DASAR TEKNOLOGI MAKLUMAT DAN KOMUNIKASI UNIVERSITI UTARA MALAYSIA (Versi 4.0)

UUMIT
08 November 2023

BAB **MUKA SURAT**

BAB 1

DASAR UMUM ICT

BAB 1: DASAR UMUM ICT

1.1 Tujuan

Menerangkan secara umum dasar pengurusan dan penggunaan sumber Teknologi Maklumat dan Komunikasi (ICT) di Universiti Utara Malaysia (UUM) dan diterima pakai sebagai Dasar Umum. Mana-mana dasar terperinci untuk setiap sumber yang disenaraikan dalam Dasar ICT UUM adalah tertakluk kepada Dasar Umum ini.

1.2 Tafsiran

Dalam Dasar ICT UUM, melainkan jika konteksnya menghendaki makna yang lain:

PENYATAAN	ERTINYA
Access Point (AP)	Peralatan yang membenarkan capaian tanpa wayar untuk berhubung dengan rangkaian.
Akaun Pengguna	Ruang storan yang diperuntukkan kepada setiap pengguna dalam sesuatu sistem atau sumber ICT. Setiap pengguna dikenal pasti melalui penggunaan identifikasi pengguna (ID).
Insiden Keselamatan ICT	Aktiviti, perbuatan atau apa-apa tindakan yang mengakibatkan perkhidmatan ICT terjejas atau tidak berfungsi sebagaimana dirujuk dalam Bab 3.
Jawatankuasa Keselamatan ICT (JKICT)	Jawatankuasa yang dinyatakan dalam perkara 2.3.2 Bab 2.
Jejak Audit (*Audit Trail)*	Kronologi rekod audit yang digunakan untuk mengenal pasti akauntabiliti pengguna sekiranya berlaku apa-apa gangguan atau masalah.

Kemudahan ICT	Merujuk kepada perkakasan, perisian, peralatan, rangkaian komunikasi, sokongan dan perkhidmatan yang berkaitan teknologi maklumat dan telekomunikasi yang disediakan oleh UUM bagi tujuan pengurusan, pentadbiran, penyelidikan dan pembangunan, pengajaran dan pembelajaran serta operasi pengguna.
Ketua Pegawai Digital ***Chief Digital Officer (CDO)***	Pegawai yang bertanggungjawab ke atas perancangan, pengurusan, penyelarasan dan pemantauan program ICT di UUM.
Maklumat Peribadi	Data atau maklumat tentang seseorang individu, termasuk tidak terhad kepada nama, tarikh lahir, no. kad pengenalan, no. staf dan sebagainya yang boleh digunakan untuk mengenali seseorang individu dan termasuk maklumat atau data peribadi sensitif.
Maklumat Rahsia atau Sulit	Segala bentuk data atau maklumat yang diklasifikasikan sebagai rahsia atau sulit oleh UUM dalam pelbagai format.
Makmal Komputer	Kemudahan ruang di mana perkhidmatan komputer dan capaian internet yang disediakan oleh UUM bagi menyokong aktiviti pentadbiran, pengajaran dan pembelajaran, penyelidikan dan pembangunan, dan perkhidmatan.
Makmal *Bring Your Own Device* (BYOD)	Kemudahan ruang di mana perkhidmatan capaian internet disediakan oleh UUM bagi menyokong aktiviti pentadbiran, pengajaran dan pembelajaran, penyelidikan dan pembangunan, dan perkhidmatan. Pengguna membawa peralatan sendiri untuk menggunakan kemudahan ruang dan capaian internet yang disediakan.
Pegawai Keselamatan ICT ***ICT Security Officer (*ICTSO**)***	Pegawai yang bertanggungjawab memastikan semua infrastruktur keselamatan ICT UUM menepati prinsip-prinsip keselamatan berpandukan Dasar Keselamatan ICT UUM, Dasar Kerja Keselamatan Siber dan Arahan Keselamatan Kerajaan.

Pelajar	Seseorang yang mendaftar sesuatu program akademik (sama ada sepenuh masa atau separuh masa) di UUM dan statusnya masih aktif (yang bukan berhenti, diberhentikan atau tamat pengajian).
Pemberi Maklumat	Pemberi maklumat merupakan pemilik sistem atau pemilik proses atau pemilik maklumat yang memberi maklumat kepada mana-mana pihak
Pemilik Sistem	Pusat Tanggungjawab (PTJ) yang menggerakkan pelaksanaan sesuatu sistem aplikasi dan menentukan apa-apa perubahan ke atas sistem aplikasi tersebut serta bertanggungjawab ke atas pewujudan, pengemaskinian dan kesahihan maklumat.
Pemilik Proses	PTJ yang menggunakan data dari pemilik sistem untuk kegunaan proses di PTJ tersebut.
Pemilik Maklumat	Individu yang boleh dikenal pasti melalui maklumat peribadi sedia ada di dalam Sistem Maklumat UUM.
Pengguna	Seseorang atau kumpulan orang yang dibenarkan menggunakan kemudahan ICT UUM.
Pentadbir Rangkaian	Pegawai yang bertanggungjawab mengurus, mengawal, memantau dan menyelenggara operasi dan keselamatan rangkaian.
Pengajaran dan Pembelajaran (PdP)	Proses pengajaran dan pembelajaran melibatkan guru dan pelajar semasa jadual waktu kuliah atau di luar jadual waktu kuliah.
Pengkomputeran Awan	Kemudahan perkhidmatan penempatan sistem atau *server* yang menggunakan teknologi awan (*cloud*) sama di dalam premis sendiri (*private cloud*) atau premis awam (*public cloud*).

Pentadbir Sistem	Pegawai yang bertanggungjawab mengurus, mengawal, memantau dan menyelenggara operasi dan keselamatan *server,* sistem aplikasi, laman web dan data yang disimpan.
Peralatan rangkaian	Peralatan dan komponen yang digunakan dalam sistem rangkaian seperti *switch, hub, router* dan sebagainya.
Perisian	Perisian merangkumi perisian aplikasi dan perisian sistem.
Perisian Aplikasi	Kod atur cara *(program code)* yang diperolehi; atau sistem aplikasi yang dibangunkan secara dalaman (contoh: sistem *client-server, web based* dan *mobile*). Contoh: *Microsoft Office*, Sistem Maklumat yang diperolehi atau dibangunkan oleh pihak luar, Sistem Maklumat yang dibangunkan oleh UUM.
Perisian Sistem	Kumpulan atur cara dan kemudahan *(utility)* yang membolehkan komputer berfungsi dan beroperasi. Contoh: Sistem Pengoperasian (Windows, Linux)
Perkakasan ICT	Peralatan dan komponen ICT. Contoh: Komputer, *notebook*, pencetak, pengimbas dan sebagainya.
Pusat Data UUM	Bilik *server* dan komponen berkaitan yang ditetapkan oleh UUMIT.
Pusat Tanggungjawab (PTJ)	Semua Kolej, Pusat Pengajian, Fakulti,Pusat, Akademi, Institut dan Jabatan di UUM.
Rangkaian Kampus	Infrastruktur rangkaian ICT UUM yang terdiri daripada rangkaian utama *(Core Network),* rangkaian kawasan setempat (LAN) dan rangkaian tanpa wayar (WiFi).

Server	Komputer yang mempunyai keupayaan tinggi dan memberi perkhidmatan berpusat.
Sistem Maklumat UUM	Sistem yang mengandungi semua aplikasi yang menyimpan maklumat UUM yang diperolehi atau dibangunkan sendiri secara dalaman berkaitan dengan fungsi utama UUM.
Staf	Seseorang yang dilantik oleh UUM untuk sesuatu jawatan sama ada secara tetap, sementara, kontrak atau sambilan dan masih berkhidmat.
Sumber ICT	Aset atau maklumat, peruntukan dan sumber manusia
Teknologi Maklumat dan Komunikasi ***Information and Communication Technology (ICT)***	Merangkumi produk, peralatan dan perkhidmatan yang digunakan untuk menyimpan, mencapai, dan memanipulasi apa-apa maklumat.
UUM	Universiti Utara Malaysia.
UUMIT	UUM Information Technology.
Virtual Classroom	Kemudahan persekitaran pengajaran dan pembelajaran dalam talian di mana pensyarah dan pelajar boleh berkomunikasi dan berinteraksi, membentangkan bahan kursus, melibatkan diri, menerangkan idea dan berbincang dengan ahli kelas maya yang lain secara langsung melalui sidang video atau audio serta bekerja dalam kumpulan bersama-sama.
***Virtual Desktop Infrastructure* (VDI)**	Kemudahan komputer menggunakan teknologi *virtual* di mana kemudahan komputer desktop dan sistem pengoperasian dihoskan di dalam *server* secara berpusat dan boleh dicapai oleh pengguna secara atas talian melalui rangkaian. Kemudahan boleh dicapai menggunakan komputer, *notebook*, komputer tablet, *mobile phone* atau peranti *thin client*.

Web Master	Pegawai yang bertanggungjawab mengurus, mengawal, memantau dan menyelenggara kandungan laman web dan data yang disimpan.

1.3 Objektif

Dasar ini bertujuan:

(i) Mewujudkan persekitaran ICT berkualiti tinggi dan selamat bagi melindungi dan menjamin keselamatan sumber ICT UUM serta menyokong semua urusan UUM meliputi skop pengajaran, pembelajaran, penyelidikan dan pembangunan, perkhidmatan, pengurusan dan pentadbiran;

(ii) Memastikan semua penggunaan sumber ICT digunakan secara bertanggungjawab dan beretika selaras dengan peraturan yang berkuatkuasa di UUM; dan

(iii) Memastikan kerosakan, kemusnahan dan penyalahgunaan ICT dapat diminimumkan.

1.4 Skop

1.4.1 Sumber

Semua sumber ICT yang disenaraikan dalam Dasar ICT dan apa-apa sumber lain yang ditetapkan oleh Jawatankuasa Pemandu Teknologi Maklumat & Komunikasi (JPICT) atau mana-mana pihak berwibawa yang berkenaan sebagai sumber ICT adalah tertakluk kepada dasar ini.

1.4.2 Pengguna

Semua pengguna adalah tertakluk kepada Dasar ICT UUM. Sesiapa mengakses dan menggunakan kemudahan ICT UUM tanpa kebenaran adalah dianggap sebagai penceroboh dan boleh diambil tindakan sebagaimana yang dinyatakan dalam Dasar ICT UUM.

1.5 Am

(i) UUM bertanggungjawab menyediakan kemudahan ICT untuk kegunaan staf akademik, staf pentadbiran, staf sokongan dan pelajar bagi melaksanakan tugas mereka.

(ii) Kemudahan dan perkhidmatan ICT yang disediakan oleh UUM adalah hak mutlak UUM. Pengguna diberi kebenaran untuk menggunakan kemudahan ICT berdasarkan keperluan tugas. UUM boleh membatalkan kebenaran dan menarik balik kemudahan yang diberikan dengan memberi notis terlebih dahulu.

(iii) Kemudahan ICT yang disediakan oleh UUM hanya boleh digunakan untuk tugas rasmi. Penggunaan selain daripada itu seperti untuk tujuan peribadi, komersial dan politik adalah tidak dibenarkan dan boleh dianggap melanggar Dasar ICT UUM.

(iv) Pengguna yang menggunakan kemudahan ICT UUM sama ada di dalam atau luar kampus UUM adalah tertakluk kepada dasar ini. UUM tidak bertanggungjawab terhadap apa-apa penyalahgunaan yang dilakukan oleh pengguna.

(v) Ketua PTJ bertanggungjawab memastikan pengguna di bawah kawalan dan pengawasannya mematuhi Dasar ICT UUM.

1.6 Pematuhan kepada Undang-undang

1.6.1 Pemakaian Peruntukan

Jika terdapat apa-apa peruntukan di dalam Dasar ICT ini yang diputuskan sebagai tidak sah atau salah di sisi undang-undang yang terpakai, peruntukan tersebut akan menjadi tidak terpakai sepenuhnya dan Dasar ICT ini akan ditafsirkan seolah-olah peruntukan tersebut tidak menjadi sebahagian daripada Dasar ICT UUM ini dan peruntukan yang selebihnya di dalam Dasar ICT UUM ini adalah kekal berkesan dan berkuat kuasa sepenuhnya.

1.6.2 Pematuhan kepada Undang-undang

UUM dan setiap pengguna hendaklah mematuhi semua undang-undang dan peraturan-peraturan mengenai penggunaanICT yang berkuat kuasa di Malaysia.

1.7 Pelanggaran Dasar

(i) UUM boleh melaksanakan tindakan ke atas mana-mana pengguna yang melanggar Dasar ICT seperti di dalam Bab 12.

