumat keperluan spesifikasi perisian aplikasi ditentukan oleh Urus Setia Sistem Aplikasi sebelum perolehan dilakukan.

ii. Perisian Yang Dibangunkan Secara Dalaman

a. Pembangunan Perisian Aplikasi

Pembangunan perisian aplikasi secara dalaman dilakukan oleh Pembangun Sistem berdasarkan kitar hayat pembangunan sistem aplikasi yang merangkumi:

- Kajian kesauran sistem maklumat;
- Kajian keperluan sistem dan integrasi dengan lain-lain perisian sistem aplikasi;
- Penyediaan reka bentuk sistem;
- Pengaturcaraan sistem;
- Pengujian sistem; dan
- Latihan dan penyerahan kepada Urus Setia Sistem Aplikasi

Penasihat Sistem terlibat bagi projek-projek yang memerlukan khidmat nasihat.

b. Penyediaan Maklumat Perisian Aplikasi

Maklumat keperluan pembangunan diperolehi daripada Urus Setia Sistem Aplikasi.

3.3.2 Perisian Sistem

UKM bertanggungjawab menyediakan perisian sistem untuk membolehkan komputer berfungsi dan beroperasi. Contohnya Windows, LINUX, MAC OS dan perisian antivirus.

3.3.3 Hak milik

- i. UKM adalah Pemilik Sistem bagi semua perisian yang diperolehi atau yang dibangunkan oleh warga UKM dan pihak-pihak lain untuk tujuan pengajaran, pembelajaran, penyelidikan atau pentadbiran menggunakan sumber ICT UKM;
- ii. Bagi perisian aplikasi yang dibangunkan, maklumat mengenai semua pengarang atau pencipta asal mestilah dikekalkan; dan
- iii. Semua perisian hak milik UKM tidak boleh dijual, disewa, dilesenkan semula, dipinjam, disalin semula, disebar atau diberi kepada sesiapa atau entiti tanpa kebenaran pengurusan UKM.

3.3.4 Tanggungjawab Pengguna

- i. Pengguna bertanggungjawab untuk membaca, memahami dan mematuhi peraturan dan syarat pelesenan bagi setiap perisian yang digunakan;
- ii. Pengguna tidak dibenarkan memuat turun, membuat pemasangan dan mengguna perisian yang boleh mendatangkan gangguan dan kerosakan kepada komputer dan rangkaian UKM seperti *Kazaa*, *iMesh*, *Morpheus*, *Grokster* dan seumpamanya;

- iii. Semua pengguna tidak dibenarkan menyebarkan sebarang perisian secara tidak sah;
- iv. Sebarang bentuk permainan komputer oleh pengguna tidak dibenarkan kecuali untuk tujuan akademik dan penyelidikan setelah mendapat kelulusan daripada Ketua PTJ berkenaan;
- v. Pengguna tidak dibenarkan berkongsi ID pengguna dan kata laluan dengan pengguna lain;
- vi. Pengguna tidak dibenarkan membiarkan perisian aplikasi tidak digunakan (*unattended*) untuk tempoh yang lama; dan
- vii. Pengguna perlu log keluar (*logout*) setelah tamat atau selesai menggunakan perisian aplikasi.

3.3.5 Tanggungjawab Pihak-Pihak Lain

- i. Pihak-pihak lain bertanggungjawab untuk membaca, memahami dan mematuhi peraturan dan syarat pelesenan bagi setiap perisian yang digunakan; dan
- ii. Pihak-pihak lain yang bertanggungjawab menyediakan, mengurus, membekal, menyelenggara perkhidmatan di UKM perlu mendapat kelulusan UKM.

3.4 Perkakasan ICT

3.4.1 Hak Milik

- i. Semua perkakasan ICT yang diperolehi untuk atau bagi pihak UKM atau yang dicipta atau dipasang menggunakan peruntukan UKM oleh warga UKM dan pihak-pihak lain adalah menjadi hak milik UKM;
- ii. Bagi perkakasan ICT yang dicipta, maklumat mengenai semua pencipta asal mestilah dikekalkan; dan

- iii. Perkakasan tersebut tidak dibenarkan dijual, disewa, dipaten, dipinjam, disebar atau diberi kepada sesiapa atau entiti tanpa kebenaran pengurusan UKM.

3.4.2 Perolehan Perkakasan ICT

- i. Semua perolehan perkakasan hendaklah mengikut Prosedur Perolehan UKM;
- ii. Spesifikasi perkakasan hendaklah diperakukan oleh PTM bagi memastikan piawaian dan keseragaman dari segi teknologi dan keperluan semasa kecuali diperolehi menggunakan peruntukan atau geran penyelidikan;
- iii. Setiap perolehan perkakasan ICT yang dibeli oleh PTJ hendaklah mendapat kelulusan spesifikasi PTM; dan
- iv. Perkakasan yang dibeli hendaklah mempunyai tempoh jaminan minimum satu (1) tahun daripada pembekal utama (*manufacturer warranty*).

3.4.3 Pengagihan Perkakasan ICT

Agihan perkakasan hendaklah mengikut prosedur berikut:

i. Agihan Komputer / Notebook

Jawatan	Keterangan
Kakitangan Akademik dan Guru Bahasa	Satu (1) unit komputer atau notebook Bertanggungjawab menyerahkan komputer atau notebook ke PTM sebelum memulakan cuti belajar;
Kakitangan Pengurusan dan Profesional	Satu (1) unit komputer <i>atau</i> Satu (1) unit notebook (tertakluk kepada peruntukan)

Jawatan	Keterangan
Dekan / Pengarah / Timbalan Dekan / Timbalan Pengarah / Pengerusi Pusat Pengajian / Ketua Jabatan PTJ	Satu (1) unit komputer untuk kegunaan pentadbiran di lokasi yang ditetapkan (bilik Dekan/Pengarah) Sekiranya tamat tempoh pelantikan komputer tersebut hendaklah dikekalkan di lokasi yang berkenaan
Ketua Pusat Kecemerlangan / Webmaster / Penyelaras (dilantik oleh Universiti)	Satu (1) unit komputer tertakluk kepada tidak menerima komputer yang diperuntukkan kepada pensyarah Sekiranya lokasi berbeza Ketua Pusat Kecemerlangan / Penyelaras boleh memohon komputer tambahan tertakluk kepada kelulusan PTM
Kakitangan Lantikan Khas (Prof. Emeritus / Prof. Adjung / Prof. Pelawat / Sarjana Tamu) Felo Utama / Felo Kanan / Felo Penyelidik (lantikan terus)	Satu (1) unit komputer (mengikut tempoh pelantikan) tertakluk kepada tidak menerima komputer yang diperuntukkan kepada pensyarah kontrak Sekiranya tamat tempoh pelantikan komputer berkenaan hendaklah dikekalkan di lokasi yang berkenaan
Pensyarah Kontrak	Satu (1) unit komputer Bertanggungjawab menyerahkan komputer ke PTM selewat-lewatnya satu (1) minggu setelah tamat kontrak

Jawatan	Keterangan
Pensyarah Sementara / Tutor	Satu (1) unit komputer Bertanggungjawab menyerahkan komputer ke PTM pada hari terakhir atau selewat-lewatnya satu (1) minggu selepas memulakan cuti belajar
Kakitangan Sokongan I (Gred 27 - 40)	Diberi komputer berdasarkan keperluan kerja yang ditentukan oleh Ketua PTJ yang telah dinilai keperluannya oleh PTM
Kakitangan Sokongan II (Gred 1 - 26)	Diberi komputer berdasarkan keperluan kerja yang ditentukan oleh Ketua PTJ yang telah dinilai keperluannya oleh PTM
Dewan Kuliah Utama	Satu (1) unit komputer <i>LCD Projector</i> dibekalkan oleh JPP
Bilik Kuliah / Bilik Tutorial	Tiada agihan khusus (menggunakan <i>notebook</i> yang diagihkan ke PTJ)
Bilik Sumber Kolej Kediaman	Agihan komputer berdasarkan keperluan dari semasa ke semasa
Makmal Komputer (Pengajaran)	Agihan komputer berdasarkan kapasiti makmal berkenaan
Makmal Komputer (Penyelidikan)	Tiada agihan khusus (komputer dibeli menggunakan peruntukan geran penyelidikan masing-masing)

**ii. Agihan Notebook kepada Pengurusan Tertinggi UKM/
Dekan / Pengarah Fakulti / Pusat / Institut**

Jawatan	Keterangan
Pengurusan Tertinggi UKM/ Dekan / Pengarah Fakulti / Pusat / Institut	Satu (1) unit notebook

Nota :

Kakitangan yang tamat perkhidmatan atau bercuti melebihi tempoh enam (6) bulan termasuk tetapi tidak terhad kepada bersara atau meletak jawatan, bercuti sabatikal luar negara atau melanjutkan pengajian, perlu memaklum dan memulangkan komputer atau notebook di bawah tanggungjawabnya kepada PTM selewat-lewatnya satu (1) minggu sebelum tarikh berkenaan.

**iii. Agihan Notebook / Pencetak / LCD Projector / LCD TV / Kios
ke PTJ**

Perkakasan ICT	Keterangan
Notebook	Agihan notebook untuk kegunaan pengajaran dan pembelajaran tertakluk kepada peruntukan kewangan
Pencetak	Agihan pencetak untuk kegunaan pengajaran dan pembelajaran tertakluk kepada peruntukan kewangan
LCD Projector (Portable)	Agihan LCD Projector (Portable) untuk kegunaan pengajaran dan pembelajaran dan pentadbiran tertakluk kepada peruntukan kewangan

Perkakasan ICT	Keterangan
LCD TV	Agihan LCD TV untuk kegunaan hebahan maklumat tertakluk kepada peruntukan kewangan
Kios	Satu (1) unit kios di setiap PTJ. Unit tambahan adalah tertakluk kepada kelulusan PTM

3.4.4 Gantian Komputer atau Notebook

- i. Komputer atau notebook yang telah berusia lima (5) tahun akan diganti tertakluk kepada adanya peruntukan; dan
- ii. Komputer atau notebook asal hendaklah diserahkan kepada Ketua Pentadbiran PTJ untuk pelupusan.

3.4.5 Pemilikan Komputer atau Notebook

Kakitangan yang akan bersara dan ingin memiliki komputer atau *notebook* yang diterima semasa dalam perkhidmatan perlu membuat permohonan bertulis kepada Jawatankuasa Pelupusan UKM (Bendahari UKM sebagai Urus Setia)

3.4.6 Peminjaman Perkakasan ICT

a. Tanggungjawab Peminjam

- a. Semua peminjaman perkakasan ICT hendaklah mengikut Prosedur Pinjaman Perkakasan ICT di PTJ masing-masing;
- b. Setiap PTJ yang menyediakan kemudahan pinjaman perkakasan perlu merekod maklumat peminjaman dan pemulangan;

- c. Peminjam bertanggungjawab sepenuhnya terhadap keselamatan perkakasan ICT yang dipinjam;
- d. Peminjam perlu melaporkan secara bertulis dengan segera sekiranya berlaku kerosakan atau kehilangan perkakasan ICT yang dipinjam kepada Ketua PTJ berkenaan;
- e. Peminjam hendaklah memulangkan perkakasan yang dipinjam dalam keadaan baik, berfungsi dan dalam set lengkap pada tarikh dan masa pemulangan yang ditetapkan;
- f. Tempoh pinjaman adalah tertakluk kepada kelulusan Ketua PTJ berkenaan; dan
- g. Peminjam dari kalangan pelajar hendaklah melalui pensyarah atau pegawai di PTJ berkenaan yang secara automatik bertanggungjawab ke atas keselamatan perkakasan tersebut.

ii. Gantian Ke Atas Kehilangan Dan Kerosakan Perkakasan ICT Yang Dipinjam

- a. Peminjam hendaklah menanggung keseluruhan kos baik pulih sekiranya berlaku kerosakan disebabkan kecuaiian;
- b. Peminjam hendaklah menggantikan perkakasan ICT berdasarkan spesifikasi yang sama atau lebih tinggi sekiranya berlaku kerosakan disebabkan kecuaiian dan tidak boleh dibaiki; dan
- c. Peminjam hendaklah menggantikan perkakasan ICT yang hilang disebabkan kecuaiian berdasarkan spesifikasi yang sama atau lebih tinggi.

3.4.7 Baik Pulih dan Penyelenggaraan Perkakasan ICT

- i. Semua baik pulih dan penyelenggaraan perkakasan ICT hendaklah mengikut prosedur ditetapkan;
- ii. Bagi kerosakan perkakasan ICT yang dibekalkan oleh PTM, PTJ dikehendaki mengisi Borang Permohonan Baik Pulih Komputer. Sekiranya kerosakan tidak boleh dibaiki, PTM akan menggantikan perkakasan tersebut dengan yang setara;
- iii. Bagi kerosakan perkakasan ICT yang dibeli menggunakan peruntukan PTJ yang mematuhi spesifikasi yang ditetapkan oleh PTM, PTJ diminta membuat aduan kepada PTM untuk tujuan pemeriksaan dan baik pulih (isi Borang Permohonan Baik Pulih Komputer sertakan bukti pembelian – nota hantaran (DO) dan Surat Kelulusan Spesifikasi PTM);
- iv. PTM tidak bertanggungjawab membaikpulih perkakasan ICT bukan hak milik UKM;
- v. PTM hanya bertanggungjawab memasang perisian sistem pengoperasian (*Operating System*) yang dibenarkan sahaja;
- vi. PTM menyediakan perkhidmatan penyelenggaraan komputer di makmal PTJ, dewan kuliah dan kiosk mengikut jadual yang ditetapkan; dan
- vii. Pengguna diminta menyelenggara komputer yang telah dibekalkan secara berkala mengikut garis panduan yang ditetapkan.

3.4.8 Pelupusan Perkakasan ICT

- i. Semua perkakasan ICT yang didapati tidak sesuai dinaiktaraf atau kos penyelenggaraan atau baik pulih yang tinggi hendaklah dicadang untuk dilupuskan mengikut Prosedur Pelupusan (rujuk Pekeliling Bendahari Bil. 15/2008);

- ii. Bagi perkakasan ICT yang dibekalkan oleh PTM, cadangan pelupusan kepada Jawatankuasa Pelupusan UKM akan ditentukan oleh PTM;
- iii. Bagi perkakasan ICT yang dibeli menggunakan peruntukan PTJ, PTJ diminta membuat cadangan kepada Jawatankuasa Kecil Teknikal Pelupusan Komputer yang dipengerusikan oleh Pengarah PTM untuk semakan dan pengesahan sebelum dikemukakan ke Jawatankuasa Pelupusan Aset UKM; dan
- iv. Perkara yang perlu diambil kira untuk melupuskan perkakasan ICT:
 - a. Keupayaan dan atau kecekapan peralatan adalah rendah atau semakin menjadi rendah berbanding dengan beban kerja;
 - b. Tidak dapat memenuhi keperluan semasa disebabkan perubahan teknologi;
 - c. Kos penyelenggaraan dan atau kos pengoperasian komputer terlalu tinggi berbanding dengan prestasi peralatan dan atau kos alat ganti melebihi 50% daripada harga asal;
 - d. Kekerapan berlaku ralat adalah tinggi;
 - e. Syarikat pembekal tidak lagi memberikan khidmat sokongan ke atas peralatan ICT berkenaan; dan
 - f. Alat ganti sukar atau tidak boleh diperolehi di pasaran
- v. Langkah berjaga-jaga hendaklah diambil sebelum pelupusan dilaksanakan. Ini termasuk menghapuskan semua kandungan data dalam perkakasan ICT khususnya rahsia rasmi sebelum ia dilupuskan;
- vi. Panduan jangka hayat perkakasan ICT seperti berikut:

Perkakasan ICT	Jangka hayat
Komputer	5 tahun
Notebook	5 tahun

Pencetak	5 tahun
LCD Projector	5 tahun
Server	5 tahun

- vii. Mana-mana perkakasan ICT yang dilupuskan akan diganti baru tertakluk kepada adanya peruntukan.