(ii) Tindakan pencegahan awal termasuk sekatan atau

penggantungan secara sementara tidak melebihi 30 hari ke atas apa-apa unsur pelanggaran Dasar ICT boleh dilaksanakan oleh UUMIT bagi tujuan pencegahan atau bertujuan untuk meminimakan gangguan dan risiko yang boleh menjejaskan UUM atau kemudahan ICT yang disediakan.

(iii) Apa-apa aduan tentang pelanggaran Dasar ICT boleh dibuat kepada ICTSO, CDO atau sistem aduan rasmi yang disediakan oleh UUM. Jawatankuasa Keselamatan ICT boleh melantik Jawatankuasa Penyiasat untuk meneliti laporan dan menentukan sama ada siasatan terperinci perlu dilakukan.

(iv) Jawatankuasa Keselamatan ICT hendaklah mengadakan mesyuarat termasuk mesyuarat khas (jika perlu) bagi meneliti kes-kes pelanggaran Dasar ICT sebagaimana yang telah dilaporkan termasuk laporan berkaitan tindakan pencegahan awal yang diambil oleh UUMIT.

(v) Jawatankuasa Keselamatan ICT hendaklah meneliti setiap laporan yang berkaitan dengan pelanggaran dasar dan peraturan oleh pengguna serta memutuskan tindakan selanjutnya berdasarkan kepada jenis pelanggaran dan keadaan semasa pelanggaran.

(vi) Tindakan atau penalti maksima yang boleh diambil oleh Jawatankuasa Keselamatan ICT ke atas apa-apa kes pelanggaran dasar atau peraturan oleh pengguna adalah penggantungan penggunaan kemudahan ICT tidak melebihi satu (1) tahun.

(vii) Pengguna yang telah disabitkan kesalahan pelanggaran dasar atau peraturan boleh membuat rayuan ke atas tindakan atau penalti yang telah diputuskan oleh Jawatankuasa Keselamatan ICT. Rayuan secara bertulis boleh dikemukakan kepada Naib Canselor dalam tempoh **14** hari selepas keputusan tersebut dimaklumkan.

(viii) Naib Canselor boleh mengekalkan, mengubah atau mengakas keputusan yang telah ditetapkan oleh Jawatankuasa Keselamatan ICT. Keputusan Naib Canselor adalah muktamad.

(ix) Jawatankuasa Keselamatan ICT atau Naib Canselor boleh merujuk pengguna yang disabitkan melanggar Dasar ICT UUM, kepada Jawatankuasa Tatatertib Staf atau Pihak Berkuasa Tatatertib Pelajar mengikut mana-mana berkenaan, untuk tindakan selanjutnya.

1.8 Teknologi Maklumat Peringkat Kebangsaan

Dasar ini adalah tertakluk kepada:

(i) Akta Aktiviti Kerajaan Elektronik 2007 *[Akta 680];*

(ii) Akta Rahsia Rasmi 1972 (Akta 88)
(iii) Akta Tandatangan Digital1997 *[Akta 562];*
(iv) Akta Hakcipta 1987 *[Akta 332];*
(v) Akta Jenayah Komputer 1997 *[Akta 563];*
(vi) Akta Teleperubatan 1997 *[Akta 564];*
(vii) Akta Komunikasi dan Multimedia 1998 *[Akta 588];*
(viii) Akta Suruhanjaya Komunikasi dan Multimedia Malaysia 1998 *[Akta 589];*
(ix) Akta Perlindungan Data Peribadi 2010 *[Akta 709];*
(x) Akta Universiti dan Kolej Universiti 1971 *[Akta 30];*
(xi) Akta Badan-Badan Berkanun (Tatatertib dan Surcaj) 2000 *[Akta 605];*
(xii) Arahan Teknologi Maklumat;
(xiii) Surat Pekeliling Am Bilangan 3 Tahun 2015 - Garis Panduan Permohonan Kelulusan Teknikal Dan Pemantauan Projek Teknologi Maklumat Dan Komunikasi (ICT) Agensi Sektor Awam;
(xiv) Surat Pekeliling Perbendaharaan Bil. 3 Tahun 2013 - Garis Panduan Mengenai Pengurusan Perolehan Information Telecomunication Technology (ICT) Kerajaan;
(xv) Surat Pekeliling Am Bil. 3 Tahun 2009 Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam;
(xvi) Surat Pekeliling Am Tahun 2006 Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat (ICT) Sektor Awam;
(xvii) Garis Panduan Pengurusan Keselamatan ICT Sektor Awam Malaysia (MyMIS);
(xviii) Pekeliling Am Bil. 3 Tahun 2000: Rangka Dasar Keselamatan ICT Kerajaan;
(xix) Pekeliling Kemajuan Pentadbiran Awam Bil. 2 Tahun 2015 Pengurusan Laman Web Agensi Sektor Awam;
(xx) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2021 Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam;
(xxi) Rangka Tindakan (Blueprint) Ekonomi Digital Malaysia;
(xxii) Pelan Strategik Pendigitalan Sektor Awam (2021 – 2025); dan
(xxiii) Apa-apa pindaan terhadap akta, pekeliling dan garis panduan dari semasa ke semasa.

1.9 Pindaan

Dasar ini adalah tertakluk kepada perubahan dari semasa ke semasa. UUM berhak meminda, membatal, mengehad dan menambah mana-mana dasar mengikut kesesuaian dan keperluan semasa.

BAB 2

DASAR PENGURUSAN ICT

BAB 2: DASAR PENGURUSAN ICT

2.1 Tujuan

Menerangkan secara umum aspek pengurusan organisasi dan pembangunan ICT UUM.

2.2 Skop

(i) Pengurusan organisasi ICT yang mempunyai kuasa dan kepakaran untuk merancang, melaksana dan mengurus keperluan ICT di UUM menerusi strategi yang ditetapkan; dan

(ii) Pembangunan ICT bagi merancang, mengurus, melaksana dan menyelenggara keperluan ICT di UUM menerusi strategi yang ditetapkan.

2.3 Pengurusan Organisasi

2.3.1 Jawatankuasa Pemandu Teknologi Maklumat & Komunikasi (JPICT) UUM

(i) Keanggotaan:

(a) Naib Canselor yang hendaklah menjadi Pengerusi;
(b) Semua Timbalan Naib Canselor;
(c) Semua Penolong Naib Canselor;
(d) Pendaftar;
(e) Bendahari;
(f) Ketua Pustakawan;
(g) Penasihat Undang-Undang;
(h) Seorang ahli Senat yang dipilih oleh Senat;
(i) Tidak lebih daripada enam (6) ahli yang dilantik oleh Naib Canselor, seorang daripadanya hendaklah merupakan profesor dalam bidang ICT:
    1) Dekan Pusat Pengajian Pengkomputeran(SOC);
    2) Seorang profesor dalam bidang ICT ;
    3) Pengarah Pejabat Pengurusan Risiko;
    4) Pengarah JPP.
(j) Pengarah UUMIT yang bertindak sebagai Setiausaha.

(ii) Fungsi:

(a) menetapkan dasar teknologi maklumat UUM;

(b) memantau keberkesanan penggunaan teknologi maklumat;

(c) menilai pencapaian penggunaan serta perancangan pelaksanaan teknologi maklumat di UUM;

(d) memperaku dan meluluskan projek-projek berkaitan ICT tertakluk kepada prosedur perolehan; dan

(e) menubuhkan Jawatankuasa Kerja jika perlu;

(iii) JPICT hendaklah mengadakan mesyuarat sekurang-kurangnya sekali setahun;

2.3.2 Jawatankuasa Keselamatan ICT

(i) Keanggotaan:

(a) Timbalan Naib Canselor (Penyelidikan dan Inovasi) yang hendaklah menjadi Pengerusi;
(b) Pendaftar;
(c) Penasihat Undang-Undang;
(d) Pengarah Jabatan Keselamatan;
(e) Pengarah Jabatan Pembangunan dan Penyenggaraan;
(f) Pengarah Pejabat Pengurusan Risiko;
(g) Pengarah UUMIT; dan
(h) Timbalan Pengarah UUMIT, yang bertindak sebagai Setiausaha

(ii) Fungsi:

Jawatankuasa ini ditubuhkan untuk memantau penguatkuasaan Dasar ICT UUM, meneliti kes-kes pelanggaran Dasar ICT dan memutuskan tindakan selanjutnya;

(iii) Jawatankuasa ini hendaklah mengadakan mesyuarat mengikut keperluan pada tarikh, masa dan kaedah yang ditetapkan oleh Pengerusi dan mesyuarat hendaklah dipanggil oleh Setiausaha.

2.3.3 UUMIT

(i) UUMIT diketuai oleh seorang Pengarah dan bertanggungjawab dalam merancang, melaksana, mengurus, memantau, menyelenggara dan menjalankan operasi projek-projek ICT di UUM;

(ii) UUMIT hendaklah mempunyai staf teknikal yang mempunyai kepakaran ICT dan staf pentadbiran/ sokongan secukupnya;

(iii) Timbalan Naib Canselor (Penyelidikan dan Inovasi (TNC (P & I)) dilantik sebagai CDO;

(iv) Pengarah UUMIT sebagai ICTSO.

2.4 Pembangunan ICT

2.4.1 Perancangan ICT

(i) Perancangan hendaklah memenuhi fungsi dan keperluan UUM dalam pengajaran, pembelajaran, penyelidikan, perundingan, pentadbiran dan pengurusan; dan

(ii) Perancangan hendaklah selaras dengan agenda ICT Negara dan mematuhi Dasar, Peraturan dan Garis Panduan yang ditentukan oleh Kerajaan Malaysia.

2.4.2 Perolehan ICT

(i) UUMIT dan PTJ hendaklah memastikan perolehan mematuhi Prosedur Perolehan UUM dan Kerajaan kecuali bagi kes tertentu dengan mendapat perakuan/ kelulusan pihak berkuasa UUM;

(ii) UUMIT dan PTJ hendaklah memastikan semua perolehan memenuhi teknologi terkini yang bersesuaian dan mendapat perakuan spesifikasi oleh **Jawatankuasa Perolehan/Jawatankuasa Penilai Spesifikasi/Pegawai Teknikal UUMIT mengikut mana yang berkenaan**;

(iii) UUMIT dan PTJ hendaklah memastikan semua perisian berlesen mempunyai lesen yang sah.

2.4.3 Pemasangan dan Penyenggaraan

(i) Pemasangan perkakasan dan/atau perisian hendaklah dilakukan di bawah penyeliaan UUMIT; dan

(ii) PTJ hendaklah memastikan peralatan ICT diselenggara mengikut termpoh masa yang ditetapkan oleh UUMIT.

2.4.4 Naik taraf atau Pelupusan

(i) Semua naik taraf perkakasan dan perisian aplikasi (selain daripada yang dibangunkan secara dalaman) hendaklah mendapat kelulusan Jawatankuasa Penilai Spesifikasi/Teknikal UUMIT; dan

(ii) Perkakasan yang tidak berkeupayaan dan/atau tidak sesuai untuk dinaik taraf atau diperbaiki boleh dicadang untuk pelupusan mengikut Prosedur Pelupusan UUM.

2.4.5 Pembangunan Sumber Manusia

(i) Merancang keperluan sumber manusia yang secukupnya bagi menyokong perkhidmatan ICT di UUM;

(ii) Merancang dan melaksana pelan Pembangunan sumber manusia bagi meningkatkan pengetahuan dan kemahiran teknikal; dan

(iii) Merancang dan melaksana pelan pembangunan sumber manusia bagi meningkatkan pengetahuan dan kemahiran asas ICT serta penggunaan aplikasi ICT untuk pengguna.

BAB 3

DASAR KESELAMATAN ICT

BAB 3: DASAR KESELAMATAN ICT

3.1 Objektif

(i) Memastikan kelancaran operasi ICT UUM dan meminimumkan kerosakan atau kemusnahan sumber ICT;
(ii) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan
(iii) Mencegah salah guna atau kecurian sumber ICT UUM.

3.2 Skop

(i) Aspek keselamatan sumber ICT; dan
(ii) Aspek reka bentuk dan capaian sumber ICT.

3.3 Penyataan Dasar

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

(ii) Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan sumber ICT.

(iii) Terdapat empat (4) komponen asas keselamatan ICT iaitu:

(a) Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;

(b) Menjamin setiap maklumat adalah tepat dan sempurna;

(c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

(d) Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

(iv) Dasar Keselamatan ICT UUM merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

(a) Kerahsiaan - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;

(b) Integriti - Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;

(c) Tidak Boleh Disangkal - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;

(d) Kesahihan - Data dan maklumat hendaklah dijamin kesahihannya; dan

(e) Ketersediaan - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

3.4 Keselamatan Pusat Data

3.4.1 Pentadbir Pusat Data UUM

UUMIT adalah Pentadbir Pusat Data UUM dan bertanggungjawab ke atas keseluruhan operasi Pusat Data UUM yang terdiri daripada Pusat Data *(Data Centre)* dan PusatPemulihan Bencana *(Disaster Recovery Centre).*

3.4.2 Kawalan Keselamatan Fizikal

Bagi memastikan kawalan keselamatan fizikal ke atas Pusat Data UUM adalah pada tahap yang baik, Pentadbir Pusat Data UUM hendaklah memastikan Pusat Data UUM dilengkapi dengan ciri-ciri berikut:

(i) Peralatan utiliti sokongan elektrik seperti *Uninterruptible Power Supply (UPS)*, Set

peralatan utiliti sokongan elektrik seperti *Uninterruptible Power Supply (UPS)*, Set *Generator* dan sumber bekalan elektrik yang mencukupi bagi mengelakkan gangguan bekalan elektrik di Pusat Data;

(ii) Sistem pendingin hawa yang bersesuaian bagi menyokong proses penyejukan ke atas peralatan yang ditempatkan di Pusat Data dengan suhu yang bersesuaian dengan peralatan;

(iii) Sistem pencegah kebakaran bagi melindungi peralatan jika berlaku kebakaran;

(iv) Peralatan keselamatan bagi mengawal capaian secara *remote* ke atas peralatan;

(v) Melindungi pengkabelan dengan pemasangan konduit atau lain-lain mekanisma perlindungan yang bersesuaian;

(vi) Mekanisma kawalan akses ke atas staf dan pihak-pihak lain yang dibenarkan masuk ke Pusat Data;

(vii) Mekanisma kawalan kepada semua sumber ICT yang ditempatkan di Pusat Data termasuk *server*, storan dan suis rangkaian; dan

(viii) Mekanisma pemantauan secara fizikal ke atas Pusat Data bagi meminimakan risiko gangguan perkhidmatan.

3.4.3 Kawalan Terhadap Pangkalan Data

(i) Pentadbir Pangkalan Data bertanggungjawab mengawal capaian ke atas pangkalan data yang ditempatkan di Pusat Data UUM;

(ii) Integriti data yang disimpan di dalam pangkalan data dijamin melalui kawalan capaian data yang ditentukan oleh Pentadbir Pangkalan Data;

(iii) Pentadbir Pangkalan Data berhak untuk memasang peralatan keselamatan yang bersesuaian bagi tujuan memantau dan merekodkan apa-apa aktiviti pangkalan data; dan

(iv) Pentadbir Pangkalan Data adalah bertanggungjawab melaksanakan tugas-tugasrutin ke atas pangkalan data seperti:

(a) *Performance tuning* secara berkala;
(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);* dan
(f) Melaksanakan *back up* atau *restore*.

3.4.4 Kawalan Capaian Logikal

(i) Pentadbir Sistem adalah bertanggungjawab mengawal capaian ke atas sistem pengoperasian yang ditempatkan di Pusat Data UUM.

(ii) Pentadbir Sistem hendaklah melaksanakan kawalan dan penyenggaraan bagi memastikan integriti sistem pengoperasian daripada terdedah kepada apa-apa pencerobohan keselamatan. Maka penyenggaraaan yang perlu dilaksanakan ialah:

(a) semakan secara berkala hak capaian pengguna ke atas sistem pengoperasian;

(b) kemas kini *patches* (yang bersesuaian dan perlu sahaja) bagi mengatasi kelemahan sistem pengoperasian yang telah dikenal pasti oleh pembekal;

(c) menyemak dan mengimbas sistem pengoperasian secara berkala bagi mengenal pasti apa-apa kelemahan yang boleh disalahguna oleh pihak yang tidak bertanggungjawab; dan

(d) menaik taraf sistem pengoperasian (jika perlu) kepada versi terkini sesuai dengan spesifikasi peralatan ICT sedia ada.

(iii) Kawalan ke atas pengguna dibuat bagi memastikan hanya pengguna yang sah sahaja boleh mencapai sistem pengoperasian. Mekanisma kawalan capaian ke atas pengguna adalah seperti

dalam perkara 3.4.5 di bawah.

3.4.5 Identifikasi Pengguna

(i) Pengguna boleh terdiri daripada individu atau kumpulan pengguna yang berkongsi akaun kumpulan pengguna yang sama. Dalam kedua-dua keadaan, pengguna perlu bertanggungjawab ke atas keselamatan akaun yang digunakan. Langkah yang diambil untuk mengenal pasti pengguna yang sah ialah:

(a) memberi satu (1) ID yang unik kepada setiap pengguna individu;

(b) menyimpan dan menyelenggara semua ID pengguna yang bertanggungjawab untuk setiap aktiviti;

(c) memastikan adanya kemudahan pengauditan untuk menyemak semua aktiviti pengguna; dan

(d) memastikan semua ID pengguna yang diwujudkan adalah berdasarkan permohonan.

(ii) Bagi memastikan ID pengguna yang tidak aktif tidak disalahgunakan, Pentadbir Sistem boleh:

(a) menggantung semua kemudahan ID yang tidak digunakan dan menghapuskan ID berkenaan berdasarkan kepada tarikh surat arahan pertukaran atau tamat perkhidmatan; dan

(b) menghapus semua kemudahan untuk pengguna yang berpindah Jabatan utama perkhidmatan.

(iii) Audit *trail* untuk setiap aktiviti pengguna hendaklah disimpan dan diarkib terutamanya untuk pengguna yang boleh mencapai maklumat sulit agar dapat dikenal pasti sekiranya berlakunya pencerobohan maklumat.

(iv) Pengesahan Pengguna *(User Authentication)*

Proses ini bertujuan mengenal pasti hanya pengguna yang sah dibenarkan menggunakan sistem melalui penggunaan kata laluan. Sistem mestilah boleh menyediakan kemudahan bagi:

(a) kata laluan dimasukkan dalam bentuk yang tidak boleh dilihat;

(b) panjang kata laluan sekurang-kurangnya lapan (8) aksara;

(c) merupakan kombinasi daripada aksara dan angka atau simbol-simbol lain;

(d) enkripsi *(encryption)* kata laluan semasa penghantaran;

(e) cubaan capaian dihadkan.

3.4.6 Audit *Trail*

(i) UUM bertanggungjawab menyedia dan menyimpan rekod audit *trail* bagi mengenal pasti akauntabiliti pengguna dan keselamatan. Penggunaan audit *trail* untuk sistem pengoperasian perlu diwujudkan untuk:

(a) Capaian kepada maklumat yang kritikal;
(b) Capaian kepada perkhidmatan rangkaian; dan
(c) Keistimewaan atau kebenaran tertentu yang melebihi kebenaran sebagai pengguna biasa digunakan seperti arahan keselamatan dan fungsi Pentadbir Sistem.

(ii) Maklumat audit *trail* merangkumi

(a) identifikasi (ID) pengguna;

(b) fungsi, sumber dan maklumat yang digunakan atau dikemas kini;

(c) tarikh dan masa penggunaan;

(d) alamat IP pengguna atau stesen

kerja secara khusus; dan

(e) transaksi dan program yang dijalankan secara khusus.

(iii) UUM akan mengambil tindakan berikut semasa penyediaan audit *trail*:

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

(b) meneliti audit *trail* secara berjadual;

(c) meneliti dan melaporkan apa-apa masalah keselamatan dan kejadian luar biasa;

(d) menyimpan maklumat audit *trail* untuk jangka masa tertentu bagi keperluan operasi dan keselamatan; dan

(e) mengawal maklumat audit *trail* daripada dihapus, diubah suai, ditipu atau disusun semula.

3.4.7 Penyalinan dan Pemulihan Maklumat *(Backup/ Restore)*

(i) Proses *backup* perlu dilaksanakan secara berkala iaitu harian, mingguan dan bulanan.

(ii) Permohonan *backup* perlu dibuat oleh pengguna dan pihak pentadbir data memastikan data yang perlu di*backup*.

(iii) Data *backup* dibuat sekurang-kurangnya dalam tiga (3) generasi dan salinan data yang kritikal akan disalin ke Pusat Pemulihan Bencana.

(iv) Data yang di*backup* merangkumi sistem pengoperasian.

(v) Salinan *backup* dibuat untuk simpanan/*restore* dan juga untuk tujuan *disaster recovery*.

(vi) Ujian *restore* atau proses audit data dijalankan secara berkala menggunakan salinan data *backup*

bagi memastikan:

(a) data *backup* boleh dibaca dan digunakan;

(b) data yang di*backup* adalah data yang betul; dan

(c) pelan untuk pemulihan berfungsi dengan baik.

(vii) Menggunakan teknik *backup* secara *'full'* atau *'incremental'* di mana yang sesuai.

(viii) Prosedur *backup/restore* hanya dilaksanakan oleh pihak Pentadbir Sistem.

(ix) Memastikan keseluruhan sistem pengoperasian server termasuk data boleh dipulihkan menggunakan media *backup.*

(x) Memastikan media *backup* adalah yang terkini dan memenuhi piawaian di pasaran dan boleh dipulihkan menggunakan teknologi terkini.

(xi) Jangka hayat media *backup* perlu dipastikan apabila media berkenaan hendak digunakan semula *(recycle).*

(xii) Wujudkan prosedur bertulis yang diluluskan oleh pihak pengurusan mengenai langkah-langkah yang perlu diambil jika berlaku bencana dan kehilangan data.

(xiii) Prosedur *backup/restore* didokumenkan dan diuji.

3.4.8 Pusat Pemulihan Bencana *(Disaster Recovery Centre)*

(i) Hanya *server* yang menjalankan fungsi kritikal sahaja akan ditempatkan di Pusat Pemulihan Bencana.

.

(ii) Hanya data yang kritikal sahaja akan dibuat salinan dari Pusat Data ke Pusat Pemulihan Bencana.

(iii) Data-data kritikal ini merangkumi:

(a) Sistem Maklumat UUM seperti Portal, ASIS, PERSIS, GAIS, SECURIS, FIMS, SAMS, RAIIS, SISTEM KLINIK dan lain-lain

(b) Sistem Kedatangan Staf dan Pelajar;

(c) Sistem Emel;

(d) Sistem e-Learning; dan

(e) Laman web UUM dan laman web Pusat Pengajian.

3.4.9 Pengurusan

Pentadbir Pusat Data hendaklah bertanggungjawab:

(i) memastikan semua sumber ICT yang ditempatkan di Pusat Data UUM berada dalam keadaan selamat dan berisiko minima daripada apa-apa ancaman yang telah dikenal pasti.

(ii) Memastikan persekitaran dan ruang kerja di Pusat Data UUM adalah selamat dan berisiko minima dari apa-apa ancaman yang telah dikenal pasti.

(iii) Melaksanakan penilaian risiko keselamatan secara berkala ke atas Pusat Data UUM bagi mengenal pasti apa-apa risiko yang wujud serta mengambil tindakan yang bersesuaian bagi memastikan keselamatan Pusat Data UUM adalah berada pada tahap yang baik.

(iv) Mewujudkan prosedur bertulis yang diluluskan oleh pihak pengurusan mengenai langkah-langkah dalam melaksana dan menyenggara operasi Pusat Data.

(v) Proses penyalinan dari Pusat Data ke Pusat Pemulihan Bencana perlu dibuat secara berkala sama ada secara *'real- time'*, *'hourly'* atau *'daily'*.

(vi) Ujian Pemulihan Bencana haruslah dibuat secara berkala bagi memastikan Pusat Pemulihan

Bencana berada dalam tahap kesediaan yang tinggi jika berlaku bencana di Pusat Data.

(vii) Mewujudkan prosedur bertulis yang diluluskan oleh pihak pengurusan mengenai langkah-langkah yang perlu dibuat jika berlaku bencana.

(viii) Melaksanakan prosedur pemindahan ke Pusat Pemulihan Bencana dan pemindahan kembali ke Pusat Data didokumenkan dan diuji.

3.5 Keselamatan Aplikasi

UUMIT bertanggungjawab melaksana dan mengawal tahap capaian sistem aplikasi.