3.4.9 Tanggungjawab Pengguna

- i. Pengguna tidak berhak mengganggu dengan apa cara sekali pun perkakasan yang bukan berada di bawah kawalannya. Ini termasuk mengguna atau mengambil tanpa kebenaran, mencerooboh dan mencuri perkakasan ICT atau komponennya; dan
- ii. Penggunaan secara perkongsian (*sharing*) adalah menjadi tanggungjawab bersama pengguna terbabit dan perlu mempunyai syarat dan peraturan yang dipersetujui oleh pengguna.
- iii. Pengguna bertanggungjawab untuk menyelenggara secara asas (*basic maintenance*) atau memastikan bahawa perkakasan yang dibekal berada dalam keadaan yang baik dan boleh digunakan.

3.4.10 Kehilangan Perkakasan ICT

- i. **Tindakan Pengguna Sekiranya Berlaku Kehilangan Perkakasan ICT yang diagihkan**
 - Pengguna hendaklah mengambil tindakan berdasarkan prosedur berikut (Rujuk Pekeliling Bendahari Bil. 15/2008 dan Pekeliling Bendahari Bil. 8/2009):
 - Membuat laporan di Bahagian Keselamatan UKM (dalam tempoh 24 jam dari masa kehilangan diketahui sekiranya kehilangan berlaku di dalam UKM);

- Membuat laporan di Balai Polis berhampiran (dalam tempoh 24 jam dari masa kehilangan diketahui sekiranya kehilangan berlaku di dalam dan luar UKM);
- Membuat laporan di Balai Bomba (bagi kes kebakaran sahaja);
- mengisi Kehilangan Aset (UKM/BEN-FR02/WP04);
- mengemukakan dokumen berikut bersama Borang Laporan Awal Kehilangan Aset (KEW.PA28):
 - salinan Laporan Bahagian Keselamatan UKM
 - salinan Laporan Polis
 - salinan Laporan Bomba (bagi kes kebakaran sahaja)
 - salinan Inbois dan Pesanan Rasmi aset / perkakasan berkenaan
 - salinan Kad Daftar Aset
 - gambar ditempat kejadian (jika berkenaan)

dengan segera kepada Bendahari UKM dan salinan kepada PTM.

ii. Tanggungan Pengguna Ke Atas Kehilangan Dan Kerosakan Perkakasan ICT Yang Diagihkan

- a. Pengguna hendaklah menanggung keseluruhan kos baik pulih sekiranya berlaku kerosakan disebabkan kecuaiian; dan
- b. Pengguna hendaklah menggantikan perkakasan ICT yang hilang disebabkan kecuaiian berdasarkan spesifikasi yang sama atau lebih tinggi.



UNIVERSITI KEBANGSAAN MALAYSIA
National University of Malaysia

Dasar dan Peraturan ICT Universiti Kebangsaan Malaysia

Bab 4: Penggunaan Makmal Komputer

Bab 4: Penggunaan Makmal Komputer

4.1 Tujuan

Menerangkan penguatkuasaan peraturan penggunaan makmal komputer di UKM bagi tujuan pengajaran dan pembelajaran dan sebagai garis panduan Pentadbir Makmal Komputer PTJ.

4.2 Skop

Setiap pengguna mesti mematuhi syarat dan peraturan penggunaan makmal yang ditetapkan berdasarkan kepada peruntukan di dalam Bab ini.

4.3 Penggunaan Makmal

4.3.1 Penggunaan makmal komputer adalah tertakluk kepada aktiviti UKM atau aktiviti yang dibenarkan oleh PTJ sahaja;

4.3.2 Pengguna adalah dilarang untuk melakukan perkara berikut :

- i. sembang siber (*chatting*);
- ii. makan dan minum;
- iii. menghisap rokok;
- iv. membuat bising termasuk tetapi tidak terhad kepada berbual, berbincang, memasang dan mendengar muzik;
- v. mengganggu pengguna lain dengan apa cara sekalipun, termasuk menimbulkan rasa aib, marah dan tidak selesa;
- vi. berkelakuan tidak senonoh atau mengaibkan;
- vii. menukar kedudukan komputer dan peranti;
- viii. menukar konfigurasi komputer;
- ix. menambah atau membuang sebarang perisian;
- x. menyimpan atau memuat turun maklumat atau data ke dalam cakera keras komputer;
- xi. membawa keluar sebarang peralatan dari makmal; dan
- xii. membawa keluar peranti dan perkakasan komputer.

- 4.3.3 Pengguna hendaklah mendapat kebenaran Pentadbir Makmal Komputer untuk memasang perisian lain ke dalam komputer;
- 4.3.4 Pengguna hendaklah mematuhi sebarang arahan tambahan dari Pentadbir Makmal Komputer yang bertugas; dan
- 4.3.5 Pengguna hendaklah berpakaian mengikut Etika Pakaian Universiti yang dikuatkuasakan termasuk memakai tanda nama setiap masa.

4.4 Tempahan Makmal Komputer

- i. Tempahan penggunaan makmal komputer hendaklah direkodkan ke dalam Buku Log atau sistem secara *online* yang berkuatkuasa;
- ii. Rekod tersebut hendaklah mempunyai sekurang-kurangnya maklumat berikut:
 - a. Tarikh penggunaan
 - b. Nama Pengguna atau Pemohon
 - c. Masa mula penggunaan
 - d. Masa tamat penggunaan

4.5 Rekod Penggunaan Komputer Makmal

- i. Semua penggunaan komputer di dalam makmal (sama ada yang disambung ke rangkaian UKM atau tidak) mesti direkodkan ke dalam Buku Log atau sistem secara *online* yang dikuatkuasakan;
- ii. Rekod tersebut hendaklah mempunyai sekurang-kurangnya maklumat berikut:
 - a. Tarikh penggunaan
 - b. Nama Pengguna
 - c. No. Matrik / No. Pekerja / No. Kad Pengenalan
 - d. Masa mula penggunaan
 - e. Masa tamat penggunaan
 - f. Tandatangan pengguna (jika manual)

- iii. Buku Log ini (sama ada berbentuk digital atau manual) perlu disimpan dengan baik sekurang-kurangnya untuk tempoh dua (2) tahun bagi tujuan rujukan jika diperlukan.

4.6 Budi Bicara Pentadbir Makmal Komputer

- i. Walau apa pun yang dinyatakan di dalam Bab ini, Pentadbir Makmal Komputer boleh menggunakan budi bicaranya untuk memberikan arahan tambahan berdasarkan keperluan dari semasa ke semasa; dan
- ii. Budi bicara tersebut mestilah tidak mengatasi sebarang peruntukan dibawah Dasar ini dan tidak akan mengecualikan liabiliti beliau daripada dikenakan sebarang tindakan penguatkuasaan dan pematuhan dibawah Bab 9.

4.7 Tindakan Penguatkuasaan dan Pematuhan

Mana-mana pihak yang gagal untuk mematuhi peruntukan Bab ini sama ada dengan niat sengaja atau dengan tinggalan salah boleh dikenakan tindakan penguatkuasaan bagi tujuan pematuhan dibawah Bab 9.



Dasar dan Peraturan ICT Universiti Kebangsaan Malaysia

Bab 5: Pengurusan Rangkaian UKM

Bab 5: Pengurusan Rangkaian UKM

5.1 Tujuan

Menentukan penyediaan, pengoperasian dan penyelenggaraan perkakasan serta perisian rangkaian untuk perkhidmatan rangkaian UKM.

5.2 Skop

Rangkaian UKM merangkumi rangkaian *wired* dan *wireless* yang disediakan oleh UKM atau pihak-pihak lain dengan mendapat nasihat daripada Perunding Rangkaian UKM yang dilantik.

Terma Rujukan Perunding Rangkaian UKM seperti berikut:

- i. Merangka keperluan teknologi terkini rangkaian UKM;
- ii. Memberikan khidmat nasihat pembangunan rangkaian di UKM; dan
- iii. Menjalankan pengujian terhadap rangkaian yang digunakan

5.3 Penyediaan Perkhidmatan Rangkaian UKM

- i. Semua perolehan sumber rangkaian hendaklah mengikut Prosedur Perolehan UKM dan spesifikasi peralatan rangkaian diluluskan oleh PTM ();
- ii. Perolehan peralatan rangkaian seperti *routers* dan *wireless access point* oleh PTJ adalah tidak dibenarkan kecuali dengan kelulusan PTM;
- iii. Sumber rangkaian merangkumi peralatan rangkaian, termasuk tetapi tidak terhad kepada peralatan rangkaian seperti *hubs*, *switches* dan *routers*;

- iv. Perisian aplikasi rangkaian merangkumi perisian sama ada dibeli atau dimuat turun daripada Internet seperti e-mel, *web browser* dan lain-lain; dan
- v. Konfigurasi rangkaian merangkumi kaedah takrifan dan reka bentuk bagi penggunaan alamat IP dan teknologi serta protokol rangkaian yang digunakan seperti teknologi Gigabit, protokol TCP/IP dan lain-lain.

5.4 Konfigurasi Pengoperasian Rangkaian UKM

- i. *Server* yang digunakan untuk tujuan penyelidikan yang menggunakan rangkaian secara intensif (*high bandwidth usage*) perlu ditempatkan dalam rangkaian persendirian (LAN) yang dipisahkan daripada rangkaian UKM. Sebarang ujian yang memerlukan penggunaan rangkaian UKM secara terus perlu mendapat kelulusan PTM;
- ii. *Server* yang digunakan untuk projek pelajar dan kegunaan dalaman perlu mendapat perakuan daripada Penyelia Projek atau Dekan dan diluluskan oleh PTM. Alamat IP statik (*static IP*) perlu digunakan untuk *server* ini. Alamat IP global (*global IP*) boleh dipohon untuk projek yang memerlukan capaian Internet;
- iii. Alamat IP tidak dibenarkan diubah sama sekali kecuali setelah mendapat kelulusan PTM; dan
- iv. *Login* dan kata laluan untuk *id root* dan *super-user* adalah di bawah kawalan dan tanggungjawab Pentadbir Rangkaian sepenuhnya.

5.5 Penyambungan Rangkaian UKM

- i. Perolehan peralatan rangkaian dan penyambungan ke rangkaian UKM perlu mendapat kelulusan PTM. Konfigurasi penyambungan hendaklah dibuat oleh pembekal di bawah pengawasan dan kawalan PTM;
- ii. Sebarang penyambungan rangkaian ke rangkaian UKM yang tidak mendapat kebenaran PTM adalah menyalahi peraturan dan UKM berhak memutuskan penyambungan tersebut;

- iii. Penyambungan Rangkaian Antara Kampus (CAN) dan Rangkaian Luas (WAN) oleh pengguna tidak dibenarkan sama sekali; dan
- iv. Setiap bangunan baru yang akan dibina perlu memasukkan keperluan infrastruktur rangkaian yang ditentukan bersama oleh pengguna, PTM dan Jabatan Pengurusan Pembangunan (JPP). Kos pemasangan infrastruktur rangkaian perlu dimasukkan dalam kos peruntukan pembinaan bangunan.

5.6 Penggunaan Kemudahan Rangkaian UKM

- i. Pengguna tidak dibenarkan dalam apa cara sekali pun untuk mengganggu pengguna lain di dalam rangkaian UKM dan Internet. Gangguan ini termasuk tetapi tidak terhad kepada menghantar maklumat rambang (*spam*) secara e-mel atau mesej *online* dan lain-lain;
- ii. Pengguna tidak boleh membenarkan sumber rangkaian di bawah kawalannya termasuk tetapi tidak terhad kepada nod rangkaian dan kad *wireless* untuk diguna oleh pihak-pihak lain walaupun kepada warga UKM tanpa mendapat kelulusan PTM;
- iii. Pengguna bertanggungjawab sepenuhnya terhadap semua aktiviti yang dilakukannya termasuk tetapi tidak terhad kepada stesen kerja, komputer peribadi atau PDA yang melibatkan atau melalui rangkaian UKM termasuk akses ke Internet dan rangkaian yang lain;
- iv. Mana-mana komputer yang menjadi sumber ancaman atau penyebaran virus akan disekat capaiannya ke rangkaian UKM sehingga komputer tersebut disahkan bebas dari ancaman virus; dan
- v. *Server* untuk kegunaan lain (contoh kafe siber) tidak dibenarkan menggunakan rangkaian UKM untuk mengelak gangguan rangkaian;

5.7 Tindakan Penguatkuasaan dan Pematuhan

Mana-mana pihak yang gagal untuk mematuhi peruntukan Bab ini sama ada dengan niat sengaja atau dengan tinggalan salah boleh dikenakan tindakan penguatkuasaan bagi tujuan pematuhan di bawah Bab 9.



Dasar dan Peraturan ICT Universiti Kebangsaan Malaysia

Bab 6: Penggunaan Internet atau Intranet

Bab 6: Penggunaan Internet atau Intranet

6.1 Tujuan

Menentukan tatacara penggunaan dan peraturan perkhidmatan Internet atau Intranet bagi melahirkan pengguna yang beretika selaras dengan UKM sebagai institusi ilmu.

6.2 Skop

- i. Penggunaan kemudahan e-mel UKM dan bukan UKM;
- ii. Pembangunan laman web di UKM, sama ada dibangunkan secara berpusat oleh Unit Kandungan Web Universiti (UNIKWeb) menggunakan laman web utama atau secara berasingan oleh PTJ; dan
- iii. Penggunaan Internet atau Intranet termasuk tetapi tidak terhad kepada capaian sistem aplikasi atau portal UKM, laman web, pemindahan data atau maklumat dan perbincangan melalui *list group* atau *chat room*.

6.3 Kemudahan *E-Mail*

Kemudahan *e-mail* disediakan untuk warga UKM, PTJ atau persatuan rasmi UKM.

6.3.1 Permohonan Akaun *E-Mail*

- i. Permohonan hendaklah dibuat sekali sahaja dengan menggunakan Borang Permohonan e-mail atau menggunakan surat rasmi;
- ii. Pengguna individu tidak dibenarkan memohon dan atau memiliki lebih daripada satu (1) akaun *e-mail* atau alamat

e-mail UKM pada satu-satu masa pada *server* yang didaftarkan; dan

- iii. Setiap alamat *e-mail* yang disediakan adalah untuk kegunaan individu atau PTJ atau persatuan berkenaan sahaja dan tidak boleh digunakan oleh pihak lain sama ada dengan kebenaran atau tanpa kebenaran;

6.3.2 Tanggungjawab Pengguna

- i. Aktiviti *spamming*, *mail-bombing*, *phishing* dan atau penyebaran *e-mail* dengan kandungan tidak beretika (seperti perniagaan, lucah, ugutan, perkauman dan gangguan) kepada individu, *mailing list* atau *discussion group* sama ada di dalam rangkaian UKM atau ke Internet adalah tidak dibenarkan;
- ii. Pengguna digalakkan menukar kata laluan akaun *e-mail* secara berkala (dicadangkan dibuat setiap enam (6) bulan). Penggunaan kata laluan yang sukar diramal oleh penggadam adalah digalakkan;
- iii. Pengguna tidak boleh berkongsi kata laluan akaun *e-mail* dengan pengguna lain;
- iv. Akaun *e-mail* setiap pengguna tidak boleh digunakan oleh pihak lain walaupun dengan kebenaran;
- v. Pengguna dilarang menggunakan kemudahan *e-mail* untuk sebarang aktiviti yang tidak dibenarkan oleh peraturan UKM dan undang-undang negara;
- vi. Pengguna bertanggungjawab ke atas *mailbox* masing-masing untuk memastikan ruang storan mencukupi dan melakukan *back up* kandungan *e-mail* secara berkala;
- vii. Pengguna digalakkan menggunakan *e-mail* UKM untuk urusan rasmi. UKM berhak menghalang penggunaan *e-mail*

selain daripada *e-mail* UKM jika didapati membebankan rangkaian UKM;

- viii. Pengguna hendaklah log keluar atau tutup *browser* yang digunakan setelah sesi capaian akaun *e-mail* selesai bagi mengelakkan akaun *e-mail* diceroboh; dan
- ix. Pengguna hendaklah melaporkan kepada *Postmaster* sekiranya pengguna bercuti atau berkursus dalam tempoh yang panjang untuk pemantauan dan penyelenggaraan. Akaun *e-mail* yang tidak aktif dalam tempoh 45 hari tanpa pemakluman kepada *Postmaster* akan dipasifkan;

6.3.3 Penamatan Akaun E-Mail

UKM boleh menamatkan kemudahan akaun *e-mail* yang telah diberikan kepada warga UKM atas sebab berikut:

- i. kakitangan telah tamat perkhidmatan;
- ii. pelajar telah tamat pengajian atau ditamatkan pengajian;
- iii. persatuan yang telah dibubarkan secara rasmi;
- iv. permintaan daripada kakitangan atau pelajar sendiri; dan
- v. kakitangan atau pelajar tidak bersetuju dengan dasar yang ditetapkan.

6.3.4 Penafian

- i. UKM berhak memasang sebarang jenis perisian atau perkakasan penapisan *e-mail* 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 UKM;
- ii. UKM 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 UKM;

- iii. UKM 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;
- iv. Bagi kes kerosakan *e-mail*, *Postmaster* hanya bertanggungjawab untuk memulihkan kembali (*restore*) maklumat akaun pengguna dan bukannya kandungan atau *mailbox* pengguna;
- v. 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
- vi. *Postmaster* dengan kelulusan UKM berhak memeriksa dan melihat isi kandungan *e-mail* dan ruang storan pengguna dari semasa ke semasa atas keperluan audit dan keselamatan.

6.4 Pembangunan Laman Web

- 6.4.1 UKM bertanggungjawab menyediakan tapak atau ruang, untuk laman web rasmi PTJ atau Persatuan atau aktiviti rasmi atau kakitangan UKM sahaja;
- 6.4.2 Ketua PTJ atau persatuan atau kakitangan UKM adalah bertanggungjawab sepenuhnya terhadap semua kandungan dan keselamatan laman web masing-masing. UKM tidak akan bertanggungjawab terhadap kandungan (rujuk **Lampiran D**) dan sebarang penyalahgunaan hakcipta yang dilakukan. UKM juga boleh menghadkan atau memansuhkan akses kepada tapak laman web tersebut;

-
- 6.4.3 Semua laman web PTJ mesti mempunyai pautan dengan laman utama UKM. UKM berhak menukar atau mengubahsuai kandungan laman web atas kepentingan UKM;
 - 6.4.4 UKM berhak menentukan perisian pembangunan laman web dan capaian pangkalan data bagi tujuan pengoptimuman penggunaan dan keselamatan;
 - 6.4.5 Laman web peribadi yang berbentuk ilmiah adalah dibenarkan dengan kelulusan UKM terlebih dahulu. UKM tidak akan bertanggungjawab terhadap kandungan dan sebarang penyalahgunaan hakcipta yang dilakukan oleh individu;
 - 6.4.6 Kandungan laman web hendaklah menggunakan sama ada Bahasa Melayu dan atau Bahasa Inggeris. Penggunaan bahasa lain perlu mendapat kelulusan UKM terlebih dahulu dan jika dibenarkan maka penggunaan bahasa tersebut hendaklah digunakan bersama dengan bahasa sama ada Bahasa Melayu atau Bahasa Inggeris dalam bentuk dwibahasa;
 - 6.4.7 Kandungan laman web hendaklah tidak mengandungi maklumat atau terdedah kepada kemasukan maklumat yang menyalahi peraturan UKM dan undang-undang negara. Ini termasuk tetapi tidak terhad kepada maklumat yang berbentuk keganasan, lucah, hasutan dan yang boleh menimbulkan atau membawa kepada keganasan, keruntuhan akhlak dan kebencian;
 - 6.4.8 Pembangunan laman web yang memerlukan kawalan keselamatan maklumat digalakkan menggunakan protokol keselamatan https;
 - 6.4.9 Pembangunan laman web yang berbentuk forum mesti dipantau dan dikawal oleh Webmaster berkenaan; dan
 - 6.4.10 Semua laman web PTJ atau peribadi atau persatuan yang dibangunkan sendiri perlu dimaklumkan kepada PTM dan mematuhi garis panduan yang ditetapkan oleh UKM.

6.5 Capaian Internet atau Intranet

6.5.1 Laman Yang boleh Dilayari

- i. UKM berhak menyediakan dan memasang perisian penapisan kandungan Internet atau Intranet yang dilayari;
- ii. Laman yang boleh dilayari, dilanggan dan diguna adalah berbentuk akademik dan pengetahuan. Laman yang berbentuk keganasan, lucah, hasutan, perkauman dan yang boleh menimbulkan atau membawa kepada keganasan, keruntuhan akhlak dan kebencian adalah tidak dibenarkan sama sekali, kecuali mendapat kebenaran UKM setelah mendapat sokongan Ketua PTJ bagi tujuan akademik, penyelidikan atau pentadbiran;
- iii. Capaian laman yang berbentuk hiburan tidak dibenarkan di waktu pejabat, termasuk tetapi tidak terhad kepada laman *radio online* dan *video streaming* yang membebankan rangkaian UKM; dan
- iv. UKM berhak menapis, menghalang dan menegah penggunaan mana-mana laman web yang dianggap tidak sesuai.

6.5.2 Penyalahgunaan Laman Web

- i. Pengguna dilarang mengganggu atau mencerooboh laman web mana-mana jabatan, organisasi di dalam atau luar negara;
- ii. Pengguna dilarang memasuki, menyalin, meniplak, mencetak dan menyebarkan maklumat daripada Internet yang menyalahi undang-undang negara; dan
- iii. Pengguna yang mencapai sesuatu perkhidmatan yang perlu dibayar (contohnya pangkalan data *online* komersial), hendaklah bertanggungjawab ke atas segala bayaran yang dikenakan.

6.6 Tanggungjawab Pengguna

- i. Melayari internet tanpa tujuan atau meninggalkan capaian Internet *unattended* adalah amat tidak beretika dan tidak digalakkan kerana ianya boleh menyebabkan kesesakan;
- ii. *Internet chatting* tidak digalakkan kecuali *chatting* setempat untuk tujuan rasmi. Penggunaan untuk tujuan rasmi perlu mendapat kelulusan daripada PTM secara bertulis melalui Ketua PTJ. Permohonan hendaklah menyatakan tujuan penggunaan, senarai pengguna, dan perisian yang digunakan;
- iii. Pengguna tidak dibenarkan menggunakan sumber ICT atau persendirian untuk mendapatkan atau cuba mendapatkan capaian tidak sah daripada mana-mana sistem komputer sama ada di dalam atau luar UKM. Ini termasuk membantu, mendorong, menyembunyikan percubaan untuk mencapai sistem komputer tersebut atau mencapai sumber ICT UKM dengan menggunakan identiti pengguna lain;
- iv. Pengguna tidak dibenar mencapai atau cuba mencapai sumber ICT sama ada dalam bentuk data, paparan, *keystrokes*, fail atau media storan dalam sebarang bentuk yang dimiliki oleh pengguna lain tanpa mendapat kebenaran atau kelulusan pengguna terbabit terlebih dahulu. Ini termasuk membaca, menyalin, menukar, merosak atau memadam data, program dan perisian. Penggunaan perisian seperti penganalisis rangkaian atau *sniffer* adalah dilarang sama sekali kecuali untuk tujuan penyelidikan setelah mendapat kelulusan UKM; dan
- v. Pengguna dilarang menyambung peranti elektronik termasuk tetapi tidak terhad kepada komputer peribadi atau *notebook* dan *hub* atau *switch* peribadi atau modem ke rangkaian UKM dengan tujuan mencapai sumber ICT yang tidak dibenarkan.

6.7 Tindakan Penguatkuasaan dan Pematuhan

Mana-mana pihak yang gagal untuk mematuhi peruntukan Bab ini sama ada dengan niat sengaja atau dengan tinggalan salah boleh dikenakan tindakan penguatkuasaan bagi tujuan pematuhan di bawah Bab 9.



Dasar dan Peraturan ICT Universiti Kebangsaan Malaysia

Bab 7: Akauntabiliti dan Kerahsiaan Maklumat

Bab 7: Akauntabiliti dan Kerahsiaan Maklumat

7.1 Tujuan

Menyatakan tanggungjawab pihak yang terlibat dengan penggunaan kemudahan ICT di UKM seperti berikut:

- i. memelihara dan melindungi maklumat peribadi kakitangan yang disimpan oleh UKM yang diklasifikasikan sebagai maklumat rahsia atau sulit;
- ii. menyokong usaha UKM untuk menjaga kepentingan *stakeholder*; dan
- iii. menerangkan aktiviti yang dilakukan oleh Jawatankuasa Penyelarasan Maklumat atau pengguna yang melibatkan capaian data atau maklumat yang diklasifikasikan sebagai maklumat rahsia atau sulit.

7.2 Skop

Meliputi tanggungjawab pengguna dan UKM berkaitan capaian maklumat rahsia atau sulit.

Nota : Maklumat peribadi yang diambil untuk memudahkan seseorang individu berhubung, seperti alamat yang disediakan oleh seseorang individu adalah tidak termasuk dalam Bab ini.

7.3 Capaian Maklumat Rahsia Atau Sulit

7.3.1 Capaian Maklumat Rahsia Atau Sulit Oleh Pentadbir Sistem

- i. Pentadbir Sistem mempunyai kuasa untuk mencapai, merekod, memantau data, maklumat atau kegiatan pengguna dari semasa ke semasa sebagai rutin pemantauan keselamatan ICT untuk tujuan keselamatan ICT. Contohnya, arahan dalam sistem *server* UNIX seperti

last, syslogd, acctcom, pacct yang berfungsi merekod aktiviti pengguna untuk tujuan pengauditan;

- ii. Pentadbir Sistem mempunyai kuasa tanpa perlu mendapat kebenaran UKM terlebih dahulu untuk memantau kegiatan dan aktiviti pengguna yang melanggar Dasar ICT (rujuk Bab 9 : Penguatkuasaan dan Pematuhan). Segala maklumat yang direkodkan boleh digunakan sebagai bukti. Sekiranya pelanggaran tersebut serius seperti menggunakan identiti pengguna lain untuk mencuri data atau merosakkan sumber ICT, bukti dan keterangan yang dikumpul akan dikemukakan kepada Jawatankuasa Keselamatan ICT UKM; dan
- iii. Pentadbir Sistem boleh membuat salinan sama ada dalam bentuk bercetak atau digital kesemua atau sebahagian kandungan akaun pengguna sebagai pemeliharaan bukti. Pentadbir Sistem dengan kebenaran UKM boleh mencapai maklumat atau data sulit atau rahsia pengguna seperti e-mail atau fail yang tersimpan dalam akaunnya;

7.3.2 Capaian Maklumat Rahsia Atau Sulit Oleh Pengguna

- i. Pengguna ditegah menyimpan data atau maklumat sensitif, rahsia atau sulit di dalam komputer atau akaun pengguna tanpa kebenaran; dan
- ii. Pengguna diberi jaminan bahawa selain daripada perkara yang disebutkan di atas, maklumat rahsia atau sulit yang terdapat dalam akaun pengguna tidak akan dicapai oleh sesiapa pun. Sekiranya ada individu atau pengguna lain mencapai maklumat rahsia atau sulit pengguna lain tanpa kebenaran, maka individu tersebut telah melanggar Dasar ini iaitu Bab 7 : Akauntabiliti dan Kerahsiaan Maklumat Klausa 7.3.1 : Capaian Maklumat Rahsia atau Sulit oleh Pentadbir Sistem.

7.4 Pemantauan Data Dalam Rangkaian

- 7.4.1 Pentadbir Rangkaian mempunyai kuasa untuk memantau dan merekodkan data yang berada dalam rangkaian sebagai sebahagian daripada rutin keselamatan sumber ICT. Peralatan rangkaian seperti *router* atau *server* yang menggunakan perisian tertentu mampu merekodkan data dalam rangkaian. Jaminan diberikan bahawa data yang direkodkan tidak akan didedahkan melainkan jika berlaku kejadian pelanggaran Dasar ini iaitu Bab 8 : Keselamatan ICT;
- 7.4.2 Sekiranya Pentadbir Rangkaian mengesyaki pengguna melanggar Dasar ini maka Pentadbir Rangkaian mempunyai mandat tanpa perlu mendapat kebenaran UKM untuk memantau dan merekodkan data dalam talian yang melibatkan aktiviti pengguna dengan lebih teliti. Data komunikasi daripada peralatan yang digunakan oleh pengguna yang disyaki akan direkodkan dan setiap *keystrokes* juga akan direkodkan. Data ini akan digunakan sebagai bahan bukti untuk proses pengauditan yang akan dilakukan oleh Jawatankuasa Keselamatan ICT UKM; dan
- 7.4.3 Jaminan adalah diberikan kepada pengguna bahawa selain daripada perkara yang dinyatakan di atas, adalah menjadi kesalahan jika pengguna selain daripada Pentadbir Rangkaian memantau atau merekodkan data yang berada dalam rangkaian.

7.5. Pengurusan Maklumat Rahsia Atau Sulit

7.5.1 Pengambilan Maklumat Rahsia Atau Sulit

- i. Urus Setia Sistem Aplikasi yang menggunakan maklumat peribadi seseorang mestilah menyatakan tujuannya dengan jelas dan nyata seperti berikut:
 - a. apabila maklumat peribadi diambil daripada seseorang individu itu, maklumat itu mestilah diberikan oleh Tuan Punya Maklumat tersebut dan bukan daripada orang lain; dan

-
- b. Tuan Punya Maklumat hendaklah diberitahu atau dimaklum untuk mengesahkan (tandatangan) sesuatu maklumat yang telah diberikan.
- ii. Kaedah Pengambilan Maklumat Peribadi
- a. Maklumat peribadi diambil berpandukan dasar, peraturan atau undang-undang yang dibenarkan;
- b. Maklumat peribadi tidak boleh diambil tanpa kebenaran Urus Setia Sistem Aplikasi; dan
- c. Maklumat peribadi yang terdapat di laman web UKM adalah atas tanggungjawab webmaster PTJ berkenaan. UKM tidak bertanggungjawab ke atas kesahihan maklumat peribadi yang disediakan.
- iii. Larangan Terhadap Pengambilan Maklumat Sensitif
- a. Maklumat yang dinyatakan di bawah tidak boleh diambil, digunakan atau dihebahkan. Walau bagaimanapun jika maklumat diambil dengan mendapat kebenaran Urus Setia Sistem Aplikasi untuk mengambil, mengguna, menghebah atau pun untuk tujuan prosedur di dalam mahkamah, maka maklumat ini tidak termasuk di dalam Bab ini iaitu:
- bangsa;
 - asal keluarga;
 - agama, pandangan politik, ideologi atau pun keahlian sesuatu persatuan; dan
 - maklumat kesihatan, rawatan yang diambil.
- b. Semua maklumat yang sensitif hendaklah dinyatakan dengan jelas tujuan penggunaannya semasa permohonan mendapatkan maklumat dilakukan; dan
- c. Maklumat kesihatan hanya boleh diambil oleh Pegawai Perubatan yang bertauliah.

-
- iv. Maklumat peribadi yang boleh diambil daripada Tuan Punya Maklumat :
- a. Maklumat peribadi berikut atau pun yang bersamaan dengannya boleh diambil:
 - nama
 - gelaran
 - PTJ
 - nombor telefon
 - alamat
 - b. Tujuan pengambilan dan penggunaan maklumat hendaklah dimaklumkan kepada Tuan Punya Maklumat jika maklumat tersebut perlu dihebahkan untuk tujuan tertentu; dan
 - c. Hak untuk meminta capaian maklumat peribadi dan hak untuk membuat pindaan atau pembetulan jika terdapat kesilapan hendaklah dimaklumkan kepada Urus Setia Sistem Aplikasi.
- v. Had pengambilan selain daripada Pemberi Maklumat (bukan Tuan Punya Maklumat) :
- a. Bagi kes di mana maklumat diambil daripada pihak ketiga, kebenaran hendaklah diminta daripada Urus Setia Sistem Aplikasi. Apabila maklumat yang diberi oleh seseorang kepada seseorang yang lain dengan izin Urus Setia Sistem Aplikasi perkara berikut hendaklah diikuti:
 - Tujuan pengambilan maklumat;
 - Jenis maklumat yang diambil; dan
 - Tanggungjawab untuk memastikan maklumat dijaga atau disimpan dengan baik.