3.5.1 Perisian Aplikasi

Kawalan keselamatan perisian aplikasi dilaksanakan untuk mengelakkan berlakunya capaian yang tidak sah, pengubahsuaian, pendedahan atau penghapusan maklumat. UUMIT bertanggungjawab menyediakan kawalan dan kemudahan seperti berikut:

(i) kawalan capaian penggunaan satu (1) ID dan kata laluan untuk setiap perisian aplikasi;

(ii) memastikan semua ID pengguna yang diwujudkan adalah berdasarkan permohonan;

(iii) mengehadkan tahap capaian maklumat serta fungsi berdasarkan tanggungjwab pengguna;

(iv) memberhentikan semua kemudahan untuk pengguna yang tamat perkhidmatan berkuat kuasa pada tarikh beliau tamat perkhidmatan berdasarkan surat arahan yang dikeluarkan oleh Jabatan Pendaftar kecuali kemudahan e-mel untuk pengguna yang bersara;

(v) memberhentikan semua kemudahan untuk pengguna (pelajar) yang berhenti, dilarang daripada mana-mana bahagian atau bahagian-bahagian tertentu UUM bagi tempoh yang ditetapkan, digantung daripada menjadi seorang pelajar universiti bagi tempoh yang ditetapkan atau dipecat dari UUM berkuat kuasa pada tarikh status pelajar disahkan oleh Jabatan Hal Ehwal Akademik atau pusat pengajian;

(vi) memberhentikan semua kemudahan bagi pengguna yang tamat pengajian (bergraduat) berkuat kuasa selepas tempoh tertentu dari tarikh senat berdasarkan keperluan Jabatan Hal Ehwal Akademik atau pusat pengajian; dan

(vii) mengadakan sistem log bagi setiap transaksi maklumat kritikal yang menjejaskan pentadbiran, operasi dan sistem UUM untuk tujuan jejak audit yang menentukan akauntabiliti kepada semua pengguna.

3.5.2 Pangkalan Data

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

(i) sistem keselamatan berpusat dengan kawalan capaian penggunaan ID dan kata laluan untuk setiap aplikasi; dan

(ii) kawalan capaian kepada maklumat ditentukan oleh Pentadbir Pangkalan Data.

3.5.3 Pengujian Aplikasi

UUM bertanggungjawab menguji atur cara, modul, sistem aplikasi dan integrasi sistem aplikasi bagi memastikan sistem berfungsi mengikut spesifikasi yang ditetapkan. Langkah berikut perlu diambil semasa pengujian aplikasi dijalankan:

(i) menggunakan data ujian *(dummy)* atau data lapuk *(historical);*

(ii) mengawal penggunaan data terpilih *(classified);*

(iii) mengehadkan capaian kepada staf yang terlibat sahaja;

(iv) mengadakan kaedah pemberitahuan *(flagsystem)* sekiranya capaian dan pengemaskinian maklumat dilakukan.

(v) menghapuskan maklumat yang digunakan setelah selesai pengujian (terutamanya apabila menggunakan data lapuk); dan

(vi) menggunakan persekitaran yang berasingan untuk pembangunan dan pengoperasian sistem aplikasi.

3.5.4 Perisian Berkod Jahat *(Malicious)*

Atur cara sistem aplikasi terdedah kepada kod jahat. UUM bertanggungjawab mengurangkan kemungkinan perisian yang mempunyai kod jahat melalui kawalan berikut:

(i) kod sumber *(source code)* daripada pembangun sistem aplikasi yang bereputasi dan rekod prestasi perkhidmatan yang baik serta mempunyai kepakaran teknikal yang tinggi;

(ii) mewujud dan melaksanakan program jaminan kualiti dan prosedur untuk semua sistem aplikasi yang dibangunkan secara dalaman dan luaran; dan

(iii) memastikan semua sistem aplikasi didokumenkan, diuji, disahkan fungsinya, tahan lasak (*robustness)* dan menepati spesifikasi.

3.5.5 Perubahan Versi

UUM bertanggungjawab mengawal versi sistem aplikasi apabila perubahan atau peningkatan dibuat.

3.5.6 Penyimpanan Kod Sumber *(Source Code)*

UUM bertanggungjawab mengurus dan melaksanakan kawalan penyimpanan kod sumber bagi sistem aplikasi yang dibangunkan secara dalaman atau luaran untuk tujuan penyenggaraan dan peningkatan yang merangkumi:

(i) mewujudkan prosedur penyenggaraan versi terkini;

(ii) mendokumenkan prosedur *backup* kod sumber bagi penyenggaraan versi terkini; dan

(iii) menyimpan *backup* kod sumber sekurang-

kurangnya di dua (2) lokasi yang berasingan.

3.5.7 Perisian Tidak Berlesen

(i) UUM bertanggungjawab memastikan semua perisian berlesen yang digunakan dikawal penyimpanannya dari segi lokasi serta pengedarannya. Pengguna tidak dibenarkan mengguna perisian yang tidak berlesen.

(ii) UUM tidak akan bertanggungjawab ke atas penggunaan perisian tidak berlesen (*freeware/ open source*).

3.5.8 Kawalan Kod Jahat *(Malicious Code)*

UUM 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 supaya 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 fail kepilan *(attachment)* daripada e-mel yang meragukan.

3.6 Keselamatan Peralatan Rangkaian

3.6.1 Keselamatan Pemasangan

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

3.6.2 Keselamatan Fizikal

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

(ii) Suhu hendaklah terkawal di dalam had suhu peralatan rangkaian berkenaan dengan memasang sistem pendingin hawa sepanjang masa;

(iii) Memasang *Uninterruptible Power Supply* (UPS) dengan minimum 15 minit masa beroperasi jika terputus bekalan elektrik dan perlindungan daripada kilat dan menyokong penutupan *(shut down)* server secara automatik; dan

(iv) Memasang *Generator Set* yang bersesuaian untuk memastikan peralatan berfungsi apabila berlaku gangguan bekalan elektrik.

3.6.3 Capaian Fizikal

(i) Kabel Rangkaian

Langkah yang perlu diambil untuk melindungi kabel rangkaian daripada dicapai oleh pihak yang tidak berkenaan:

(a) Melindungi kabel di kawasan awam dengan memasang *conduit* atau mekanisma perlindungan lain; dan

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

3.6.4 Capaian Peralatan Rangkaian

(i) Peralatan hendaklah ditempatkan di dalam rak di lokasi yang selamat dan terkawal;

(ii) Peralatan rangkaian hanya boleh dicapai oleh staf yang dibenarkan sahaja; dan

(iii) Menyelenggara inventori peralatan dan membuat semakan secara berkala.

3.6.5 Capaian Logikal

(i) ID dan kata laluan diperlukan untuk mencapai perisian rangkaian. Capaian hanya boleh dibuat oleh staf yang dibenarkan sahaja;

(ii) Komposisi kata laluan mestilah konsisten dengan garis panduan yang telah ditetapkan;

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

(iv) Semua perubahan konfigurasi peralatan rangkaian hendaklah direkodkan (pegawai yang membuat perubahan, pegawai yang membenarkan perubahan dibuat, perubahan yang dibuat, tarikh dan masa) dan dikendalikan secara berpusat.

3.6.6 Konfigurasi Peralatan

(i) Mengaktifkan *(enable)* perkhidmatan yang diperlukan sahaja;

(ii) Mengehadkan capaian konfigurasi kepada nod atau alamat IP yang dibenarkan sahaja;

(iii) Tidak mengaktifkan *(disable)* penyiaran trafik *(broadcast);*

(iv) Menggunakan kata laluan yang selamat; dan

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

3.6.7 Penyenggaraan Peralatan

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

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

(iii) Mengemas kini rekod penyenggaraan.

3.6.8 Kebolehcapaian Pengguna *(User Accessibility)*

(i) Hanya pengguna dibenarkan membuat penyambungan ke rangkaian UUM (rujuk Dasar Pengurusan dan Perkhidmatan Rangkaian – Bab 5);

(ii) UUM berhak mewajibkan pengguna mendaftar setiap peranti (*device*) yang hendak disambung ke rangkaian melalui sistem yang disediakan;

(iii) UUM berhak mengehadkan bilangan peranti pengguna yang boleh disambungkan ke rangkaian UUM pada satu-satu masa;

(iv) Penggunaan perisian pengintip *(sniffer)* atau penganalisis rangkaian *(networkanalyzer)* tidak dibenarkan kecuali untuk tujuan rasmi dan setelah mendapat kelulusan daripada UUMIT secara bertulis melalui Ketua PTJ. Permohonan hendaklah menyatakan tujuan penggunaan, senarai pengguna dan perisian yang digunakan.

3.6.9 Sambungan dengan Rangkaian-rangkaian Lain

(i) Capaian yang Tidak Dibenarkan

(a) Penggunaan protokol rangkaian selain daripada prosedur atau protokol yang digunakan sebagai komunikasi data dalam rangkaian (TCP/IP) ;

(b) Penggunaan *workgroup* kerana menyokong *share-level security;*

(c) Capaian secara *remote* dari luar UUM kecuali dengan kebenaran bertulis

daripada UUMIT.

(ii) Firewall

(a) Semua trafik rangkaian dari dalam ke luar UUM dan sebaliknya mestilah melalui *firewall* dan hanya trafik yang disahkan sahaja dibenarkan untuk melepasinya. (Rujuk Dasar Rangkaian UUM – Bab 5).

(b) Reka bentuk *firewall* hendaklah mengambil kira perkara berikut:

i. keperluan audit dan arkib;

ii. kebolehsediaan;

iii. kerahsiaan; dan

iv. melindungi maklumat UUM.

3.7 Keselamatan Laman Web

UUM bertanggungjawab melindungi keselamatan laman web yang diluluskan oleh UUM dari aspek kerahsiaan, integriti dan kebolehsediaan. Ini melibatkan perlindungan maklumat dan aplikasi laman web kepada capaian yang sah, proses kemas kini yang dibenarkan serta langkah-langkah bagi membolehkan laman web menyediakan perkhidmatan secara berterusan kepada pengguna.

3.7.1 Pembezaan Kategori Maklumat Umum dan Maklumat yang Dilindungi

Pihak pentadbir laman web hendaklah mengambil kira kategori maklumat yang akan dipaparkan pada sesuatu laman web. Terdapat dua (2) kategori maklumat iaitu:

(i) Maklumat umum adalah maklumat am yang boleh dicapai oleh semua pengguna tanpa sekatan.

(ii) Maklumat yang dilindungi adalah maklumat yang perlu diberi perlindungan sepanjang proses pewujudan, pengemaskinian, penyimpanan, pencapaian dan penyebaran seperti maklumat peribadi dan maklumat rahsia atau sulit, maklumat terperingkat UUM serta maklumat yang menyentuh privasi.

3.7.2 Kebolehsediaan Laman Web

(i) Pentadbir laman web hendaklah memastikan laman web/maklumat boleh dicapai bila-bila masa.

(ii) Antara proses-proses yang boleh dilaksanakan bagi memastikan kebolehsediaan dan kebolehcapaian yang berterusan adalah seperti berikut:

(a) Backup/Restore

Pentadbir laman web hendaklah memastikan salinan *backup* dibuat ke atas aplikasi dan maklumat berkaitan laman web. Maklumat lanjut berkaitan *backup/restore* adalah seperti di perenggan 3.4.7 – Penyalinan dan Pemulihan Maklumat *(backup/restore)*.

(b) Penduaan ke atas aplikasi dan maklumat berkaitan laman web hendaklah dilakukan bagi mengekalkan kesediaan maklumat serta menjamin kesinambungan perkhidmatan walaupun berlakunya gangguan atau kerosakan pada mana-mana peralatan atau sistem.

3.7.3 Kawalan Keselamatan

(i) Kawalan Keselamatan Secara Pentadbiran

(a) Pentadbir laman web hendaklah memastikan setiap dasar berkaitan dengan laman web yang sedang berkuat kuasa dipatuhi dan dilaksanakan;

(b) Pentadbir laman web perlu memastikan dasar penggunaan laman web yang sedang berkuat kuasa boleh dicapai oleh pengguna.

(ii) Kawalan Keselamatan Secara Logikal/Teknikal

(a) Pentadbir laman web hendaklah memastikan keselamatan rangkaian, *server* dan laman web dengan memasang dan menggunakan perkakasan atau perisian keselamatan berasaskan teknologi seperti (tetapi tidak terhad kepada) Antivirus, *Firewall*, *Unified Threat Management (UTM)* dan *Web Application Firewall* (WAF);

(b) Pentadbir laman web hendaklah memastikan server web yang digunakan bagi tugas-tugas membangun, mengemas kini, menyenggara dan menguji laman web hendaklah diasingkan dari server web yang digunakan sebagai *production server;*

(c) Pentadbir laman web hendaklah memastikan sistem pengoperasian, *tools* dan aplikasi yang digunakan untuk membangun, mengemas kini dan menguruskan laman web mempunyai ciri-ciri keselamatan yang terkini dan selamat;

(d) *Patching* hendaklah dilakukan bagi menutup atau menghapuskan semua perkhidmatan yang tidak diperlukan dan *security patches* terkini akan dimasukkan ke dalam server web;

(e) Pentadbir laman web hendaklah memastikan laman web yang ditempatkan di UUMIT menjalani proses imbasan keselamatan sebelum capaian kepada umum dibenarkan bagi mengesan *vulnerabilities* seperti (tetapi tidak terhad kepada) SQL *Injection dan Cross Side Scripting* (XSS).