7.5.2 Had Penggunaan Maklumat Peribadi

- i. Maklumat peribadi mestilah digunakan untuk tujuan yang telah dinyatakan ketika maklumat itu diperolehi daripada Pemberi Maklumat dalam skop yang dibenarkan oleh UKM:
 - a. Penggunaan maklumat peribadi yang telah diambil mestilah mengikut syarat berikut:
 - Tuan Punya Maklumat telah memberi kebenaran menggunakan maklumat tersebut;
 - maklumat boleh digunakan sebagai pengesahan sesuatu kontrak;
 - maklumat boleh digunakan untuk tujuan mahkamah atau perundangan; dan
 - maklumat boleh digunakan untuk melindungi Tuan Punya Maklumat dalam semua perkara.
 - b. Maklumat peribadi yang digunakan selain daripada tujuan asal ketika maklumat itu diambil, kebenaran daripada Tuan Punya Maklumat mestilah diperolehi dengan kaedah yang dinyatakan dalam Klausula 7.5.1 (ii) : Kaedah Pengambilan Maklumat Peribadi. Tuan Punya Maklumat mempunyai hak untuk tidak memberikan keizinan penggunaan maklumat tersebut.

7.5.3 Penyelenggaraan Maklumat Rahsia atau Sulit

- i. UKM bertanggungjawab memastikan ketepatan maklumat peribadi semasa dalam simpanan dan sentiasa dikemaskini untuk tujuan yang diperlukan. Maklumat rahsia atau sulit perlu dikemaskini dari semasa ke semasa mengikut keperluan. Dalam kes Tuan Punya Maklumat telah tamat perkhidmatan, pelajar berhenti atau telah bergraduat, mereka tidak dimestikan untuk mengemaskini maklumat tersebut kecuali apabila diperlukan oleh UKM;

- ii. UKM bertanggungjawab menjamin keselamatan maklumat rahsia atau sulit yang disimpan dan langkah keselamatan hendaklah diambil untuk mengelakkan maklumat dicapai secara tidak sah, dirosak, diubah, hilang dan sebagainya;
- iii. Data hendaklah dienkrif sekiranya disimpan dalam media elektronik untuk penghantaran melalui rangkaian;
- iv. UKM bertanggungjawab menjamin kerahsiaan maklumat peribadi. Individu yang bertanggungjawab menyimpan, mengumpul atau memproses data mestilah memastikan maklumat peribadi tidak disebar kepada pihak lain, selain daripada mereka yang mempunyai hak untuk mengetahui maklumat tersebut;
- v. Permintaan untuk mencapai maklumat peribadi oleh Tuan Punya Maklumat untuk tujuan pengesahan mestilah diberi untuk satu tempoh yang berpatutan. Jika terdapat kesilapan maklumat peribadi ketika diperiksa oleh Tuan Punya Maklumat, Urus Setia Sistem Aplikasi tersebut hendaklah diberitahu;
- vi. Bantahan terhadap penggunaan maklumat peribadi oleh Tuan Punya Maklumat hendaklah diterima. Walau bagaimanapun jika maklumat peribadi itu digunakan untuk tujuan pengesahan atau atas keperluan undang-undang, maka hak bantahan tersebut tidak dibenarkan; dan
- vii. Urus Setia Sistem Aplikasi mestilah memahami dan mematuhi Bab ini dan bertanggungjawab untuk memaklumkan kepada Pemberi Maklumat.

7.6 Tindakan Penguatkuasaan dan Pematuhan

Mana-mana pihak yang gagal untuk mematuhi peruntukan Bab ini sama ada dengan niat sengaja atau dengan tinggalan salah boleh dikenakan tindakan penguatkuasaan bagi tujuan pematuhan di bawah Bab 9.



Dasar dan Peraturan ICT Universiti Kebangsaan Malaysia

Bab 8: Keselamatan ICT

Bab 8: Keselamatan ICT

8.1 Tujuan

- i. Menentukan pengawalan ke atas keselamatan perkakasan ICT, perisian, pangkalan data dan operasi komputer;
- ii. Memastikan pengawalan dan pengurusan keselamatan ke atas perkakasan ICT, perisian, pangkalan data dan operasi komputer;
- iii. Menerangkan pelaksanaan keselamatan rangkaian UKM bagi tujuan komunikasi dan perkongsian maklumat serta sumber ICT; dan
- iv. Menguatkuasakan peraturan-peraturan yang termaktub di dalam Dasar ini.

8.2 Skop

- i. merangkumi aspek keselamatan perkakasan ICT, perisian dan pangkalan data; dan
- ii. aspek reka bentuk dan keselamatan rangkaian;

8.3 Keselamatan Perisian Aplikasi

8.3.1 Kawalan Terhadap Perisian Aplikasi

- i. Kawalan keselamatan perisian aplikasi dilaksanakan untuk mengelakkan berlakunya capaian oleh pengguna yang tidak sah, pengubahsuaian, pendedahan atau penghapusan maklumat;

PTM bertanggungjawab menyediakan kawalan seperti berikut:

- a. kawalan capaian penggunaan satu (1) ID pengguna dan kata laluan untuk setiap perisian aplikasi;
 - b. mengehendkan tahap capaian maklumat serta fungsi berdasarkan tanggungjawab pengguna; dan
 - c. mengadakan sistem log bagi setiap transaksi maklumat kritikal untuk tujuan jejak audit yang menentukan akauntabiliti kepada semua pengguna;
- ii. PTM bertanggungjawab menguji aturcara, modul, sistem aplikasi dan integrasi perisian aplikasi bagi memastikan sistem berfungsi mengikut spesifikasi yang ditetapkan.

Langkah berikut diambil semasa pengujian dijalankan:

- a. menggunakan data ujian (*dummy*) atau data lapuk (*historical*);
- b. mengawal penggunaan data terpilih (*classified*);
- c. mengehendkan capaian kepada kakitangan yang terlibat sahaja;
- d. mengadakan kaedah pemberitahuan (*flag system*) sekiranya capaian dan pengemaskinian maklumat dilakukan;
- e. menghapuskan maklumat yang digunakan setelah selesai pengujian (terutamanya apabila menggunakan data lapuk); dan
- f. menggunakan persekitaran yang berasingan untuk pembangunan dan pengoperasian sistem aplikasi.

- iii. Pengguna hanya boleh memasang dan menggunakan perisian yang berdaftar dan dilindungi di bawah Akta Hakcipta Tahun 1997;

8.3.2 Kawalan Terhadap Perisian Tidak Berlesen

UKM bertanggungjawab memastikan hanya perisian berlesen digunakan oleh warga UKM. Semua perisian berlesen yang digunakan dikawal penyimpanannya dari segi lokasi serta pengedarannya.

8.3.3 Kawalan Terhadap Penyimpanan *Source Code*

UKM bertanggungjawab mengurus dan melaksanakan kawalan penyimpanan *source code* bagi perisian aplikasi yang dibangunkan secara dalaman atau luaran untuk tujuan penyelenggaraan dan peningkatan yang merangkumi:

- a. mewujudkan prosedur penyelenggaraan versi terkini;
- b. mendokumentasikan prosedur *back up* kod sumber bagi penyelenggaraan versi terkini; dan
- c. menyimpan *back up* kod sumber di tiga (3) lokasi yang berasingan

8.3.4 Kawalan Terhadap Perisian Berkod Jahat (*Malicious Code*) dan Merosakkan (*Defective*)

- i. Aturcara perisian aplikasi terdedah kepada kod jahat yang boleh merosakkan sistem. PTM bertanggungjawab mengurangkan kemungkinan perisian yang mempunyai kod jahat dan merosakkan melalui kawalan berikut:
 - a. Memastikan *source code* disemak oleh Pembangun Sistem yang mempunyai kepakaran teknikal yang tinggi;
 - b. mewujudkan dan melaksanakan prosedur kawalan kualiti (pengujian mengikut peringkat pembangunan) untuk

semua sistem aplikasi yang dibangunkan bebas daripada perisian berkod jahat; dan

- c. memastikan semua sistem aplikasi didokumenkan, diuji, disahkan fungsinya, tahan lasak (*robustness*), boleh dipercayai (*reliable*) dan menepati spesifikasi.

8.3.5 Kawalan Terhadap Berkod Jahat (*Malicious Code*)

UKM bertanggungjawab memastikan integriti maklumat daripada pendedahan atau kemusnahan akibat kod jahat seperti berikut:

- i. melaksanakan prosedur untuk mengurus kod jahat;
- ii. mewujudkan peraturan berkaitan memuat turun, penerimaan dan penggunaan perisian percuma (*freeware* dan *shareware*);
- iii. menyebarkan arahan dan maklumat untuk mengesan kod jahat kepada semua pengguna;
- iv. mengambil langkah pencegahan atau pemulihan serangan kod jahat seperti berikut:
 - a. mengimbas dan menghapus kod jahat menggunakan perisian anti virus yang diluluskan;
 - b. menyemak status proses imbasan dalam laporan log; dan
 - c. tidak melaksanakan (*run*) atau membuka *attachment* daripada *e-mail* yang meragukan.

8.3.6 Kawalan Terhadap Perubahan Versi

Versi baru perisian aplikasi dan sistem pengoperasian sentiasa dikeluarkan secara berkala bagi mengatasi masalah pepijat dan ancaman serta meningkatkan fungsinya. UKM bertanggungjawab mengawal versi perisian aplikasi apabila perubahan atau

peningkatan dibuat dan pematuhan kepada prosedur kawalan perubahan dipatuhi.

8.4 Keselamatan Server

8.4.1 Kawalan Keselamatan Fizikal

- i. Kawalan terhadap kakitangan dan pihak-pihak lain yang dibenarkan yang masuk ke Bilik *Server* Utama atau Bilik Komunikasi Rangkaian dan juga kawalan akses kepada semua *server* serta sumber ICT lain;
- ii. Bilik *Server* Utama atau Bilik Komunikasi Rangkaian dilengkapi dengan peralatan utiliti sokongan seperti *Uninterruptible Power Supply* (UPS), Set Generator dan sumber bekalan elektrik yang mencukupi untuk mengelakkan *single point of failure*;
- iii. Bilik *Server* Utama atau Bilik Komunikasi Rangkaian dilindungi dengan peralatan keselamatan dan kebakaran yang sesuai;
- iv. Melindungi pengkabelan dengan pemasangan konduit atau lain-lain mekanisma perlindungan; dan
- v. Mewujudkan mekanisma kawalan capaian fizikal untuk kakitangan dan pihak-pihak lain yang dibenarkan mencapai *server* berkenaan.

8.4.2 Kawalan Terhadap Pangkalan Data

- i. PTM bertanggungjawab mengawal capaian pangkalan data. Integriti data yang disimpan dalam pangkalan data dijamin melalui kawalan capaian data yang ditentukan oleh Pentadbir Pangkalan Data ; dan
- ii. PTM bertanggungjawab melaksanakan tugas-tugas rutin pangkalan data seperti :
 - a. *Performance tuning* setiap enam (6) bulan
 - b. Semakan pangkalan data secara konsisten
 - c. Semakan penggunaan ruang storan yang mencukupi

- d. Pemantauan aktiviti pangkalan data
- e. Pemantauan aktiviti *server* dan pengguna (*auditing*)
- f. Melaksanakan *back up* atau *restore*

8.4.3 Kawalan Terhadap Capaian Logikal

Kawalan dibuat semasa pemasangan sistem pengoperasian dan perisian yang dilakukan oleh kakitangan yang dibenarkan sahaja. Mekanisma kawalan capaian logikal yang dilakukan adalah seperti berikut:

i. Identifikasi Pengguna

- a. Pengguna sistem terdiri daripada individu atau kumpulan pengguna yang berkongsi akaun kumpulan pengguna yang sama dan bertanggungjawab ke atas keselamatan sistem yang digunakan.

UKM mengenalpasti pengguna yang sah melalui langkah berikut:

- memberi satu (1) ID yang unik kepada setiap pengguna individu;
- menyimpan dan menyelenggara semua ID pengguna yang bertanggungjawab untuk setiap aktiviti;
- memastikan adanya kemudahan pengauditan untuk menyemak semua aktiviti pengguna;
- memastikan semua ID pengguna yang diwujudkan adalah berdasarkan permohonan; dan
- perubahan ID pengguna untuk perisian aplikasi perlu mendapat kebenaran daripada Urus Setia Sistem Aplikasi tersebut.

- b. UKM mengenalpasti ID pengguna yang tidak aktif tidak disalahgunakan melalui langkah berikut:
- menggantung semua kemudahan ID yang tidak digunakan selama 60 hari dan menghapuskan ID berkenaan selepas daripada tempoh 60 hari tersebut; dan
 - menghapus semua kemudahan untuk pengguna yang berpindah jabatan atau tamat perkhidmatan;

ii. Kesahihan Pengguna (*User Authentication*)

Proses pengesahan pengguna bertujuan mengenalpasti hanya pengguna yang sah dibenarkan mencapai sistem melalui ID pengguna dan kata laluan yang diberikan. Sistem mestilah boleh menyediakan kemudahan seperti berikut:

- a. kata laluan dimasukkan dalam bentuk yang tidak boleh dilihat;
- b. panjang kata laluan sekurang-kurangnya lapan (8) aksara dengan kombinasi daripada aksara, angka dan simbol-simbol lain;
- c. kata laluan semasa penghantaran dienkrif (*encryption*);
- d. fail kata laluan disimpan berasingan daripada data sistem aplikasi utama; dan
- e. cubaan capaian dihadkan kepada lima (5) kali sahaja. ID pengguna berkenaan perlu digantung selepas lima (5) kali cubaan berturut-turut gagal.

iii. *Back up* Maklumat

Back up diperlukan untuk mengekalkan integriti dan ketersediaan maklumat serta kemudahan pemprosesan ICT. Proses *back up* melibatkan fail penting, data, perisian aplikasi

dan dokumentasi. PTM bertanggungjawab *restore* sepenuhnya jika berlaku masalah atau kerosakan;

PTM akan mengambil tindakan berikut semasa penyediaan *back up*:

- a. Mendokumen prosedur *back up* dan *restore*;
- b. Proses *back up* dibuat secara berjadual dan semasa perubahan konfigurasi pada sistem;
- c. Pita *back up* perlu disimpan di tempat berasingan dan selamat. Akses kepada lokasi storan hendaklah dikawal dengan ketat daripada akses tanpa izin;
- d. Menyimpan tiga (3) generasi pita *back up* untuk tempoh satu (1) tahun; dan
- e. Menguji pita *back up* dan prosedur *restore* dua (2) kali setahun.

iv. Penyelenggaraan

UKM memastikan integriti sistem pengoperasian (*Operating System contohnya: Windows XP*) daripada terdedah kepada sebarang pencerobohan keselamatan dengan melaksanakan kawalan dan penyelenggaraan seperti berikut:

- a. Mengemaskini *patches* yang disahkan daripada agensi keselamatan berdaftar seperti MyCERT dan GCERT terkini untuk mengatasi kelemahan sistem; dan
- b. Menaiktaraf sistem pengoperasian kepada versi terkini sesuai dengan spesifikasi peralatan ICT sedia ada.

8.5 Keselamatan Peralatan Rangkaian

8.5.1 Kawalan Terhadap Keselamatan Pemasangan Peralatan Rangkaian

Setiap peralatan yang akan dipasang mestilah mematuhi *Factory Acceptance Check* (FAC) sebelum pemasangan dan konfigurasi dilakukan.