(iii) Kawalan Keselamatan Secara Fizikal

Seperti di perenggan 3.4.2 – Kawalan Keselamatan Fizikal

3.7.4 Audit Keselamatan

(i) UUMIT berhak untuk membuat audit keselamatan terhadap laman web yang ditempatkan di UUM dari semasa ke semasa; dan

(ii) UUMIT berhak untuk menyekat capaian ke laman web yang didapati mempunyai *vulnerabilities* dan terdedah kepada ancaman keselamatan sehingga tindakan penambahbaikan diambil.

3.7.5 Web *Hosting*

(i) Laman web yang ditempatkan di PTJ mestilah mengambil kira faktor-faktor keselamatan seperti di perenggan 3.7.2 – Kebolehsediaan Laman Web dan perenggan 3.7.3 – Kawalan Keselamatan.

(ii) PTJ yang mahu menggunakan perkhidmatan web *hosting* yang disediakan oleh pihak ketiga mestilah:

(a) mematuhi faktor-faktor keselamatan seperti di perenggan:
3.7.2 – Kebolehsediaan Laman Web;
3.7.3 – Kawalan Keselamatan; dan

(b) mendapat kebenaran daripada UUMIT.

3.8 Keselamatan Penggunaan E-mel

3.8.1 Tanggungjawab Pengguna

(i) Bertanggungjawab terhadap kandungan dan penyenggaraan kotak mel pada komputer peribadi;

(ii) Sentiasa mengimbas fail dalam kotak mel dengan perisian *antivirus* bagi memastikan fail yang dihantar/diterima melalui lampiran *(attachment)* bebas daripada virus; dan

(iii) E-mel hendaklah tidak mengandungi kandungan yang boleh merosakkan akaun, stesen kerja, server komputer dan rangkaian.

3.9 Keselamatan Penggunaan Komputer untuk Pengajaran di Dewan Kuliah, Bilik Kuliah dan Makmal Komputer

(i) Hanya staf yang dibenarkan sahaja yang boleh memasang apa-apa perisian pada komputer di dewan kuliah, bilik kuliah atau makmal komputer;

(ii) Pemasangan sejenis perisian *keylogger* yang boleh merekod apa-apa aktiviti pengguna komputer adalah dilarang sama sekali; dan

(iii) Pengguna digalakkan menghapuskan semua fail berkaitan selepas menggunakan komputer di dewan kuliah, bilik kuliah atau makmal komputer.

3.10 Pengurusan Insiden Keselamatan ICT

(i) Pengguna hendaklah melaporkan insiden keselamatan ICT kepada UUM *Computer & Emergency Response Team* (*UUMCERT*) 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 UUM 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 menceroboh, menyeleweng dan insiden yang tidak diingini.

(ii) ICTSO perlu menentukan tahap keutamaan insiden, melaporkan insiden kepada Agensi Keselamatan Siber Negara (NACSA) jika perlu dan mengambil langkah pemulihan awal.

(iii) Keanggotaan UUMCERT hendaklah terdiri daripada pegawai-pegawai yang dinamakan oleh ICTSO.

BAB 4

DASAR PERISIAN DAN PERKAKASAN ICT

BAB 4: DASAR PERISIAN DAN PERKAKASAN ICT

4.1 Tujuan

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

4.2 Skop

(i) Semua perisian yang diperolehi atau dibangunkan oleh UUM yang digunakan atau berada dalam simpanan pengguna; dan

(ii) Semua perkakasan hak milik UUM yang digunakan atau berada dalam simpanan pengguna.

4.3 Perisian

4.3.1 Perisian Aplikasi

(1) Perisian Aplikasi yang dibuat perolehan

(i) Maklumat keperluan spesifikasi Perisian Aplikasi ditentukan oleh Pemilik Sistem sebelum perolehan dilakukan

(ii) Semua perolehan perisian hendaklah mengikut Prosedur Perolehan UUM dan spesifikasi perisian diluluskan oleh Jawatankuasa Perolehan UUMIT.

(iii) Semua perolehan perisian untuk kegunaan UUM digalakkan menggunakan versi terkini dan mestilah menggunakan perisian yang telah dilengkapkan dengan lesen yang sah.

(iv) Penggunaan perisian adalah tertakluk kepada terma dan syarat penggunaan yang ditetapkan oleh pihak UUM, pembekal atau pembangun.

(v) UUM tidak akan bertanggungjawab terhadap apa-apa perolehan dan penggunaan perisian tanpa lesen oleh pengguna.

(vi) Permohonan untuk perolehan perisian hendaklah dibuat kepada Pengarah UUMIT melalui Ketua PTJ.

(vii) Kelulusan untuk perolehan adalah tertakluk kepada peruntukan kewangan tahunan yang telah diluluskan oleh UUM.

(viii) Bagi perolehan perisian yang tiada peruntukan, PTJ hendaklah membuat permohonan ke mesyuarat Jawatankuasa Pengurusan atau JPICT UUM setelah mendapat perakuan UUMIT.

(ix) Ketua PTJ bertanggungjawab memastikan perisian yang dimohon benar-benar diperlukan.

(x) Pensyarah tidak dibenarkan memohon perolehan perisian untuk kegunaan pelajar pasca-siswazah di bawah seliaannya.

(2) Perisian yang dibangunkan secara dalaman

(A) Permohonan Perisian Aplikasi

(i) Setiap permohonan untuk pembangunan aplikasi baharu atau perubahan terhadap aplikasi sedia ada hendaklah dimajukan secara rasmi kepada UUMIT.

(ii) UUMIT akan menyemak kesesuaian permohonan berdasarkan sumber (perisian aplikasi sedia ada, tenaga kerja dan peruntukan) dan menetapkan keutamaan permohonan untuk dilaksanakan.

(B) Pembangunan Perisian Aplikasi

Semua cadangan untuk membangunkan perisian aplikasi secara dalaman hendaklah dirujuk kepada UUMIT bagi memastikan semua cadangan adalah selaras dengan Pelan Strategik Maklumat UUM dan bagi mengelakkan pertindihan pembangunan perisian aplikasi. Pembangunan perisian aplikasi secara dalaman sama ada pembangunan perisian aplikasi baharu atau perubahan ke atas perisian aplikasi sedia ada dilakukan oleh Pembangun Sistem berdasarkan kitar hayat pembangunan sistem aplikasi yang merangkumi:

(i) Kajian kesauran sistem maklumat;

(ii) Kajian keperluan sistem dan integrasi dengan lain-lain perisian sistem aplikasi;

(iii) Penyediaan reka bentuk sistem;

(iv) Pengaturcaraan sistem;

(v) Pengujian sistem; dan

(vi) Latihan dan penyerahan kepada Pemilik Sistem Aplikasi

(C) Penyediaan Maklumat Perisian Aplikasi

Maklumat keperluan pembangunan diperolehi daripada Pemilik Sistem selaras dengan perenggan 8.3.

(D) Pengurusan Sistem Aplikasi

Pemilik Sistem bertanggungjawab mengurus sistem aplikasi selaras dengan perenggan 8.3.

(E) Integrasi Perisian Aplikasi

Setiap permohonan integrasi perlu mendapatkan kebenaran daripada Pemilik Sistem terlebih dahulu sebelum proses integrasi dilaksanakan.

(F) Kualiti Data dan Maklumat Perisian Aplikasi

Pemilik Sistem bertanggungjawab ke atas kesahihan data dan maklumat selaras dengan perenggan 8.3.

(G) Penamatan Perisian Aplikasi

Pemilik Sistem adalah bertanggungjawab untuk memaklumkan penamatan perisian aplikasi secara rasmi kepada UUMIT. Perisian Aplikasi yang tidak lagi digunakan akan diambil tindakan seperti berikut:

i) Ditutup capaian kepada pengguna;
ii) Penyenggaraan sistem ditamatkan; dan
iii) Kemudahan server dan rangkaian ditutup.

4.3.2 Perisian Sistem

UUM bertanggungjawab menyediakan perisian sistem untuk membolehkan komputer berfungsi dan beroperasi. Contohnya Windows, LINUX, macOS dan perisian antivirus.

4.3.3 Hak Milik

(i) UUM adalah Pemilik Sistem bagi semua perisian yang diperolehi atau yang

dibangunkan oleh warga UUM dan pihak-pihak lain untuk tujuan pengajaran, pembelajaran, penyelidikan atau pentadbiran menggunakan sumber ICT UUM.

(ii) Bagi perisian aplikasi yang dibangunkan, maklumat mengenai semua pengarang atau pencipta asal mestilah dikekalkan.

(iii) Semua perisian hak milik UUM tidak boleh dijual, disewa, dilesenkan semula, dipinjam, disalin semula, disebar atau diberi kepada sesiapa atau entiti tanpa kebenaran pengurusan UUM.

(iv) Semua perisian aplikasi yang dikomersilkan perlu dibayar royalti kepada PTJ yang membangunkannya.

(v) Semua perisian aplikasi yang diguna pakai oleh mana-mana pihak boleh dikenakan bayaran dengan kadar tertentu dan dibayar mengikut Dasar Pengkomersilan Harta Intelek UUM.

4.3.4 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 UUM misalnya perisian P2P *(peer to peer).*

(iii) Pengguna tidak dibenarkan menyebar apa-apa perisian secara tidak sah.

(iv) Apa-apa 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.

(vii) Pengguna perlu log keluar *(logout)* setelah tamat atau selesai menggunakan perisian aplikasi.

(viii) Pengguna bertanggungjawab ke atas keselamatan data perisian aplikasi yang digunakannya

4.3.5 Tanggungjawab pihak-pihak lain

(i) Pihak-pihak lain bertanggungjawab untuk membaca, memahami dan mematuhi peraturan dan syarat pelesenan bagi setiap perisian yang digunakan.

(ii) Pihak-pihak lain yang bertanggungjawab menyedia, mengurus, membekal, menyelenggara perkhidmatan di UUM perlu mendapat kelulusan UUM.

(iii) Bagi tujuan perenggan ini, pihak-pihak lain termasuklah anak syarikat UUM, pembekal, penyewa fasiliti, perunding, individu yang dilantik oleh UUM.

4.4 Perkakasan ICT

4.4.1 Hak Milik

(i) Semua perkakasan ICT yang diperolehi untuk atau bagi pihak UUM atau yang dicipta atau dipasang menggunakan peruntukan UUM oleh staf atau pelajar UUM adalah menjadi hak milik UUM.

(ii) Bagi perkakasan ICT yang dicipta, maklumat mengenai semua pencipta asal mestilah dikekalkan.

(iii) Perkakasan ICT tersebut tidak dibenarkan dijual, disewa, dipaten, dipinjam, diderma, dipajak atau diberi kepada sesiapa atau entiti tanpa kebenaran pengurusan UUM.

4.4.2 Perolehan Perkakasan ICT

(i) Semua perolehan perkakasan ICT hendaklah mengikut dasar perolehan di Bab 2 perenggan 2.4.2 Perolehan ICT.

(ii) Setiap spesifikasi perkakasan ICT hendaklah dirujuk kepada UUMIT bagi memastikan proses penyenggaraan dapat dilaksanakan dengan lancar.

(iii) Spesifikasi perkakasan ICT hendaklah diperakukan oleh Jawatankuasa Perolehan UUMIT bagi memastikan piawaian dan keseragaman dari segi teknologi dan keperluan semasa.

(iv) PTJ hendaklah memastikan perkakasan ICT yang dibeli mempunyai tempoh jaminan minimum satu (1) tahun daripada pembekal utama (*manufacturer warranty*)

(v) Komputer yang digunakan hendaklah disemak secara berkala bagi memastikan komputer dapat berfungsi secara optimum.

4.4.3 Tanggungjawab Pengguna

(i) Pengguna bertanggungjawab untuk mematuhi peraturan bagi setiap perkakasan yang digunakan.

(ii) Pengguna bertanggungjawab di atas apa-apa kerosakan atau kehilangan peralatan yang disebabkan kecuaian pengguna.

(iii) Pengguna hendaklah menghantar peralatan komputer yang masih dalam jaminan kepada pembekal untuk dibaiki.

(iv) Pengguna tidak dibenarkan meminjam, menukar, mengambil atau memindahkan komponen atau peralatan tanpa kelulusan daripada Ketua PTJ masing-masing.

(v) Ketua PTJ bertanggungjawab terhadap pengemaskinian rekod-rekod aset/inventori perkakasan yang berkenaan.

(vi) Apa-apa bentuk penyalahgunaan perkakasan adalah tidak dibenarkan dan tindakan boleh diambil terhadap pengguna.