8.5.2 Kawalan Terhadap Konfigurasi Peralatan Rangkaian

Kawalan terhadap konfigurasi peralatan rangkaian berikut hendaklah dilaksanakan oleh kakitangan yang terlatih dan dibenarkan sahaja:

- i. Mengaktifkan (*enable*) perkhidmatan rangkaian yang diperlukan sahaja;
- ii. Mengehadkan capaian konfigurasi peralatan rangkaian kepada nod atau alamat IP yang dibenarkan sahaja;
- iii. Mematikan penyiaran trafik (*disable broadcast*); dan
- iv. Menggunakan kata laluan yang selamat.

8.5.3 Kawalan Terhadap Keselamatan Fizikal

- i. Kabel rangkaian hendaklah dilindungi dengan memasang *conduit* dan atau lain-lain mekanisma perlindungan;
- ii. Penggunaan tanpa wayar dilindungi dengan diletakkan di tempat selamat dan atau lain-lain mekanisma perlindungan;
- iii. Peralatan rangkaian hendaklah ditempatkan di dalam rak di lokasi yang selamat dan bebas daripada risiko di luar jangkaan seperti banjir, kilat, gegaran, kekotoran dan sebagainya;

- iv. Peralatan rangkaian hanya boleh dicapai oleh kakitangan yang terlatih dan dibenarkan sahaja;
- v. Had suhu peralatan rangkaian berkenaan dikawal dengan memasang sistem penghawa dingin sepanjang masa;
- vi. *Uninterruptible Power Supply* (UPS) dipasang dengan minimum 15 minit masa beroperasi sekiranya terputus bekalan elektrik dan perlindungan daripada kilat (*power surge protector*);
- vii. Generator Set yang bersesuaian dipasang untuk memastikan peralatan berfungsi apabila berlaku gangguan bekalan elektrik;
- viii. Pusat pendawaian (*wiring closet*) diletakkan di dalam ruang atau bilik yang berkunci dan hanya boleh dicapai oleh kakitangan yang dibenarkan sahaja; dan
- ix. Menyelenggara inventori peralatan rangkaian dan membuat semakan secara berkala.

8.5.4 Kawalan Terhadap Capaian Logikal

i. Rangkaian Berwayar (*wired*)

- a. ID pengguna dan kata laluan diperlukan untuk mencapai perisian rangkaian. Capaian hanya boleh dibuat oleh kakitangan yang dibenarkan sahaja;
- b. Komposisi kata laluan mestilah konsisten dengan garis panduan yang telah ditetapkan;
- c. Maklumat capaian ke *router* (nama pegawai bertanggungjawab, tarikh, masa dan aktiviti) hendaklah direkodkan;
- d. Rangkaian UKM hanya menerima trafik daripada alamat IP dalaman yang berdaftar sahaja;

- e. Semua perubahan konfigurasi suis rangkaian hendaklah dilogkan (nama pegawai bertanggungjawab, tarikh dan masa); dan
- f. Perubahan perisian konfigurasi mestilah direkodkan (pegawai yang membuat perubahan, pegawai yang membenarkan perubahan dibuat dan tarikh) dan dikendalikan secara berpusat.

ii. Rangkaian Wayarles (WiFi)

- a. Penggunaan nama *access point* (SSID AP) seperti yang telah diperuntukkan contoh: tetamu-ukm atau pelajar;
- b. Penyambungan dan penghalaan *access point* hendaklah ke rangkaian UKM;
- c. kawalan terhadap capaian warga UKM dan pihak-pihak lain dilakukan melalui penggunaan IP secara dinamik (DHCP); dan
- d. mewujudkan mekanisme kawalan capaian untuk warga UKM dan pihak-pihak lain mencapai sesuatu *server* yang berkenaan sahaja
- e. Penggunaan nama *access point* (SSID) seperti yang telah ditetapkan oleh UKM (contoh: tetamu-ukm)

8.5.5 Kawalan Terhadap Penyelenggaraan Peralatan Rangkaian

Peralatan rangkaian hendaklah dipasang, dioperasi dan diselenggara mengikut spesifikasi pengilang oleh kakitangan yang terlatih dan dibenarkan sahaja. Penyelenggaraan peralatan hendaklah direkodkan.

8.6 Keselamatan Rangkaian

8.6.1 Kebolehcapaian Pengguna (*User Accessibility*)

i. Rangkaian Setempat (*Local Area Network*)

- a. Hanya kakitangan dan pelajar UKM dibenarkan membuat penyambungan ke rangkaian UKM, rujuk Bab 5: Pengurusan Rangkaian UKM (perenggan 5.5);
- b. Pengguna luar perlu mendapatkan kebenaran PTM sebelum membuat capaian ke rangkaian UKM;
- c. Pengguna yang disahkan sahaja dibenarkan membuat capaian ke rangkaian UKM;
- d. Penggunaan perisian pengintip (*sniffer*) atau penganalisis rangkaian (*network analyzer*) tidak dibenarkan; dan
- e. Status komputer (*IP Address* dan lokasi *port*) hendaklah disemak setiap tahun oleh PTM untuk memastikan komputer didaftarkan dan berfungsi dengan baik.

ii. Rangkaian Wayarles (*WIFI*)

- a. Hanya kakitangan dan pelajar UKM dibenarkan menggunakan rangkaian wayarles UKM rujuk Bab 5: Pengurusan Rangkaian UKM (perenggan 5.5);
- b. Pengguna luar perlu mendapatkan kebenaran UKM secara *online* sebelum menggunakan rangkaian tanpa wayar;
- c. Pengguna yang disahkan sahaja dibenarkan membuat capaian ke Rangkaian UKM; dan
- d. Penggunaan perisian pengintip (*sniffer*) atau penganalisis rangkaian (*network analyzer*) tidak dibenarkan;

8.6.2 Sambungan Dengan Lain-Lain Rangkaian

i. Capaian Yang Tidak Digalakkan

- a. Penggunaan protokol rangkaian selain daripada TCP/IP seperti NetBIOS dan IPX/SPX; dan
- b. Penggunaan *workgroup* tidak digalakkan kerana menyokong *share-level security*.

ii. Firewall

- a. Semua trafik rangkaian daripada dalam ke luar UKM dan sebaliknya mestilah melalui *firewall* dan hanya trafik yang disahkan sahaja dibenarkan untuk melepasi;
- b. Reka bentuk *firewall* hendaklah mengambilkira perkara berikut:
 - keperluan audit dan arkib;
 - kebolehsediaan;
 - kerahsiaan; dan
 - melindungi maklumat UKM
- c. PTJ atau kumpulan penyelidik yang dibenarkan mempunyai *server* sendiri digalakkan menyediakan *firewall* khusus untuk tujuan keselamatan.

8.7 Keselamatan Akaun *E-mail*

8.7.1 Kawalan Terhadap Penggunaan Akaun *E-mail*

- i. Pengguna digalakkan tidak membuka *attachment* yang diragui mengandungi *letterbombs* atau virus yang boleh merosakkan komputer dan rangkaian UKM. *Attachment* yang sering mengandungi virus ialah fail yang mempunyai *extension* .exe, .zip, .pif, .scr dan sebagainya;

- ii. Pengguna digalakkan tidak menjawab *e-mail* yang tidak berkenaan seperti *spam*, ugutan atau ofensif kerana dengan menjawab *e-mail* yang sedemikian pengguna mendedahkan diri kepada aktiviti yang tidak bertanggungjawab. Pengguna adalah bertanggungjawab untuk melaporkan kepada *Postmaster*;
- iii. *Postmaster* dengan kelulusan Pengarah PTM berhak memeriksa dan melihat isi kandungan *e-mail* dan ruang storan pengguna dari semasa ke semasa atas keperluan audit dan keselamatan; dan
- iv. Setiap *e-mail* rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan.

8.7.2 Kawalan Terhadap Penyelenggaraan *Mailbox*

- i. Pengguna bertanggungjawab menyelenggara kandungan *mailbox* pada komputer peribadi;
- ii. Pengguna hendaklah sentiasa mengimbas fail dalam *mailbox* dengan perisian *anti virus* bagi memastikan fail yang disimpan, dihantar atau diterima melalui *attachment* bebas daripada virus;
- iii. *e-mail* hendaklah tidak mengandungi maklumat rahsia atau sulit yang boleh disalahgunakan untuk merosakkan akaun, stesen kerja, *server* dan rangkaian UKM; dan
- iv. Pengguna bertanggungjawab menghapuskan kandungan *e-mail* yang tidak penting, tidak mempunyai nilai arkib dan yang tidak diperlukan lagi.

8.7.3 Kawalan Terhadap Penggunaan Perisian *e-Mail*

- i. Pengguna digalakkan menggunakan perisian *e-mail* rasmi UKM yang lebih selamat daripada ancaman dan penyebaran virus untuk urusan rasmi; dan
- ii. Pengguna yang tidak menggunakan perisian *e-mail* rasmi UKM hendaklah sentiasa membuat *back up* terhadap kandungan *e-mail* berkenaan.

8.8 Jejak Audit

- i. UKM bertanggungjawab menyediakan dan menyimpan rekod jejak audit bagi mengenalpasti akauntabiliti pengguna dan keselamatan. Jejak audit perlu diwujudkan apabila terdapat:
 - a. capaian kepada maklumat kritikal;
 - b. capaian kepada perkhidmatan rangkaian; dan
 - c. keistimewaan atau kebenaran tertentu yang melebihi kebenaran sebagai pengguna biasa digunakan seperti arahan keselamatan dan fungsi *super-user*.
- ii. Rekod jejak audit merangkumi :
 - a. identifikasi pengguna (ID pengguna dan kata laluan);
 - b. fungsi, sumber dan maklumat yang digunakan atau dikemaskini;
 - c. tarikh dan masa penggunaan;
 - d. alamat IP; dan
 - e. maklumat terperinci mengenai perubahan atau status permintaan;

- iii. UKM akan mengambil tindakan berikut semasa penyediaan jejak audit:
 - a. meneliti dan melaporkan sebarang aktiviti yang diragui dan kejadian luar biasa dengan segera kepada UKMCERT;
 - b. menyimpan rekod jejak audit untuk jangka masa tertentu bagi keperluan operasi dan keselamatan; dan
 - c. mengawal rekod jejak audit daripada dihapus, diubahsuai, ditipu atau disusun semula.
- iv. Jejak audit untuk setiap aktiviti pengguna hendaklah disimpan dan diarkib terutamanya untuk pengguna yang boleh mencapai maklumat sulit agar dapat dikenalpasti sekiranya berlakunya pencerobohan maklumat.

8.9 Pengurusan Insiden Keselamatan ICT

- i. Pengguna hendaklah melaporkan insiden keselamatan ICT kepada UKMCERT dengan kadar segera sekiranya mendapati:
 - a. Percubaan (sama ada gagal atau berjaya) untuk mencapai sistem atau data tanpa kebenaran (*probing*);
 - b. Serangan kod jahat (*malicious code*) seperti virus, trojan horse, worms dan sebagainya;
 - c. Gangguan yang disengajakan (*unwanted disruption*) atau halangan pemberian perkhidmatan (*denial of service*);
 - d. Menggunakan sistem untuk pemprosesan data atau penyimpanan data tanpa kebenaran (*unauthorized access*);
 - e. Pengubahsuaian ciri-ciri perkakasan, perisian data atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak;

- f. Maklumat didapati hilang, didedah kepada pihak yang tidak diberi kuasa atau disyaki hilang atau didedahkan kepada pihak yang tidak diberi kuasa;
 - g. Sistem Maklumat Universiti digunakan tanpa kebenaran atau disyaki sedemikian;
 - h. Kata laluan atau mekanisme kawalan sistem akses hilang, dicuri atau didedahkan atau disyaki hilang, dicuri atau didedahkan;
 - i. kejadian perkara luar biasa di dalam sistem seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan
 - j. percubaan mencero boh, menyeleweng dan insiden yang tidak diingini;
- ii. ICTSO perlu menentukan tahap keutamaan insiden, melaporkan insiden kepada GCERT dan mengambil langkah pemulihan awal.

8.10 Tindakan Penguatkuasaan dan Pematuhan

Mana-mana pihak yang gagal untuk mematuhi peruntukan Bab ini boleh dikenakan tindakan penguatkuasaan bagi tujuan pematuhan di bawah Bab 9.



**Dasar dan Peraturan ICT
Universiti Kebangsaan Malaysia**

Bab 9:

Tindakan Penguatkuasaan Dan Pematuhan

Bab 9: Tindakan Penguatkuasaan dan Pematuhan

9.1 Tujuan

- i. Menyatakan penguatkuasaan dan tindakan yang perlu diambil terhadap pelanggaran mana-mana bahagian di dalam Dasar ini;
- ii. Warga UKM dan pihak-pihak lain yang berkaitan bertanggungjawab untuk membaca, memahami dan mematuhi Dasar ini;
- iii. Penguatkuasaan dan tindakan yang diambil adalah sebagai salah satu langkah untuk mendidik pengguna supaya mematuhi Dasar ini; dan

9.2 Skop

Meliputi semua peraturan yang dinyatakan di dalam Dasar ini serta mana-mana Akta, Arahan, Pekeliling dan Peraturan yang berkaitan di peringkat kebangsaan.

9.3 Jenis Pelanggaran

Pelanggaran yang berlaku terfokus kepada bab tertentu seperti berikut:

Bab	Tindakan Terhadap Pelanggaran
Bab 2	Tindakan Terhadap Pelanggaran Penggunaan Perisian Tidak Berlesen
Bab 3	Tindakan Terhadap Pelanggaran Pinjaman Perkakasan ICT
Bab 4	Tindakan Terhadap Pelanggaran Peraturan Penggunaan Makmal Komputer
BAB 5	Tindakan Terhadap Pelanggaran Penggunaan Kemudahan Rangkaian UKM
Bab 6	Tindakan Terhadap Pelanggaran Penggunaan <i>E-Mail</i>
Bab 6	Tindakan Terhadap Pelanggaran Pembangunan Kandungan Laman Web

Bab	Tindakan Terhadap Pelanggaran
Bab 6	Tindakan Terhadap Pelanggaran Capaian Internet Atau Intranet
Bab 7	Tindakan Terhadap Pelanggaran Capaian Maklumat Sulit