4.4.4 Pengagihan Perkakasan ICT

(i) Semua pengagihan perkakasan ICT hendaklah mendapat kelulusan Ketua PTJ.

(ii) Pengagihan perkakasan ICT daripada sumber lain tertakluk kepada kelulusan Ketua PTJ.

(iii) Semua staf layak diberi perkakasan ICT berdasarkan keperluan kerja yang ditentukan oleh Ketua PTJ setelah dinilai keperluannya oleh PTJ.

(iv) Staf yang tamat perkhidmatan (bersara, meletak jawatan, diberhentikan, tamat kontrak atau dibuang kerja), bercuti sabatikal atau melanjutkan pengajian, perlu memaklum dan memulangkan perkakasan ICT di bawah tanggungjawabnya kepada PTJ selaras dengan pekeliling perkhidmatan dan peraturan kewangan yang ditetapkan.

4.4.5 Baik pulih komputer

(i) UUM hanya bertanggungjawab membaik pulih/mengganti perkakasan komputer yang di bawah hak milik UUM sahaja.

(ii) Baik pulih dan selenggaraan komputer tertakluk kepada peraturan kewangan mengenai tatacara pengurusan aset UUM.

(iii) UUM tidak bertanggungjawab ke atas keselamatan data yang ditempatkan di dalam perkakasan komputer yang dibaik pulih.

4.4.6 Penggantian Komputer

Komputer yang memenuhi salah satu ciri berikut layak diganti, tertakluk kepada peruntukan kewangan dan kelulusan pihak UUM:

(i) berusia lima (5) tahun atau lebih;

(ii) rosak dan tiada alat ganti; atau

(iii) tidak ekonomik untuk dibaik pulih.

4.4.7 Pelupusan Komputer

(i) Apa-apa peralatan komputer yang hendak dilupuskan hendaklah dimaklumkan kepada UUMIT serta mematuhi dasar pelupusan di perenggan 2.4.4 Naik taraf atau Pelupusan, Bab 2.

(ii) PTJ bertanggungjawab sepenuhnya ke atas urusan pelupusan sebelum proses pemeriksaan teknikal peralatan dilakukan oleh pegawai yang dilantik oleh Jabatan Bendahari.

BAB 5

DASAR PENGURUSAN DAN PERKHIDMATAN RANGKAIAN

BAB 5: DASAR PENGURUSAN DAN PERKHIDMATAN RANGKAIAN

5.1 Tujuan

Menentukan penyediaan, penggunaan, penyenggaraan dan pengoperasian bagi perkhidmatan Rangkaian Kampus UUM.

5.2 Skop

(i) Sumber rangkaian merangkumi peralatan rangkaian, termasuk tetapi tidak terhad kepada peralatan rangkaian seperti *hubs, switches, routers* dan *wireless access points;*

(ii) Perisian Aplikasi rangkaian merangkumi perisian sama ada dibeli atau dimuat turun daripada Internet seperti sistem pemantauan rangkaian, network analyzer dan lain-lain;

(iii) Konfigurasi rangkaian adalah reka bentuk alamat IP serta protokol rangkaian yang digunakan merangkumi teknologi Gigabit, protokol TC/IP dan lain-lain;

(iv) Penyambungan rangkaian adalah termasuk Rangkaian Setempat (LAN) sama ada melalui rangkaian berwayar atau tanpa wayar dan Rangkaian Luas (WAN).

5.3 Pentadbir Rangkaian

UUMIT adalah Pentadbir Rangkaian yang bertanggungjawab mengawal selia penggunaan, penyediaan, penyenggaraan dan pengoperasian bagi perkhidmatan Rangkaian Kampus UUM dan penyambungan kepada semua sumber rangkaian yang dihubungkan.

5.4 Hak Milik

Semua sumber rangkaian yang diperolehi oleh setiap PTJ adalah menjadi hak milik UUM.

5.5 Perolehan

(i) Semua perolehan sumber rangkaian hendaklah mengikut Prosedur Perolehan UUM.

(ii) Perolehan peralatan rangkaian termasuk tetapi tidak terhad kepada *router, switch, network cable, wireless access point* oleh PTJ adalah tidak dibenarkan kecuali dengan kelulusan UUMIT.

(iii) Perolehan tambahan termasuk tetapi tidak terhad kepada punca data dan *wireless access point* untuk kegunaan PTJ hendaklah menggunakan peruntukan PTJ berkenaan.

(iv) Pentadbir Rangkaian tidak akan bertanggungjawab ke atas apa-apa masalah yang timbul berkaitan perolehan yang dibuat oleh PTJ tanpa melalui UUMIT.

5.6 Kemudahan Rangkaian Kampus

(i) Pengguna tidak dibenarkan dalam apa cara sekali pun mengganggu pengguna lain di dalam rangkaian kampus dan Internet. Gangguan ini termasuk tetapi tidak terhad kepada menghantar *spam* secara e-mel, mesej atas talian *(online)*, DOS *(Denial of Service)* dan lain-lain;

(ii) Pengguna tidak boleh memberikan sumber rangkaian di bawah jagaannya untuk kegunaan orang lain walaupun pelajar atau staf UUM tanpa mendapat kelulusan UUMIT.

(iii) Pengguna bertanggungjawab sepenuhnya terhadap semua aktiviti yang menggunakan Rangkaian Kampus termasuk akses ke Internet dan rangkaian yang lain.

(iv) UUMIT boleh menyekat capaian mana-mana peranti yang menjadi sumber ancaman atau penyebaran virus ke Rangkaian Kampus sehingga peranti tersebut disahkan bebas dari ancaman virus/malware dan lain-lain.

(v) Setiap ubah suai bangunan atau pembinaan bangunan perlu memasukkan keperluan infrastruktur rangkaian dan kos yang ditentukan bersama oleh pengguna, UUMIT dan Jabatan Pembangunan dan Penyenggaraan.

5.7 Penyambungan Rangkaian

(i) Perolehan peralatan rangkaian dan penyambungan ke Rangkaian Kampus perlu mendapat kelulusan UUMIT. Konfigurasi penyambungan yang dibuat oleh pembekal hendaklah dilaksanakan di bawah seliaan UUMIT.

(ii) Sebarang sambungan ke Rangkaian Kampus yang tidak mendapat kebenaran UUMIT adalah menyalahi peraturan dan UUMIT berhak memutuskan penyambungan tersebut.

(iii) PTJ tidak boleh membenarkan pihak luar memasang apa-apa kabel atau peralatan rangkaian di dalam kampus kecuali dengan kebenaran UUMIT.

5.8 Pemberian Alamat IP

(i) Pemberian alamat IP adalah tertakluk kepada syarat-syarat yang ditetapkan oleh UUMIT dari semasa ke semasa.

(ii) Syarat-syarat pemberian alamat IP adalah seperti berikut:

(a) Hanya *server* rasmi yang perlu dicapai dari luar UUM boleh mempunyai alamat IP global.
(b) Hanya *server* dan peranti rasmi untuk kegunaan dalaman UUM akan diberi alamat IP dalaman.
(c) Sebarang pemberian alamat IP global perlu mendapat kebenaran daripada UUMIT.

(iii) Sistem pemberian alamat IP bagi perkakasan ICT adalah menggunakan teknologi *DHCP (Dynamic Host Configuration Proctocol).* Alamat IP Statik diberikan untuk *server,* peralatan rangkaian dan perkakasan yang dikongsi seperti alamat pencetak.

BAB 6

DASAR PENGURUSAN DAN PENGGUNAAN KEMUDAHAN PDP

BAB 6: DASAR PENGURUSAN DAN PENGGUNAAN KEMUDAHAN PDP

6.1 Tujuan

Menerangkan tatacara pengurusan dan penggunaan kemudahan PdP di UUM dan sebagai garis panduan umum untuk pentadbir kemudahan PdP di PTJ.

6.2 Skop

Semua kemudahan PdP adalah hak milik UUM tanpa mengira pihak yang menguruskannya. Kemudahan PdP terdiri daripada persekitaran fizikal dan *virtual* untuk memastikan pelaksanaan PdP di UUM berjalan dengan lancar.

Kemudahan - kemudahan PdP termasuk tetapi tidak terhad kepada kemudahan seperti berikut:

i) Dewan Kuliah;
ii) Makmal Komputer;
iii) Student Lounge;
iv) Smart Classroom;
v) Virtual Classroom;
vi) Virtual Lab; dan
vii) Lain-lain teknologi berkaitan.

6.3 Penggunaan Kemudahan PdP

i) Penggunaan Dewan Kuliah adalah berdasarkan jadual PdP yang disediakan oleh HEA;

ii) Penggunaan Student Lounge diuruskan oleh PTJ yang bertanggungjawab;

iii) Penggunaan Smart Classroom diuruskan oleh PTJ yang bertanggungjawab;

iv) Penggunaan Virtual Classroom akan ditentukan oleh tatacara platform yang dibangunkan;

v) Penggunaan Virtual Lab akan ditentukan oleh tatacara platform yang dibangunkan

6.4 Penggunaan Makmal Komputer

(i) Penggunaan makmal komputer adalah tertakluk kelulusan UUMIT dan pihak yang menguruskan makmal.

(ii) UUMIT hanya bertanggungjawab menyediakan peralatan komputer dan perisian tetapi tidak termasuk projektor, pencetak dan alat tulis.

(iii) Pihak yang menguruskan makmal hendaklah memaklum dan menguatkuasakan peraturan penggunaan makmal komputer kepada pengguna.

(iv) Peraturan makmal yang digubal hendaklah melarang pengguna melakukan perkara berikut:

(a) memuat naik atau memuat turun bahan-bahan yang mengandungi unsur lucah, menghina, menghasut dan memfitnah;
(b) melayari laman sesawang yang mengandungi unsur lucah, menghina, menghasut dan memfitnah;
(c) mengganggu pengguna lain dengan apa cara sekalipun, termasuk menimbulkan rasa aib, marah dan tidak selesa;
(d) menukar kedudukan komputer dan peranti;
(e) menukar konfigurasi komputer;
(f) menambah atau membuang apa-apa perisian;
(g) menyimpan atau memuat turun maklumat atau data ke dalam cakera keras komputer;
(h) membawa keluar tanpa kebenaran apa-apa peralatan dari makmal.

(v) Perisian yang disediakan di makmal adalah perisian yang dibeli oleh UUMIT. Perisian selain dari yang disediakan oleh UUMIT hendaklah diuruskan oleh pihak yang membuat tempahan (perisian yang sah sahaja dibenarkan);

(vi) Pengguna hendaklah mendapat kebenaran pentadbir makmal komputer untuk memasang perisian lain ke dalam komputer;

(vii) Apa-apa peralatan yang dibawa keluar atau masuk ke makmal hendaklah mendapat kebenaran UUMIT;

(viii) Pengguna perlu membawa *laptop* sendiri untuk penggunaan di makmal BYOD;

(ix) Pengguna juga boleh menggunakan kemudahan VDI di makmal komputer yang menyediakan kemudahan tersebut.

6.5 Tempahan Makmal

(i) Tempahan makmal oleh PTJ dalam UUM hendaklah dibuat sekurang-kurangnya tiga (3) hari bekerja sebelum tarikh penggunaan makmal. Untuk penggunaan secara khusus termasuk tetapi tidak terhad kepada sistem peperiksaan dalam talian, tempahan makmal hendaklah dibuat sekurang-kurangnya lima (5) hari bekerja sebelum tarikh penggunaan makmal.

(ii) Tempahan makmal oleh organisasi luar UUM hendaklah dibuat sekurang-kurangnya dua (2) minggu sebelum tarikh penggunaan makmal.

(iii) Tempahan makmal yang mengandungi maklumat berikut hendaklah dibuat secara bertulis kepada pengurus makmal.

(a) Tarikh;
(b) Masa;
(c) Tujuan;
(d) Bilangan pengguna; dan
(e) Perisian yang hendak digunakan.

(iv) Bayaran tuntutan elaun lebih masa kepada petugas makmal yang dikehendaki bertugas pada hari cuti atau di luar waktu pejabat hendaklah ditanggung oleh pihak yang membuat tempahan.

(v) Pihak yang membuat tempahan bertanggungjawab untuk memastikan perisian yang dimohon menepati keperluan pengguna.

(vi) Pembatalan tempahan hendaklah dilakukan sekurang-kurangnya 24 jam sebelum penggunaan makmal melalui e-mel kepada pihak yang mengurus makmal.

(vii) Rekod tempahan makmal melalui e-mel atau surat hendaklah disimpan oleh pihak yang mengurus makmal.

(viii) Pihak yang mengurus makmal berhak menukar lokasi makmal mengikut kesesuaian tempahan.

(ix) Pihak yang mengurus makmal berhak menolak tempahan yang tidak memenuhi Dasar Pengurusan dan Penggunaan kemudahan PdP.

BAB 7

DASAR PENGGUNAAN KEMUDAHAN DAN PERKHIDMATAN INTERNET

BAB 7: DASAR PENGGUNAAN KEMUDAHAN DAN PERKHIDMATAN INTERNET

7.1 Tujuan

Menentukan tatacara penggunaan dan peraturan perkhidmatan Internet bagi memastikan penggunaan kemudahan adalah selaras dengan peraturan yang berkuatkuasa dari semasa ke semasa.

7.2 Skop

Penggunaan Internet termasuk tetapi tidak terhad kepada capaian sistem aplikasi/portal UUM, e-mel, laman web, pemindahan data atau maklumat dan perbincangan melalui *list group,* aplikasi *video conference, chat room* atau media sosial.

7.3 Penggunaan e-mel

7.3.1 Penyediaan Akaun E-mel

(i) Kemudahan e-mel ini diberikan secara automatik apabila mendaftar sebagai staf UUM seperti berikut:

(a) Kumpulan Pengurusan Tertinggi;
(b) Kumpulan Pengurusan dan Profesional; dan
(c) Kumpulan Sokongan.

(ii) Walau bagaimanapun, untuk staf sambilan, kemudahan ini diberikan berdasarkan permohonan daripada staf melalui pengesahan Ketua PTJ.

(iii) Setiap PTJ akan diberikan akaun e-mel khusus untuk kegunaan PTJ. Apa-apa penghantaran e-mel oleh PTJ ke UUMNET perlu mendapat kelulusan Ketua PTJ terlibat.

(iv) Semua pengguna diberikan kemudahan ruang storan seperti berikut:

Kategori	Saiz (GigaBytes)
Naib Canselor	10
Timbalan Naib Canselor	9
Ahli JPU	8
Dekan, Ketua PTJ, Profesor, Profesor Madya, Penjawat Utama, Pegawai Gred 54	7

Pensyarah, Pegawai Gred 48 - 52	6
Pegawai Gred 41 – 44, Penolong Pegawai dan Setiausaha Pejabat Gred 27 – 40	5
Staf Sokongan Gred 17 – 26	3
Staf Sokongan Gred 1 – 16	1
Lain-lain	1

7.3.2 Syarat-syarat Penggunaan (Am)

(i) Aktiviti *spamming* atau *mail-bombing* dan penyebaran e-mel dengan kandungan tidak beretika (seperti lucah, ugutan, perkauman, hasutan dan gangguan) kepada individu, *mailing list* atau *discussion group* sama ada di dalam rangkaian atau ke Internet adalah tidak dibenarkan.

(ii) UUM berhak memasang apa-apa jenis perisian atau perkakasan penapisan e-mel dan virus (e-mel *filter* and antivirus) yang difikirkan sesuai. Ianya digunakan untuk mencegah, menapis, menyekat atau menghapuskan mana-mana e-mel yang disyaki mengandungi virus, berunsur *spamming* atau kandungan yang tidak beretika daripada memasuki/keluar server, stesen kerja atau Rangkaian Kampus.

(iii) UUM tidak bertanggungjawab terhadap pengguna yang menjadi penghantar *(sender)* atau penerima *(receiver)* kepada apa-apa e-mel yang berunsur *spamming* atau penyebaran e-mel dengan kandungan tidak beretika.

(iv) UUM tidak bertanggungjawab terhadap apa-apa kerosakan, kehilangan atau apa-apa kesan lain kepada maklumat, aplikasi, kotak e-mel atau fail yang disimpan oleh pengguna di dalam stesen kerja atau server akibat daripada penggunaan perkhidmatan Rangkaian Kampus.

(v) Pengguna disarankan menukar kata laluan secara berkala. Penggunaan kata laluan yang sukar diramal oleh penggodam adalah digalakkan
(Rujuk Dasar Keselamatan ICT perenggan 3.4.4 Kawalan Capaian Logikal).

7.3.3 Syarat-syarat Penggunaan (Khusus)

(i) Pengguna individu tidak dibenarkan memohon dan/atau memiliki lebih daripada satu (1) akaun e-mel atau alamat e-mel UUM pada satu-satu masa pada server yang didaftarkan.

(ii) Pengguna hendaklah menggunakan akaun e-mel yang disediakan oleh UUM untuk semua urusan rasmi di UUM. UUM berhak untuk tidak melayan apa-apa komunikasi yang menggunakan e-mel luar.

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

(iv) Pengguna dilarang menggunakan kemudahan e-mel untuk apa-apa aktiviti yang tidak dibenarkan oleh peraturan UUM dan undang-undang negara.

(v) Pengguna bertanggungjawab ke atas kotak e-mel *(mailbox)* masing-masing untuk memastikan ruang storan mencukupi dan melakukan *backup* kandungan e-mel secara berkala.

(vi) Bagi kes kerosakan e-mel, Pentadbir Sistem hanya bertanggungjawab untuk memulihkan kembali *(restore)* maklumat akaun pengguna dan bukannya kandungan/ kotak e-mel *(mailbox)* pengguna.

(vii) Pentadbir Sistem berhak memeriksa dan melihat isi kandungan e-mel dan ruang storan pengguna dari semasa ke semasa atas keperluan audit dan keselamatan.

(viii) Pentadbir Sistem boleh membuang fail yang mempunyai extension seperti .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, .Ink, .wab, .dbx, .eml dan .zip dan fail yang mempunyai kapasiti melebihi 8 *megabytes* (MB) yang dijumpai dalam tapak yang dihoskan tanpa memberi apa-apa notis.

(ix) Pentadbir Sistem boleh membuang e-mel yang terdapat di dalam folder *Deleted Items* melebihi 30 hari, tanpa memberi apa-apa notis.

7.3.4 Tindakan Penguatkuasaan dan Pematuhan

(i) UUM berhak untuk menyekat atau menggantung kemudahan akaun e-mel yang telah diberikan kepada pengguna atas sebab berikut:

(a) Terdapat aktiviti *spamming* atau *mail-bombing* dan penyebaran e-mel dengan kandungan tidak beretika (seperti lucah, ugutan, perkauman, hasutan dan gangguan) kepada individu, *mailing list* atau *discussion group* sama ada di dalam rangkaian atau ke Internet.

(b) Penggunaan kemudahan e-mel untuk apa-apa aktiviti yang tidak dibenarkan oleh peraturan UUM dan undang-undang negara.

(c) Penyebaran e-mel yang mengandungi virus**.**

7.3.5 Penamatan Akaun e-Mel

(i) UUM boleh menamatkan kemudahan akaun e-mel yang telah diberikan kepada pengguna atas sebab berikut:

(a) Staf telah tamat perkhidmatan (tidak termasuk staf yang bersara);

(b) Pelajar yang telah tamat pengajian; dan

(c) Persatuan yang telah dibubarkan secara rasmi.

7.4 Penggunaan Kemudahan Aplikasi Sidang Video

7.4.1 Garis Panduan Pengurusan Keselamatan Penggunaan Persidangan Video (Video Conferencing) dalam UUM bertujuan sebagai panduan kepada PTJ mengenai pengurusan keselamatan perlindungan berhubung perkara rasmi dan rahsia rasmi PTJ dalam penggunaan persidangan video (video conferencing).

7.4.2 Persidangan video menjadi alternatif kepada pegawai UUM dan PTJ ke arah merealisasikan Kerajaan Digital bagi meningkatkan sistem penyampaian perkhidmatan. Sistem penyampaian ini boleh dilaksanakan menerusi pelbagai medium dan saluran komunikasi seperti penggunaan aplikasi dalam talian sama ada menggunakan aplikasi dalaman atau komersial.

7.4.3 Peraturan penggunaan kemudahan hendaklah selaras dengan Surat Pekeliling Am Bil 3 Tahun 2022 Garis Panduan Pengurusan Keselamatan Penggunaan Persidangan Video yang berkuatkuasa dari semasa ke semasa.

7.5 Capaian Internet

7.4.1 Capaian Laman Web/Media Sosial

(i) UUM berhak menyediakan dan memasang perisian aplikasi penapisan kandungan Internet/Intranet yang dilayari.

(ii) Laman yang boleh dilayari, dilanggan dan diguna adalah berbentuk akademik dan pengetahuan. Laman yang berbentuk keganasan, lucah, hasutan dan yang boleh menimbul atau membawa kepada keganasan, keruntuhan akhlak dan kebencian adalah tidak dibenarkan kecuali mendapat kebenaran bertulis terlebih dahulu daripada UUMIT setelah mendapat sokongan Ketua PTJ bagi tujuan akademik, penyelidikan atau pentadbiran.

(iii) Melayari Internet tanpa tujuan atau meninggalkan capaian Internet *unattended* adalah amat tidak beretika dan tidak digalakkan kerana ianya boleh menyebabkan kesesakan.

(iv) UUM berhak menapis, menghalang, mengehad dan menegah penggunaan mana-mana laman web yang dianggap tidak sesuai.

(v) UUM juga berhak menetapkan kadar penggunaan *bandwidth* Internet yang bersesuaian bagi setiap pengguna/aplikasi/laman web dengan tujuan untuk memastikan kelancaran prestasi penggunaan Internet.

(vi) Mana-mana pengguna yang telah menggunakan sepenuhnya kuota yang diberi masih boleh melayari hternet. Bagaimana pun UUM akan mengehadkan kelajuan prestasi capaian untuk pengguna terlibat.

(vii) UUM juga berhak mengenakan caj ke atas kuota tambahan yang dimohon oleh pengguna berdasarkan peraturan yang diluluskan oleh pihak berkuasa UUM.

(viii) UUM berhak menetapkan capaian laman web dan media sosial tertakluk kepada polisi yang ditetapkan oleh UUM.

7.4.2 Penyalahgunaan Laman Web/Media Sosial

(i) Pengguna dilarang mengganggu atau menceroboh laman web/media sosial mana-mana jabatan, organisasi di dalam/luar negara.

(ii) Pengguna dilarang memasuki, menyalin, menciplak, mencetak dan menyebarkan maklumat daripada Internet yang menyalahi undang-undang.

(iii) Pengguna tidak dibenarkan menggunakan sumber ICT UUM/persendirian untuk mendapatkan atau cuba mendapatkan capaian tidak sah *(unauthorised)* daripada mana-mana sistem komputer sama ada di dalam atau luar UUM. Ini termasuk membantu, mendorong, menyembunyikan percubaan untuk mencapai sistem komputer tersebut atau mencapai sumber ICT UUM dengan menggunakan identiti pengguna lain.

(iv) Pengguna tidak dibenar mencapai atau cuba mencapai sumber elektronik (data, paparan, *keystrokes*, fail atau media storan) dalam apa-apa bentuk yang dimiliki oleh pengguna lain tanpa mendapat kebenaran/kelulusan pengguna terbabit terlebih dahulu. Ini termasuk membaca, menyalin, menukar, merosak atau memadam data, program dan perisian.

(v) Penggunaan perisian seperti penganalisis rangkaian *(network analyzer)* atau pengintip *(sniffer)* adalah dilarang sama sekali kecuali untuk tujuan rasmi. Penggunaan untuk tujuan rasmi perlu mendapat kelulusan daripada Pengarah UUMIT secara bertulis melalui Ketua PTJ. Permohonan hendaklah menyatakan tujuan penggunaan, senarai pengguna dan perisian yang digunakan. Permohonan hendaklah dibuat sekurang-kurangnya tiga (3) hari bekerja dari tarikh diperlukan.

(vi) Penggunaan perisian capaian jarak jauh *(remote access)* atau *VPN (Virtual Private Network)* dilarang sama sekali kecuali untuk tujuan rasmi. Penggunaan untuk tujuan rasmi perlu mendapat kelulusan daripada Pengarah UUMIT secara bertulis melalui ketua PTJ. Permohonan hendaklah menyatakan tujuan penggunaan, tempoh penggunaan, senarai pengguna dan perisian yang digunakan. Permohonan hendaklah dibuat sekurang-kurangnya tiga (3) hari bekerja dari tarikh diperlukan.

BAB 8

DASAR AKAUNTABILITI DAN KERAHSIAAN MAKLUMAT

DASAR 8 DASAR AKAUNTABILITI DAN KERAHSIAAN MAKLUMAT

8.1 Tujuan

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

(i) Memelihara dan melindungi semua maklumat yang disimpan di dalam pangkalan data UUM dan *server* UUM termasuk dan tidak terhad kepada maklumat yang diklasifikasikan sebagai maklumat rahsia atau sulit.

(ii) Menyokong usaha UUM untuk menjaga kepentingan *stakeholder*.