9.4 Jenis Pelanggaran dan Tindakan Terhadap Pelanggaran

i. Tindakan Terhadap Pelanggaran Penggunaan Perisian Tidak Berlesen	
Pelanggaran	Tindakan Terhadap Pelanggaran
<p>a. Memuat turun, mengubahsuai, mendedahkan, membuat pemasangan, menghapuskan dan menggunakan perisian yang boleh menyebabkan kerosakan komputer dan Rangkaian UKM;</p> <p>b. Menjual, menyewa, melesen semula, meminjamkan, menyalin semula, menyebar atau memberi semua perisian hakmilik UKM kepada individu atau entiti tanpa kebenaran UKM; dan</p> <p>c. Sebarang bentuk permainan komputer (kecuali untuk tujuan pengajaran dan penyelidikan) tanpa kelulusan Ketua PTJ.</p>	<p>a. Pengguna diminta untuk <i>uninstall</i> perisian yang tidak berlesen tersebut; dan</p> <p>b. Pengguna dikenakan penggantungan penggunaan kemudahan ICT di UKM oleh Jawatankuasa Keselamatan ICT UKM.</p>

ii. Tindakan Terhadap Pelanggaran Pinjaman Perkakasan ICT	
Pelanggaran	Tindakan Terhadap Pelanggaran
<p>a. Peminjam memulangkan perkakasan ICT yang dipinjam dalam keadaan tidak berfungsi (rosak) dan dalam set tidak lengkap pada tarikh yang ditetapkan;</p> <p>b. Peminjam mencerooboh dan mencuri</p>	<p>d. Peminjam menanggung keseluruhan kos baik pulih;</p> <p>e. Peminjam menggantikan perkakasan ICT berdasarkan spesifikasi yang sama atau lebih tinggi sekiranya berlaku</p>

ii. Tindakan Terhadap Pelanggaran Pinjaman Perkakasan ICT

Pelanggaran	Tindakan Terhadap Pelanggaran
<p>perkakasan ICT atau komponennya; dan</p> <p>c. Peminjam menghilangkan perkakasan ICT yang dipinjam</p>	<p>kerusakan disebabkan kecuaiian dan tidak boleh dibaiki; dan</p> <p>f. Peminjam menggantikan perkakasan ICT yang hilang disebabkan kecuaiian berdasarkan spesifikasi yang sama atau lebih tinggi</p>

iii. Tindakan Terhadap Pelanggaran Penggunaan Kemudahan Rangkaian UKM

Pelanggaran	Tindakan Terhadap Pelanggaran
<p>a. Pengguna tidak boleh membenarkan sumber rangkaian di bawah kawalannya termasuk tetapi tidak terhad kepada nod rangkaian dan kad <i>wireless</i> untuk diguna oleh pihak-pihak lain walaupun kepada warga UKM tanpa mendapat kelulusan PTM;</p> <p>b. Perolehan peralatan rangkaian dan penyambungan ke rangkaian UKM perlu mendapat kelulusan PTM. Konfigurasi penyambungan hendaklah dibuat oleh pembekal di bawah pengawasan dan kawalan PTM</p>	<p>a. UKM akan memutuskan penyambungan rangkaian; atau</p> <p>b. UKM akan meningkatkan tahap keselamatan capaian bagi pengguna yang amat memerlukan kemudahan tersebut (tertakluk kepada justifikasi penggunaan); atau</p> <p>c. UKM akan menggantikan sistem capaian yang tiada kawalan kepada sistem capaian di bawah kawalan PTM sepenuhnya</p>

iv. Tindakan Terhadap Pelanggaran Peraturan Penggunaan Makmal Komputer

Pelanggaran	Tindakan Terhadap Pelanggaran
<p>a. Menggunakan komputer bukan untuk tujuan akademik seperti main 'computer game' atau</p>	<p>Pengguna yang melanggar mana-mana peraturan yang ditetapkan boleh diambil tindakan tegas,</p>

ii. Tindakan Terhadap Pelanggaran Pinjaman Perkakasan ICT

Pelanggaran	Tindakan Terhadap Pelanggaran
<p>sembang siber (<i>chatting</i>);</p> <p>b. makan dan minum;</p> <p>c. menghisap rokok;</p> <p>d. membuat bising termasuk tetapi tidak terhad kepada berbual, berbincang, memasang dan mendengar muzik;</p> <p>e. mengganggu pengguna lain dengan apa cara sekalipun, termasuk menimbulkan rasa aib, marah dan tidak selesa;</p> <p>f. berkelakuan tidak senonoh atau mengaibkan;</p> <p>g. menukar kedudukan komputer dan peranti;</p> <p>h. menukar konfigurasi komputer;</p> <p>i. menambah atau membuang sebarang perisian;</p> <p>j. menyimpan atau memuat turun maklumat atau data ke dalam cakera keras komputer;</p> <p>k. membawa keluar sebarang peralatan dari makmal; dan</p> <p>l. membawa keluar peranti dan perkakasan komputer.</p>	<p>termasuk tetapi tidak terhad kepada:</p> <p>a. Dilarang masuk menggunakan peralatan di dalam makmal;</p> <p>b. Ditarik balik kemudahan akaun pengguna (jika ada);</p> <p>c. Mengganti atau membayar kos peralatan yang dicuri, hilang atau rosak atas kecuaiian semasa penggunaan; dan</p> <p>d. Dihadapkan ke Jawatankuasa Tatatertib Kakitangan bagi kakitangan atau Pihak Berkuasa Tatatertib Pelajar bagi pelajar</p>

iv. Tindakan Terhadap Pelanggaran Penggunaan E-Mail

Pelanggaran	Tindakan Terhadap Pelanggaran
a. Menggunakan akaun <i>e-mail</i> atau menyamar sebagai pihak lain;	a. Diberi <i>e-mail</i> amaran oleh Pentadbir Sistem;
b. Menggunakan kemudahan <i>e-mail</i> untuk sebarang aktiviti yang tidak dibenarkan oleh peraturan UKM dan undang-undang negara; dan	b. Disekat daripada menggunakan kemudahan <i>e-mail</i> UKM; dan
c. Melakukan aktiviti <i>spamming</i> , <i>mail-bombing</i> , <i>phishing</i> dan atau penyebaran <i>e-mail</i> dengan kandungan tidak beretika kepada individu, <i>mailing list</i> atau <i>discussion group</i> sama ada di dalam rangkaian UKM atau ke Internet;	c. Digantung penggunaan kemudahan ICT di UKM oleh Jawatankuasa Keselamatan ICT UKM.

v. Tindakan Terhadap Pelanggaran Pembangunan Kandungan Laman Web

Pelanggaran	Tindakan Terhadap Pelanggaran
a. Membangunkan laman web yang mengandungi pautan kepada maklumat atau terdedah kepada kemasukan maklumat yang menyalahi peraturan UKM dan undang-undang negara; dan	a. Amaran kepada pemilik laman web; dan
b. Ini termasuk tetapi tidak terhad kepada maklumat yang berbentuk keganasan, lucah, hasutan dan yang boleh menimbulkan atau membawa kepada keganasan, keruntuhan akhlak dan kebencian;	b. Capaian laman web disekat atau dibatalkan.

vi. Tindakan Terhadap Pelanggaran Capaian Internet atau Intranet

Pelanggaran	Tindakan Terhadap Pelanggaran
<p>a. Mengganggu atau mencero boh laman web mana-mana jabatan, organisasi di dalam atau luar negara;</p> <p>b. Memasuki, menyalin, meniplak, mencetak dan menyebarkan maklumat daripada Internet yang menyalahi undang-undang negara;</p> <p>c. Menggunakan sumber ICT UKM atau persendirian untuk mendapatkan atau cuba mendapatkan capaian tidak sah daripada mana-mana sistem komputer sama ada di dalam atau luar UKM. Ini termasuk membantu, mendorong, menyembunyikan percubaan untuk mencapai sistem komputer tersebut atau mencapai sumber ICT UKM dengan menggunakan identiti pengguna lain;</p> <p>d. Mencapai atau cuba mencapai sumber elektronik sama ada dalam bentuk data, paparan, <i>keystrokes</i>, fail atau media storan dalam sebarang bentuk yang dimiliki oleh pengguna lain tanpa mendapat kebenaran atau kelulusan pengguna terbabit terlebih dahulu. Ini termasuk membaca, menyalin, menukar, merosak atau memadam data, program dan perisian;</p> <p>e. Menyambung peranti elektronik termasuk tetapi tidak terhad kepada komputer peribadi atau notebook dan <i>hub</i> atau <i>switch</i> peribadi atau modem ke rangkaian UKM dengan tujuan mencapai sumber ICT yang tidak dibenarkan; dan</p> <p>f. Menggunakan perisian penggadam komputer atau rangkaian</p>	<p>a. Alamat IP <i>port</i> capaian yang berkenaan disekat sepanjang tempoh siasatan; dan</p> <p>b. Menyita kemudahan ICT yang diberikan.</p>

vii. Tindakan Terhadap Pelanggaran Capaian Maklumat Sulit

Pelanggaran	Tindakan Terhadap Pelanggaran
<p>a. Menggunakan kemudahan ICT untuk menyimpan data atau maklumat sensitif, rahsia atau sulit di dalam komputer atau akaun pengguna tanpa kebenaran;</p> <p>b. Menggunakan identiti pengguna lain untuk mencuri data atau merosakkan sumber ICT; dan</p> <p>c. Mencapai data atau maklumat pengguna lain tanpa kebenaran</p>	<p>a. ID pengguna dibatalkan;</p> <p>b. <i>Port</i> capaian yang berkenaan disekat sepanjang tempoh siasatan;</p> <p>c. Menyita kemudahan ICT yang diberikan;</p> <p>a. Dihadapkan ke Jawatankuasa Tatatertib Kakitangan bagi kakitangan atau Pihak Berkuasa Tatatertib Pelajar bagi pelajar.</p>



UNIVERSITI KEBANGSAAN MALAYSIA
National University of Malaysia

Dasar dan Peraturan ICT Universiti Kebangsaan Malaysia

Bab 10: e-Pembelajaran

Bab 10: e-Pembelajaran

10.1 Tujuan

Memperihal dan memperincikan Bab ini untuk meningkatkan kualiti pengajaran dan pembelajaran kursus yang ditawarkan di peringkat prasiswazah dan siswazah. Bab ini disediakan berdasarkan Pelan Strategik UKM serta resolusi berkaitan dengan e-Pembelajaran UKM dibuat semasa Bengkel Pelaksanaan Dasar ICT UKM pada tahun 2005.

10.2 Skop

Meliputi aspek takrif e-Pembelajaran, dasar umum e-pembelajaran, tahap e-Pembelajaran, peranan dan tanggungjawab pengurusan, fakulti, pensyarah dan pelajar, kualiti kandungan e-pembelajaran serta Hak Cipta dan Harta Intelek.

10.3 Takrif

Secara umumnya, e-Pembelajaran adalah persekitaran elektronik yang berpusatkan pelajar dan pembelajaran bertujuan meningkatkan keberkesanan proses dan prestasi pengajaran dan pembelajaran.

i. Skop e-Pembelajaran

Skop e-Pembelajaran adalah bentuk instruksi (pengajaran dan pembelajaran) yang dikendalikan melalui media elektronik dan atau sistem rangkaian komputer bertujuan meningkatkan keberkesanan proses pengajaran & pembelajaran.

ii. Sistem Pengurusan e-Pembelajaran (SPe-P)

Sistem Pengurusan e-Pembelajaran (SPe-P) adalah perisian sistem pengurusan berarahan yang mempunyai komponen seperti berikut:

- a. Komponen Kandungan/Bahan Kursus
- b. Komponen Rekabentuk Instruksi
- c. Komponen Pensyarah
- d. Komponen Pelajar
- e. Komponen Penilaian
- f. Komponen Komunikasi
- g. Komponen Pentadbir
- h. Komponen Pentadbir Sistem

10.4 Umum

- i. e-Pembelajaran di UKM adalah kaedah instruksi pelengkap serta sistem sokongan yang digunakan oleh pensyarah bertujuan meningkatkan kualiti dan keberkesanan pengajaran dan pembelajaran;
- ii. e-Pembelajaran di UKM digunakan dalam mod *blended learning* iaitu gabungan antara kaedah pembelajaran konvensional dan kaedah pembelajaran maya. Justeru, pensyarah dan pelajar masih bertemu di bilik kuliah secara bersemuka mengikut jadual yang ditetapkan oleh UKM;
- iii. Maklumat asas (silibus) setiap kursus yang ditawarkan oleh UKM pada setiap semester diperingkat prasiswazah dan siswazah disediakan secara atas talian mengikut format Kerangka Kelayakan Malaysia (KKM);
- iv. Kandungan kursus secara atas talian perlu diperkayakan secara berperingkat;
- v. Semua pensyarah perlu meningkatkan pengetahuan, kemahiran untuk menguruskan pengajaran dan pembelajaran secara atas talian;

- vi. Semua pelajar perlu mempunyai pengetahuan dan kemahiran berkaitan e-Pembelajaran; dan
- vii. UKM bertanggungjawab menyediakan sumber, latihan dan sokongan berkaitan dengan e-pembelajaran.

10.5 Tahap Pelaksanaan e-Pembelajaran

i. Tahap 1

- a. Maklumat kursus yang merangkumi sinopsis, objektif, hasilan pembelajaran, kandungan, kaedah pengajaran dan pembelajaran bentuk penilaian, rujukan asas, perincian beban pembelajaran pelajar serta maklumat kontak pensyarah wajib disediakan; dan
- b. Setiap pensyarah dan pelajar berkomunikasi melalui e-mel mengenai kursus yang ditawarkan berdasarkan garis panduan yang disediakan (PPA/Pe-P/2007/3).

ii. Tahap 2

- a. Pensyarah merancang & melaksanakan aktiviti berikut melalui SPe-P UKM:
 - Menyediakan Nota Kuliah (dalam bentuk *pdf* dan atau dalam bentuk yang sesuai mengikut bidang) secara atas talian;
 - Menguruskan Forum/Perbincangan secara atas talian berdasar garis panduan yang disediakan (PPA/SPe-P/2007/4);
 - Menyediakan soalan latihan/kuiz secara atas talian;
 - Menyediakan alternatif kepada pelajar untuk menghantar tugas secara atas talian berdasarkan garis panduan yang disediakan (PPA/SPe-P/2007/5); dan

- Menyediakan sumber rujukan tambahan secara atas talian.

iii. Tahap 3

- a. Pensyarah membangunkan kandungan pembelajaran interaktif akses sendiri dalam bentuk *Learning Objects*. Bahan pembelajaran tersebut perlu disediakan berdasarkan pedagogi yang menepati piawai *Shareable Content Object Reference Model (SCORM)*.

10.6 Peranan Dan Tanggungjawab

i. Pengurusan Universiti

- a. Majlis Teknologi Maklumat UKM bertanggungjawab menetapkan hala tuju dan dasar serta strategi pelaksanaan e-Pembelajaran UKM; dan
- b. menyediakan dana untuk menjayakan pelaksanaan e-Pembelajaran di UKM

ii. Pusat Pembangunan Akademik

- a. Merancang, menyelaras dan memantau pelaksanaan e-Pembelajaran di UKM;
- b. Mempengerusi Jawatankuasa e-Pembelajaran UKM yang bertanggungjawab melaporkan perancangan, pemantauan & pelaksanaan e-Pembelajaran kepada Majlis Teknologi Maklumat UKM;
- c. Meningkatkan literasi dan latihan kepada pensyarah berkaitan dengan e-Pembelajaran;
- d. Menyediakan latihan sokongan kepada pensyarah untuk membangunkan kandungan pengajaran interaktif akses sendiri

dalam bentuk *Learning Objects* yang menepati piawai SCORM; dan

- e. Mengawal, memantau serta menambahbaik kualiti pengajaran dalam mod e-pembelajaran.

iii. Fakulti atau Pusat Kembangan Pendidikan (PKP)

- a. Membentuk Jawatankuasa Pelaksanaan e-Pembelajaran di peringkat fakulti bagi memantau pelaksanaan e-Pembelajaran di fakulti;
- b. Memastikan maklumat asas semua kursus yang ditawarkan oleh Fakulti disediakan secara atas talian melalui SPe-P UKM;
- c. Merancang supaya setiap pensyarah menguasai kemahiran yang secukupnya berkaitan e-Pembelajaran;
- d. Pensyarah bertanggungjawab sepenuhnya terhadap kandungan pengajaran yang dimasukkan dalam SPe-P UKM dan mengemaskini dari masa ke semasa sekurang-kurangnya sekali setiap semester;
- e. Pensyarah secara berperingkat memperkayakan kandungan aktiviti kursus termasuk nota kuliah, forum, soalan latihan atau kuiz, tugas dan sumber rujukan secara atas talian melalui SPe-P UKM;
- f. Pensyarah secara berperingkat memperkayakan kandungan kursus dalam bentuk *Learning Objects* atau bahan pembelajaran interaktif secara akses sendiri melalui SPe-P UKM;
- g. Pensyarah melaksanakan garis panduan umum e-Pembelajaran yang bersesuaian:
 - Garis Panduan Umum e-Pembelajaran Kursus (PPA/Pe-P/2007/1)

- Garis Panduan e-Mel Kursus (PPA/P-eP/2007/3)
 - Garis Panduan Forum/Diskusi Atas Talian Kursus (PPA/P-eP/2007/4)
 - Garis Panduan Penghantaran Tugas Kursus Secara Atas Talian (PPA/P-eP/2007/5)
 - Garis Panduan Bantuan Teknikal Sistem Pengurusan e-Pembelajaran UKM (PPA/P-eP/2007/6)
- h. Pensyarah bertanggungjawab menjaga privasi pelajar berkaitan dengan tugas dan interaksi dalam e-mel atau forum kursus. Sekiranya pensyarah ingin menggunakan maklumat tersebut untuk tujuan penyelidikan dan/atau penerbitan perlulah mendapat kebenaran pelajar terlebih dahulu (PPA/Pe-P/2007/2);
- i. Kontrak Kod Amalan Pelajar Atas Talian ditandatangani oleh pelajar yang melaksanakan aktiviti atau tugas kursus yang sebahagian atau sepenuhnya dikendalikan secara atas talian (PPA/Pe-P/2007/7);
- j. Pelajar memahami dan mematuhi garis panduan yang disediakan oleh pensyarah seperti berikut:
- Garis Panduan Umum e-Pembelajaran Kursus (PPA/Pe-P/2007/1)
 - Garis Panduan e-Mel Kursus (PPA/P-eP/2007/3)
 - Garis Panduan Forum/Diskusi Atas Talian Kursus (PPA/P-eP/2007/4)
 - Garis Panduan Penghantaran Tugas Kursus Secara Atas Talian(PPA/P-eP/2007/5)
 - Garis Panduan Bantuan Teknikal Sistem Pengurusan e-Pembelajaran UKM (PPA/P-eP/2007/6)

iv. Pusat Teknologi Maklumat

- a. Menyedia dan menyelenggara infrastruktur perkakasan, rangkaian, perisian dan sokongan yang berkaitan dengan e-Pembelajaran;
- b. Menjamin keselamatan serta integriti data dalam SPE-P UKM;
- c. Membuat *back up* data setiap semester dan disimpan selama dua (2) tahun;
- d. Menyediakan pegawai yang mengurus serta menyelenggara SPE-P UKM; dan
- e. Menyediakan sokongan teknikal kepada perkara (a – d)

v. Jawatankuasa Kualiti Kandungan e-Pembelajaran

- a. Kualiti kandungan bahan asas pengajaran setiap kursus yang disediakan oleh pensyarah secara atas talian seperti nota kuliah dan soalan latihan atau kuiz perlulah selaras dengan objektif dan hasil pembelajaran kursus serta memenuhi piawai yang ditetapkan oleh Fakulti masing-masing;
- b. Kualiti kandungan bahan pembelajaran yang dibangunkan oleh pensyarah dalam bentuk *Learning Objects* atau bahan interaktif akses sendiri dalam SPE-P UKM perlulah memenuhi piawai SCORM dan dikawal mutunya oleh sebuah Jawatankuasa yang dipengerusikan oleh PPA; dan
- c. Jawatankuasa Kualiti Kandungan e-Pembelajaran mengawal kualiti kandungan bahan e-pembelajaran interaktif akses sendiri dalam bentuk *Learning Objects*.

vi. Pusat Perkembangan Pelajar

Melatih pelajar menggunakan sistem e-Pembelajaran

10.7 Hak Cipta Dan Harta Intelek

10.7.1 Bahan e-pembelajaran yang dibangunkan oleh pensyarah dalam SPE-P UKM adalah tertakluk kepada Dasar Teknologi Maklumat dan Komunikasi UKM berkaitan Hak Cipta dan Harta Intelek iaitu:

- i. Semua bahan pengajaran yang dibangunkan menggunakan kemudahan dan sokongan yang disediakan oleh UKM adalah hak bersama pensyarah dan UKM. UKM berhak menggunakan bahan tersebut untuk diajar oleh pensyarah lain selain pensyarah yang menyediakan bahan pengajaran tersebut. Pensyarah bagaimana pun boleh menggunakan kandungan tersebut untuk kegunaan lain seperti pengajaran di dalam kelas, penyelidikan, penerbitan serta pembentangan dalam seminar; dan
- ii. Sekiranya pensyarah menerima ganjaran dan/atau insentif dalam bentuk pengurangan beban tugas, geran atau sugu hati kerana membangunkan bahan e-Pembelajaran serta mendapat bantuan Pereka Instruksi dan/atau *Content Developer* yang disediakan oleh UKM, hak cipta yang dihasilkan adalah milik UKM. Ianya tidak boleh digunakan diluar UKM tanpa mendapat kebenaran UKM terlebih dahulu.

10.8 Lain-lain

10.8.1 UKM berhak mengubah dasar ini dari masa ke semasa; dan

10.8.2 Dasar e-Pembelajaran UKM disemak sekurang-kurangnya setiap tiga (3) tahun bagi memenuhi keperluan serta kehendak semasa dengan mengambil kira semua *stakeholder*.



Dasar dan Peraturan ICT Universiti Kebangsaan Malaysia

Bab 11:

**Perihal Pemakaian, Pematuhan dan
Pertikaian Undang-undang**

Bab 11: Perihal Pemakaian, Pematuhan dan Pertikaian Undang-undang

11.1 Pemakaian Dasar Teknologi Maklumat UKM

Dengan berkuatkuasanya Dasar Teknologi Maklumat UKM Versi 3.0 berkuatkuasa 1 Oktober 2009 maka dasar-dasar terdahulu adalah dengan sendirinya terbatal iaitu:

- i. Polisi Teknologi Maklumat UKM Versi 1.0 (tarikh kuatkuasa : 26 Mac 2007)
- ii. Dasar Teknologi Maklumat UKM Versi 2.0 (tarikh kuatkuasa : 1 Julai 2008)

11.2 Pemakaian Peruntukan Undang – Undang Malaysia

Jika terdapat mana-mana peruntukan di dalam Dasar Teknologi Maklumat dan Komunikasi UKM atau sebahagian daripadanya yang diputuskan sebagai tidak sah atau terbatal atau tidak boleh dikuatkuasakan oleh mana-mana peruntukan undang-undang yang sedang berkuatkuasa atau oleh Mahkamah, maka peruntukan tersebut akan menjadi tidak sah atau terbatal dan atau tidak boleh dikuatkuasakan setakat mana yang bertentangan dan akan ditafsirkan seolah-olah peruntukan tersebut tidak menjadi sebahagian daripada Dasar Teknologi Maklumat dan Komunikasi UKM.

11.3 Pematuhan Kepada Undang – Undang

UKM dan setiap pengguna adalah dengan ini dikehendaki mematuhi segala undang-undang dan peraturan-peraturan mengenai penggunaan ICT yang sedang berkuatkuasa di Malaysia.

11.4 Pertikaian Undang-Undang

Jika berlaku sebarang pertikaian penggunaan Dasar ini ia adalah tertakluk di bawah bidang kuasa mahkamah dan undang-undang yang sedang berkuatkuasa di Malaysia.



Dasar dan Peraturan ICT Universiti Kebangsaan Malaysia

Lampiran

- **Lampiran A** : Struktur Majlis Teknologi Maklumat
- **Lampiran B** : Peranan Ketua Pegawai Maklumat (CIO)
- **Lampiran C** : Senarai Tugas ICTSO
- **Lampiran D** : Garis Panduan Pembangunan Laman Web

Majlis Teknologi Maklumat	
Terma Rujukan:	
<ul style="list-style-type: none"> menetapkan dasar dan dasar teknologi maklumat UKM memantau keberkesanan penggunaan teknologi maklumat menilai pencapaian penggunaan serta perancangan pelaksanaan teknologi maklumat di UKM 	
Keahlian Jawatankuasa:	
Pengerusi : Naib Canselor Urusetia : Pusat Teknologi Maklumat Ahli : <ul style="list-style-type: none"> TNC (HEAA) TNC (HEPI) TNC (HEPA) TNC (HEJIM) Penasihat Undang-Undang 	<ul style="list-style-type: none"> Pendaftar Bendahari Ketua Pustakawan Pengerusi (JKIO, JKTW, JKeP, JKPM) Wakil MIMOS Wakil MAMPU Wakil MDEC Ahli lain yang akan dilantik oleh Naib Canselor

Pusat Teknologi Maklumat

Jawatankuasa Infrastruktur dan Operasi	Jawatankuasa e-Pembelajaran	Jawatankuasa Penyelaras Maklumat	Jawatankuasa Tapak Web	Jawatankuasa Keselamatan ICT
Terma Rujukan	Terma Rujukan:	Terma Rujukan:	Terma Rujukan:	Terma Rujukan:
<ul style="list-style-type: none"> Merancang keperluan prasarana ICT Menyelaras pelaksanaan prasarana dan pembangunan Sistem ICT Menyelaras keperluan dan pelaksanaan Sistem Pengurusan Maklumat Universiti (SMPU) dan Sistem Sokongan Memantau penguatkuasaan langkah keselamatan ICT 	<ul style="list-style-type: none"> Merancang, menyelaras dan memantau pelaksanaan e-Pembelajaran Meningkatkan literasi dan latihan berkaitan dengan e-Pembelajaran Mengawal, memantau dan menambahbaik kualiti kandungan pengajaran dan e-Pembelajaran 	<ul style="list-style-type: none"> Menyelaras data/maklumat Universiti meliputi kakitangan, pelajar, penyelidikan, kewangan dan lain-lain Menyemak kesahihan dan ketepatan data Menyelaras pelaporan data dalam Sistem Maklumat Eksekutif 	<ul style="list-style-type: none"> Menyelaras dan memantau Kandungan Tapak Web UKM dan PTJ 	<ul style="list-style-type: none"> Membangun, menilai dan mengkaji semula Dasar ICT UKM dari semasa ke semasa; Menyebarkan dan menguatkuasakan Dasar kepada Warga UKM dan memantau pematuhannya; Menerima aduan Insiden Keselamatan ICT dan menjalankan siasatan teknikal ke atas sebarang pelanggaran Dasar; Menyediakan laporan Insiden Keselamatan ICT berdasarkan laporan daripada UKMCERT dan mengemukakan kepada Jawatankuasa Tatatertib Kakitangan bagi kakitangan dan Pihak Berkuasa Tatatertib Pelajar bagi pelajar; Memantau dan menambahbaik kaedah pelaksanaan keselamatan ICT di UKM
Keahlian Jawatankuasa	Keahlian Jawatankuasa	Keahlian Jawatankuasa	Keahlian Jawatankuasa	Keahlian Jawatankuasa
Pengerusi : Pengarah PTM (CIO) Urusetia : Pusat Teknologi Maklumat Ahli : <ul style="list-style-type: none"> Pendaftar Bendahari Ketua Pustakawan Pengarah PPUKM Pengarah JPP Timbalan Pengarah (Sistem Aplikasi & Pengurusan Maklumat) Timbalan Pengarah (Sokongan Penyelidikan & Pendidikan) Prof. Dr. Abdul Razak Hamdan Encik Sulaiman Jalil (ICTSO) Ketua Pusat Teknologi Maklumat PPUKM Wakil berkaitan daripada Fakulti/Pusat/Institut 	Pengerusi : TP e-Pembelajaran Urusetia : PPA Ahli : <ul style="list-style-type: none"> Pengarah PTM Ketua Pustakawan Dekan Fakulti Pendidikan Dekan FTSM Pengarah PKP Ahli-ahli lain yang dilantik oleh Pengerusi mengikut kesesuaian kepakaran yang diperlukan 	Pengerusi : Penyelaras Maklumat UKM Urusetia : PPKK Ahli : <ul style="list-style-type: none"> Bendahari Ketua Pustakawan Pengarah PTM Pengarah PPPI Pengarah Pejabat Perhubungan Alumni Pengarah PPS Pengarah PKP Pengarah Pejabat Hubungan Antarabangsa Timb. Pendaftar BSM Timb. Pendaftar BPA Ketua PP&P Ketua PPAK Ketua Pejabat Hubungan Industri Ketua Pengurusan Kualiti 	Pengerusi : Pengurus UNIKWeb Urusetia : UNIKWeb dan dibantu oleh PTM Ahli : <ul style="list-style-type: none"> Pengarah PTM Pengarah Pejabat Hubungan Antarabangsa Ketua Pejabat Perhubungan Awam & Korporat Ketua Pejabat Hubungan Industri Webmaster PTJ 	Pengerusi : Pengarah PTM (CIO) Urusetia : PTM Ahli: <ul style="list-style-type: none"> Prof. Dr. Kasmiran Jumari Penasihat Sistem TP (PP) / ICTSO TP (SPP)
				<ul style="list-style-type: none"> TP (SAPP) Ketua BPR Ketua BPD Wakil FTSM Wakil FKAB Ketua PTM PPUKM

PERANAN KETUA PEGAWAI MAKLUMAT (CIO)

Bagi menentukan pembangunan dan penggunaan ICT yang lebih terancang, semua agensi Kerajaan telah diminta melantik Ketua Pegawai Maklumat yang bertanggungjawab ke atas perancangan, pengurusan, penyelarasan dan pemantauan program ICT agensi masing-masing.

Buku Panduan CIO Sektor Awam telah menetapkan peranan terperinci CIO dan *expected outcome* dapat membantu CIO memahami peranan masing-masing dengan lebih jelas:

Peneraju Perubahan melalui Penjajaran Pelan Strategik ICT (ISP) Kementerian/Negeri/Agensi dengan Keperluan Pelan Pembangunan Nasional, Pelan Strategik Kementerian /Negeri/Agensi dan ISP Sektor Awam	
Peranan	<i>Expected Outcome</i>
i. Memastikan Pelan Strategik ICT (ISP) agensi yang selari dengan ISP Sektor Awam dan Pelan Strategik Agensi; ii. Memastikan <i>blueprint Enterprise Architecture</i> (EA) agensi tersedia; dan iii. Memantapkan struktur tadbir urus ICT agensi	i. Pengagihan sumber yang lebih cekap dan berkesan; ii. Projek-projek yang dirancang mengikut piawaian dan masa yang ditetapkan; iii. Penjajaran pelaksanaan program ICT yang lebih tersusun dan teratur; dan (iv) Peningkatan kadar kejayaan pelaksanaan projek-projek ICT agensi.

Melaksana dan Menyelaras Penggunaan Dasar, Standard dan Amalan Terbaik Global	
Peranan	<i>Expected Outcome</i>
Menyediakan dan memantau peraturan, dasar, amalan terbaik global dan standard ICT untuk memastikan pelaksanaan program/projek ICT berjaya sepenuhnya.	Peningkatan kadar kejayaan pelaksanaan projek-projek ICT Agensi.

Menyelaras Penggalakan Pembudayaan ICT (<i>ICT Acculturation</i>) dalam Sistem Penyampaian Perkhidmatan Sektor Awam	
Peranan	<i>Expected Outcome</i>
<ul style="list-style-type: none"> i. Memastikan kesesuaian teknologi dengan aplikasi yang dibangunkan; ii. Membangunkan set kemahiran keupayaan personel ICT agensi untuk inisiatif bisnes yang berasaskan ICT; dan iii. Memastikan peningkatan kualiti dan bilangan penyediaan perkhidmatan <i>online</i> dalam sistem penyampaian agensi. 	<ul style="list-style-type: none"> i. Peningkatan tahap perkhidmatan ICT agensi; ii. Peningkatan tahap kompetensi personel ICT dalam bidang pembangunan program ICT; dan iii. Mempertingkatkan keberkesanan kos dan <i>Return On Investment (ROI)</i> dalam pelaksanaan program ICT agensi.

Melaksana dan Menyelaras Inovasi Aplikasi Kerajaan Elektronik, Infrastruktur dan Keselamatan ICT	
Peranan	<i>Expected Outcome</i>
<ul style="list-style-type: none"> i. Menyelaras, memantau dan menggalakan <i>interoperability</i> dan integrasi antara sistem aplikasi dan pangkalan data; ii. Memastikan pengukuhan dan penyeragaman pengoperasian infrastruktur ICT. (Contohnya PKI); dan iii. Memastikan pelan keselamatan maklumat disediakan (Contohnya GCERT dan DRC) 	<ul style="list-style-type: none"> i. Penjimatan sumber dari segi kos, masa dan tenaga bagi pelaksanaan ICT melalui perkongsian aplikasi ICT agensi; ii. Peningkatan kadar penggunaan repositori aplikasi ICT agensi; iii. Peningkatan tahap <i>Return On Investment (ROI)</i> terhadap pelaksanaan program ICT; iv. Peningkatan tahap integrasi dan <i>interoperability</i> bagi aplikasi dan infrastruktur ICT agensi; v. Peningkatan tahap keselamatan dan kebolehpercayaan aplikasi ICT; dan vi. Peningkatan tahap keyakinan terhadap keselamatan perkhidmatan ICT

Senarai Tugas Pegawai Keselamatan ICT (ICTSO)

1. Menyediakan semua infrastruktur keselamatan ICT menepati prinsip-prinsip keselamatan berpandukan Rangka Dasar Keselamatan ICT dan Arahan Keselamatan yang disediakan oleh Ketua Pegawai Keselamatan Kerajaan;
2. Menyedia dan mengkaji semula dokumen infrastruktur keselamatan ICT bagi tujuan audit keselamatan ICT;
3. Mengenal pasti bidang-bidang keselamatan ICT yang perlu diberi perhatian rapi dan mengambil tindakan segera mengatasinya;
4. Memastikan tahap keselamatan ICT adalah terjamin setiap masa;
5. Menentukan semua pegawai dan staf jabatan memahami keperluan standard, garis panduan, prosedur dan langkah keselamatan di bawah Dasar Keselamatan ICT Kerajaan;
6. Menentukan semua pegawai dan staf jabatan mematuhi, garis panduan, prosedur dan langkah keselamatan di bawah Dasar Keselamatan ICT Kerajaan;
7. Menjalankan penilaian risiko dan program keselamatan berpandukan kepada standard, garis panduan, prosedur dan langkah keselamatan ICT. Proses penilaian risiko ialah proses menganalisis dan menterjemah risiko;
8. Mengadakan Pelan Rancangan Pematuhan yang bertujuan untuk mengurus risiko yang timbul akibat daripada ketidakpatuhan kepada standard, garis panduan, prosedur dan langkah keselamatan ICT;
9. Melaporkan kepada Bahagian Keselamatan ICT, MAMPU, Jabatan Perdana Menteri sebarang insiden pelanggaran keselamatan seperti kejadian-kejadian berikut:
 - Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa, atau disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa
 - Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian

- Kata laluan atau mekanisma kawalan sistem akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan
 - Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar
 - Berlaku percubaan mencerooboh, penyelewengan dan insiden-insiden yang tidak diingini
10. Membantu dalam pembangunan khusus bagi standard atau garis panduan yang mematuhi keperluan Rangka Dasar Keselamatan ICT Kerajaan bagi semua aplikasi dalam jabatan;
11. Sentiasa berusaha meningkatkan pengetahuan supaya mengetahui ancaman-ancaman, teknologi dan kaedah-kaedah kawalan maklumat/asset ICT terkini melalui pembacaan, seminar, kursus dan latihan sambil bekerja;
12. Sentiasa bersedia dan menyebarkan amaran awal terhadap ancaman-ancaman yang boleh menyebabkan kerosakan besar kepada asset ICT, contohnya serangan virus terbaru; dan
13. Mengurus keseluruhan program-program keselamatan ICT dalam agensi.



Garis Panduan

Pembangunan Laman Web PTJ

Universiti Kebangsaan Malaysia

GARIS PANDUAN PEMBANGUNAN LAMAN WEB PTJ UKM

Isi kandungan

1.0 TUJUAN

2.0 SKOP

3.0 KONSEP

4.0 INFRASTRUKTUR DAN KANDUNGAN LAMAN WEB

- 4.1 Muka Utama Laman Web
- 4.2 Versi Bahasa
- 4.3 Menu
- 4.4 Enjin Carian
- 4.5 Pautan
- 4.6 Dokumen Web
- 4.7 Penafian

5.0 REKA BENTUK DAN SUSUN ATUR LAMAN WEB

- 5.1 Window Title
- 5.2 Logo UKM
- 5.3 Versi Bahasa
- 5.4 Menu
- 5.5 Enjin Carian
- 5.6 Teks/ Warna/ Imej/ Audio dan Video
- 5.7 Saiz Laman Web
- 5.8 Paparan
- 5.9 Browser

6.0 PAUTAN DAN CARIAN MAKLUMAT

7.0 OPERASI DAN PENYELENGARAAN LAMAN WEB

- 7.1 Kandungan
- 7.2 Pemantauan Laman Web

8.0 PELANTIKAN WEBMASTER

- 8.1 Terma Rujukan Webmaster

**GARIS PANDUAN
PEMBANGUNAN LAMAN WEB PTJ
UNIVERSITI KEBANGSAAN MALAYSIA**

1.0 TUJUAN

- i. Menjadi rujukan kepada webmaster PTJ untuk membangun dan menyelenggara laman web PTJ.
- ii. Menyelaras reka bentuk dan kandungan laman web PTJ bagi meningkatkan imej universiti.

2.0 SKOP

Melibatkan semua laman web rasmi PTJ.

3.0 KONSEP

- i. Laman web PTJ adalah mesra pengguna dan berorientasikan pelanggan. Penyediaan laman web PTJ perlu mengambil kira keperluan pelanggan seperti pelajar, kakitangan, penyelidikan, golongan korporat/ bisnes dan masyarakat umum.
- ii. PTJ juga boleh mengenal pasti pelanggan-pelanggan lain yang berkaitan dengan PTJ tersebut.
- iii. Kandungan dan susunatur hendaklah mengambil kira pelanggan yang dinyatakan di atas.

4.0 INFRASTRUKTUR DAN KANDUNGAN LAMAN WEB

Berikut merupakan kandungan minima yang perlu ada pada setiap laman web:

4.1 Muka Utama Laman Web

- i. Setiap muka utama laman web PTJ hendaklah mengandungi maklumat berikut:
 - a. Teks atau grafik yang mengandungi nama penuh PTJ berkenaan.
 - b. Maklumat perhubungan contohnya seperti alamat, nombor telefon, faks dan alamat e-mel.
- ii. Penggunaan *splash page* perlu dielakkan

4.2 Versi Bahasa

- i. Setiap laman web mesti mempunyai dua versi bahasa iaitu Bahasa Melayu dan Bahasa Inggeris. Pertambahan versi lain adalah digalakkan.
- ii. Halaman utama laman web PTJ hendaklah dalam versi Bahasa Melayu.

4.3 Menu

- i. Kandungan minimum bagi setiap menu yang perlu ada dalam setiap laman web PTJ adalah seperti berikut:-

a) **Utama / Home**

Muka laman utama web mesti mempunyai:-

- Ucapan selamat datang iaitu Selamat Datang ke Laman Rasmi 'Nama PTJ' (versi BM) dan *Welcome to 'PTJ Name' Official Website* (versi BI).
- Format yang boleh digunakan adalah bebas seperti:- *marquee text, plain text, grafik, animasi* dan lain-lain.
- Pengenalan mengenai PTJ samada dalam bentuk teks atau grafik.
- Berita atau peristiwa yang hendak di ketengahkan.

b) **Berita / Peristiwa**

Penghebahan berita dan pengumuman yang dianggap penting khususnya bagi faedah pelanggan PTJ masing-masing.

c) **Mengenai Kami / About Us**

Mengandungi penerangan mengenai PTJ.

d) **Organisasi / Organization**

Mengandungi carta organisasi PTJ.

e) **Staf / Staff**

Mengandungi direktori staf.

f) **Hubungi Kami / Contact Us**

Maklumat minimum PTJ yang perlu ada untuk dihubungi:

- Alamat
- Nombor Faks
- Nombor Telefon
- Alamat Faks
- Alamat E-mel

(Nombor telefon dan faks disertakan dengan kod negara dan kod kawasan)

g) Pautan / Links

Menyenaraikan pautan ke laman web UKM dan pautan lain yang berkaitan.

- Pautan dalam / *Internal Link*
Pautan bagi laman web di dalam UKM

- Pautan Luar / *External Link*
Pautan laman web dari agensi luar UKM

h) Peta Laman / Site Map

Memaparkan struktur laman web PTJ

- ii. Bagaimanapun setiap PTJ boleh menambah maklumat berkaitan dengan fungsi dan keperluan PTJ masing-masing.

4.4 Enjin Carian

- i. Tumpuan kepada keperluan pengguna yang disasarkan. Penekanan kepada perkataan yang digunakan oleh pengguna dalam mencari maklumat berikut:
 - Maklumat berkaitan PTJ seperti:
 - Kepakaran (PTJ berkaitan)
 - Telefon dan E-mel

 - Atau Google Search

4.5 Pautan

- i. Lebih banyak pautan laman web lain kepada muka paparan adalah lebih baik untuk penarafan enjin carian.

- ii. Pautan yang disediakan hendaklah terus kepada kandungan yang berkaitan di dalam laman web berkenaan.

4.6 Dokumen Web

- i. Laman web yang mempunyai petikan berita atau artikel yang berunsurkan hak cipta, keterangan mengenai hak cipta ini perlu disediakan seperti:-
 - Perkataan hak cipta
 - Tarikh disediakan
 - Nama pemiliknya

4.7 Penafian

- i. Penafian berikut perlu disertakan dalam laman web PTJ:

“Universiti Kebangsaan Malaysia dan *nama PTJ* tidak bertanggungjawab terhadap sebarang kehilangan atau kerugian yang dialami kerana menggunakan mana-mana maklumat yang diperoleh melalui laman web ini.”

5.0 REKA BENTUK DAN SUSUN ATUR LAMAN WEB

- i. Untuk memastikan reka bentuk yang mesra pengguna, menarik dan mudah dicapai, setiap PTJ hendaklah memberi perhatian kepada perkara berikut:
 - Masa muat turun yang pantas dan munasabah.
 - Penggunaan teknologi yang sesuai dan boleh dicapai oleh majoriti pengguna.
 - Mengadakan capaian alternatif dengan menyediakan maklumat dalam mod *text only*.
 - Reka letak sistem navigasi yang konsisten dan mudah diguna pada semua halaman

5.1 Window Title

- i. Setiap laman web perlu mempunyai *window title* iaitu (UKM : Nama Penuh PTJ)
Contoh: UKM : Pusat Teknologi Maklumat

5.2 Logo UKM

- i. Logo UKM hendaklah menggunakan logo asal tanpa sebarang perubahan.
Contohnya: diherot atau ditukar warna.
- ii. Animasi logo adalah dibenarkan tetapi tidak keterlaluan sehingga mengubah bentuk logo.
- iii. Kedudukan logo mesti berada di sebelah atas kiri setiap muka laman web.
- iv. Saiz minimum logo adalah:
Lebar – 150px dan nisbah 2:12 (lebar : tinggi)

5.3 Versi Bahasa

- i. Setiap laman web mesti mempunyai dua versi bahasa iaitu Bahasa Melayu dan Bahasa Inggeris. Pertambahan versi bahasa lain adalah digalakkan.

- ii. Halaman utama laman web PTJ hendaklah dalam versi Bahasa Melayu.

5.4 Menu

- i. Menu berikut hendaklah diletakkan di sebelah atas, manakala menu lain boleh diletakkan di mana-mana tempat yang bersesuaian mengikut kehendak PTJ.
 - Utama
 - Berita atau Peristiwa
 - Mengenai Kami
 - Organisasi
 - Staf
 - Hubungi Kami

5.5 Enjin Carian

- i. Enjin carian hendaklah berada di sebelah atas laman web.

5.6 Teks / Warna / Imej / Audio dan Video

i. Teks

- a. Pemilihan rupa taip dan fon yang diguna haruslah mengambil kira faktor berikut:
 - Diambil daripada koleksi umum.
 - Menggunakan rupa taip dan kategori Sans Serif (contohnya : *Arial*, *Tahoma* dan *Verdana*) bagi mudah di baca.
 - Tidak menggunakan terlalu banyak jenis rupa taip dalam satu laman web yang sama.
- b. Teks yang digunakan haruslah:
 - Mengguna warna kontras dengan warna latar belakang laman web.
 - Dipecahkan kepada beberapa perenggan sekiranya teks adalah panjang.
- c. Saiz minimum fon yang perlu digunakan:
 - 2 jika menggunakan arahan html () atau
 - 10px jika menggunakan CSS
- d. Penggunaan *alt* perlu bagi setiap imej yang dipaparkan

ii. Warna

- a. Ilustrasi yang berwarna hendaklah dikekalkan dalam warna asal.
- b. Warna latar belakang laman web hendaklah kontras dengan warna teks atau ilustrasi bagi mengelakkannya tenggelam atau tidak jelas.

iii. Imej

- a. Penggunaan animasi hendaklah berpatutan, tidak membebankan laman dan menyukarkan pencapaian laman berkenaan oleh pengguna.
- b. Kurangkan penggunaan grafik yang berat, animasi dan *java applet*
- c. Jika grafik seperti *Flash* digunakan, laman web perlu memberi pilihan kepada pengguna untuk akses (versi *Flash* atau HTML).

iv. Audio dan Video

- a. Penggunaan animasi hendaklah berpatutan, tidak membebankan laman dan menyukarkan pencapaian laman berkenaan.

5.7 Saiz Laman Web

- a. Lebar laman web yang digunakan hendaklah di sesuaikan dgn resolusi skrin 800x600 px.

5.8 Paparan

- i. Penggunaan bingkai (*frames*) tidak dibenarkan.
- ii. Penggunaan jaringan (*nested*) tidak dibenarkan.

5.9 Browser

- i. Semua laman web yang dibangunkan hendaklah menyokong paparan sekurang-kurangnya *Mozilla Firefox* dan *Internet Explorer*.

6.0 PAUTAN DAN CARIAN MAKLUMAT

- i. Setiap PTJ hendaklah memastikan pautan keluar dari laman web UKM adalah bersesuaian dengan kepentingan universiti. Pautan yang membawa kesan negatif kepada universiti hendaklah dielakkan contoh:
 - a. Laman web berunsur politik.
 - b. Laman web berunsur pengiklanan / perniagaan (kecuali yang diluluskan oleh UKM).
 - c. Laman web yang menyentuh sensitiviti individu, kepercayaan dan kaum.
- ii. Setiap laman web hendaklah menyediakan mekanisme carian maklumat bagi kemudahan pengguna.

7.0 OPERASI DAN PENYELENGGARAAN LAMAN WEB

7.1 Kandungan

- i. Kandungan hendaklah sentiasa dikemaskini.
- ii. Kandungan hendaklah dapat menarik minat pengguna.
- iii. Laman web digalakkan mempunyai peta laman (*site map*)
- iv. Tarikh kemaskini hendaklah dipaparkan pada laman web utama.

7.2 Pemantauan Laman Web

- i. PTJ hendaklah mempunyai mekanisme untuk memantau setiap pautan dan *button* dalam laman web masing-masing agar berfungsi dengan baik.
- ii. PTJ digalakkan menyediakan jadual terperinci bagi tujuan mengemaskini kandungan laman web seperti tarikh terima kandungan, penyedia kandungan (*content provider*) dan tarikh muat naik ke web sebagai rujukan.

8.0 PELANTIKAN WEBMASTER

Webmaster PTJ dilantik oleh Naib Canselor

8.1 Terma Rujukan Webmaster

- i. Membangun dan menyelenggara laman web di PTJ masing-masing. Laman web mestilah sekurang-kurangnya dalam dua versi (Bahasa Melayu dan Bahasa Inggeris).
- ii. Menyelaras dan memantau pembangunan web pada peringkat jabatan/unit sekiranya ada.
- iii. Memastikan supaya maklumat laman web PTJ masing-masing adalah terkini dan tepat.

- iv. Melaporkan sebarang perubahan maklumat kepada UNIKWeb untuk dikemaskini.
- v. Menjadi Ahli Jawatankuasa Laman Web UKM.
- vi. Membuat salinan (*backup*) laman web Fakulti dari semasa ke semasa.
- vii. Melaporkan perkembangan laman web fakulti kepada pengurusan PTJ masing-masing.
- viii. Menyalurkan maklumat terkini PTJ (penyelidikan, anugerah, perlantikan, aktiviti seperti MoU, MoA, Letter of Intent, Syarahan Umum atau perdana) kepada UNIKWeb beserta gambar.

**Disediakan oleh UNIKWeb PTM
25/11/2009**