(iii) Menerangkan aktiviti yang dilakukan oleh Jawatankuasa Keselamatan ICT/JPICT/Pentadbir Sistem atau pengguna yang melibatkan capaian data atau maklumat termasuk dan tidak terhad kepada maklumat yang diklasifikasikan sebagai maklumat rahsia atau sulit.

8.2 Skop

Meliputi tanggungjawab pengguna, Pentadbir Sistem, Pentadbir Rangkaian, Pemilik Sistem, Pemilik Proses, Pemilik Maklumat dan UUM berkaitan pemilikan data, kerahsiaan data dan capaian maklumat.

8.3 Pemilik Sistem

Kesemua data yang ditempatkan di dalam pangkalan data UUM atau yang ditempatkan di dalam *server* UUM adalah hak milik UUM. Kesemua data-data tersebut dikategorikan mengikut peranan dan tanggungjawab Pemilik Sistem.

8.3.1 Peranan dan Tanggungjawab Pemilik Sistem

(a) Menyedia dan mengemas kini data dan maklumat

(b) Memastikan ketepatan dan kesahihan data dan maklumat

(c) Mengawal capaian data dan maklumat

(d) Mengurus perubahan proses

8.3.2 Senarai Pemilik Sistem

Bil.	Sistem	Pemilik Sistem
a)	Maklumat Perancangan Strategik UUM	Bahagian Perancangan Korporat
b)	Maklumat Dokumen Berasaskan Elektronik	
i	Mesyuarat Jawatankuasa Pengurusan Universiti (JPU)	Jabatan Canselori

Bil.	Sistem	Pemilik Sistem
ii	Mesyuarat Lembaga Pengarah Universiti (LPU)	Jabatan Pendaftar
iii	Mesyuarat Senat	Jabatan Hal Ehwal Akademik
iv	Mesyuarat Majlis Kualiti	Institut Pengurusan Kualiti
v	Mesyuarat Jawatankuasa Pengurusan Akademik (JKPA)	Jabatan Hal Ehwal Akademik
vi	Sistem E-Post	Jabatan Pendaftar
vii	Sistem MoU/MoA	Unit Undang-Undang
c)	Maklumat Staf dan Perkhidmatan	Jabatan Pendaftar
d)	Maklumat Kewangan	Jabatan Bendahari (Rujuk Lampiran A Pengurusan Sistem Kewangan)
e)	Maklumat Penyelidikan dan Perundingan	Pusat Pengurusan Penyelidikan dan Inovasi (RIMC)
f)	Maklumat Penerbitan	Perpustakaan Sultanah Bahiyah (PSB)
g)	Maklumat Akademik	Jabatan Hal Ehwal Akademik
h)	Maklumat Pengajaran dan Pembelajaran	Pusat Pengajaran dan Pembelajaran Universiti (UTLC)
i)	Maklumat Penginapan, Kegiatan Pelajar serta Alumni	Jabatan Hal Ehwal Pelajar
j)	Maklumat Perpustakaan	Perpustakaan Sultanah Bahiyah (PSB)
k)	Maklumat Perubatan	Pusat Kesihatan Universiti
l)	Maklumat Keselamatan Kampus	Jabatan Keselamatan
m)	Maklumat Kandungan Laman Web UUM	*Web Master*/Unit Komunikasi Korporat (UKK) Rujuk Bab 10 Dasar Pembangunan Laman Web
n)	Maklumat Kandungan Laman Web Jabatan/Pusat Pengajian	Jabatan/Pusat Pengajian berkaitan Rujuk Bab 10 Dasar Pembangunan Laman Web

Senarai ini adalah tertakluk kepada perubahan dari semasa ke semasa.

8.3.3 Peranan dan Tanggungjawab Pemilik Proses

(a) Menggunakan data dan maklumat yang dibenarkan oleh pemilik sistem dengan mengambilkira perkara-perkara seperti berikut:

(i) Tujuan pengambilan maklumat;
(ii) Jenis maklumat yang diambil; dan
(iii) Tanggungjawab untuk memastikan maklumat dijaga atau disimpan dengan baik.

(b) Memastikan ketepatan dan kesahihan data dan maklumat yang diproses;

(c) Mengawal capaian data dan maklumat;

(d) Mengurus perubahan proses.

8.4 Capaian Maklumat Rahsia atau Sulit

8.4.1 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 l*ast, syslogd, acctcom, pacct* yang berfungsi merekod aktiviti pengguna untuk tujuan pengauditan.

(ii) Jika Pentadbir Sistem mengesyaki mana-mana pengguna melanggar Dasar ICT, Pentadbir Sistem boleh merekod apa-apa maklumat yang boleh digunakan sebagai bukti dan jika terbukti berlaku pelanggaran seperti menggunakan identiti pengguna lain untuk mencuri data atau merosakkan sumber ICT, dia hendaklah melaporkan kepada ICTSO untuk dipanjangkan kepada Jawatankuasa Keselamatan ICT jika difikirkan wajar untuk dikemukakan.

(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 CDO/ICTSO boleh mencapai maklumat atau data sulit atau rahsia pengguna seperti e-mel atau fail yang tersimpan dalam akaunnya

8.4.2 Capaian Maklumat Rahsia atau Sulit oleh Pentadbir Rangkaian

(i) Pentadbir Rangkaian mempunyai kuasa untuk memantau dan merekodkan data yang berada dalam rangkaian sebagai sebahagian daripada rutin keselamatan sumber ICT. Peralatan rangkaian seperti *switch, router* atau *server* yang menggunakan perisian tertentu mampu merekodkan data dalam rangkaian.

(ii) Jika Pentadbir Rangkaian mengesyaki mana-mana pengguna melanggar Dasar ICT, dia boleh merekod apa-apa maklumat yang boleh digunakan sebagai bukti dan jika terbukti berlaku pelanggaran seperti menggunakan identiti pengguna lain untuk mencuri data atau merosakkan sumber ICT, dia hendaklah melaporkan kepada ICTSO untuk dipanjangkan kepada Jawatankuasa Keselamatan ICT jika difikirkan wajar untuk dikemukakan.

(iii) Pentadbir Rangkaian boleh membuat salinan sama ada dalam bentuk bercetak atau digital kesemua atau sebahagian kandungan data komunikasi daripada peralatan yang digunakan oleh pengguna yang disyaki termasuk setiap *keystrokes* sebagai pemeliharaan bukti.

8.4.3 Am

(i) Pengguna ditegah menyimpan data atau maklumat sensitif, rahsia atau sulit di dalam komputer atau akaun pengguna tanpa kebenaran.

(ii) Mana-mana pengguna, Pentadbir Sistem dan Pentadbir Rangkaian yang mencapai maklumat pengguna lain tanpa kebenaran adalah melanggar Dasar ini.

8.5 Pengurusan Maklumat Rahsia atau Sulit

8.5.1 Pengambilan Maklumat Rahsia atau Sulit

(i) Pemilik Sistem 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 Pemilik Maklumat tersebut dan bukan daripada orang lain.

(b) Pemilik Sistem hendaklah memberi kebenaran terlebih dahulu terhadap sesuatu maklumat yang diberikan oleh Pemilik Proses.

(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 Pemilik Sistem.

(c) *Web master* bertanggungjawab memastikan hanya maklumat peribadi yang dibenarkan sahaja boleh dipaparkan di laman web UUM. Pemilik Sistem 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 tanpa kebenaran Pemilik Sistem . Maklumat tersebut ialah:

1. bangsa;
2. agama,
3. keahlian sesuatu persatuan;
4. maklumat kesihatan, rawatan yang diambil;
5. keputusan peperiksaan;
6. maklumat kewangan;
7. tindakan tatatertib;
8. no. IC/no. passport;
9. tarikh lahir; dan
10. no. staf/no. matrik

(b) Semua maklumat yang sensitif hendaklah dinyatakan dengan jelas tujuan penggunaannya semasa permohonan mendapatkan maklumat dilakukan.

(iv) Maklumat peribadi yang boleh diambil daripada Pemilik Maklumat :

(a) UUM boleh meminta apa-apa maklumat yang berkaitan urusan kerja tetapi tidak terhad kepada maklumat berikut:

1. Nama
2. Gelaran
3. PTJ
4. Jawatan
5. Nombor telefon pejabat
6. Alamat surat menyurat
7. Alamat e-mel

(b) UUM boleh meminta apa-apa maklumat yang Berkaitan urusan pengajian tetapi tidak terhad kepada maklumat berikut:

1. nama
2. nombor matrik
3. program
4. pusat pengajian
5. alamat surat menyurat
6. alamat e-mel

(c) Tujuan pengambilan dan penggunaan maklumat hendaklah dimaklumkan kepada Pemilik Maklumat jika maklumat tersebut perlu dihebahkan untuk tujuan tertentu.

(d) Hak untuk meminta capaian maklumat peribadi dan hak untuk membuat pindaan atau pembetulan jika terdapat kesilapan hendaklah dimaklumkan kepada Pemilik Sistem.

(v) Had pengambilan maklumat rahsia atau sulit selain daripada Pemberi Maklumat:

Bagi kes di mana maklumat diambil daripada pihak ketiga, kebenaran hendaklah diminta daripada Pemilik Sistem. Apabila maklumat yang diberi oleh seseorang kepada seseorang yang lain dengan izin Pemilik Sistem perkara berikut hendaklah diikuti:

(iv) Tujuan pengambilan maklumat;
(v) Jenis maklumat yang diambil; dan
(vi) Tanggungjawab untuk memastikan maklumat dijaga atau disimpan dengan baik.

8.5.2 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 UUM:

(a) Penggunaan maklumat peribadi yang telah diambil mestilah mengikut syarat berikut:

1. Pemilik Maklumat telah memberi kebenaran menggunakan maklumat tersebut.
2. Maklumat boleh digunakan untuk tujuan perkhidmatan.
3. Maklumat boleh digunakan untuk apa-apa tujuan yang dibenarkan oleh undang-undang.

(b) Maklumat peribadi yang digunakan selain daripada tujuan asal ketika maklumat itu diambil hendaklah mendapat kebenaran daripada Pemilik Maklumat.

8.5.3 Penyenggaraan Maklumat Rahsia atau Sulit

(i) UUM bertanggungjawab memastikan ketepatan maklumat peribadi semasa dalam simpanan dan sentiasa dikemas kini untuk tujuan yang diperlukan. Pemilik Maklumat yang masih aktif perlu mengemas kini maklumat rahsia atau sulit dari semasa ke semasa mengikut keperluan.

(ii) UUM 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) UUM bertanggungjawab menjamin kerahsiaan maklumat peribadi. Pegawai yang dipertanggungjawab menyimpan, mengumpul atau memproses data mestilah memastikan maklumat peribadi tidak disebarkan kepada pihak lain, selain daripada mereka yang mempunyai hak untuk mengetahui

maklumat tersebut.

(iv) Kebenaran untuk mencapai maklumat peribadi oleh Pemilik Maklumat untuk tujuan pengesahan boleh diberi untuk satu tempoh yang munasabah. Pemilik Maklumat hendaklah memaklumkan kepada Pemilik Sistem jika terdapat kesilapan maklumat peribadi untuk tujuan pembetulan.

(v) Bantahan terhadap penggunaan maklumat peribadi oleh Pemilik Maklumat boleh dipertimbangkan. Walau bagaimanapun jika maklumat peribadi itu digunakan untuk tujuan perkhidmatan, pengajian atau atas keperluan perundangan, maka bantahan tersebut tidak akan dipertimbangkan.

BAB 9

DASAR PENGURUSAN *SERVER* DAN PENGKOMPUTERAN AWAN

BAB 9: DASAR PENGURUSAN *SERVER* DAN PENGKOMPUTERAN AWAN

9.1 Tujuan

Menerangkan peraturan dan perkara yang perlu dipatuhi untuk membangun dan mengoperasi *server* dan pengkomputeran awan di UUM.

9.2 Skop

9.2.1 *Server* merangkumi semua sistem *server* UUM (perkakasan dan perisian) termasuk yang dibenarkan untuk dibangunkan oleh pengguna iaitu:

(i) *Server* utama;
(ii) *Server* aplikasi;
(iii) *Server* rangkaian; dan
(iv) *Serve*r kegunaan setempat.

9.2.2 Terdapat dua (2) kategori *server* iaitu *server* kritikal dan *server* biasa.

(i) *Server* kritikal bermaksud *server* yang terdiri daripada salah satu atau kombinasi kriteria berikut:

(a) Digunakan untuk pelaksanaan Sistem Maklumat UUM.
(b) Menyimpan data yang penting dan kritikal.
(c) Tahap kebolehcapaian dan kesediaan *server* yang tinggi.
(d) Menawarkan perkhidmatan dan maklumat UUM kepada pihak luar.
(e) Memerlukan tahap keselamatan dan kerahsiaan yang tinggi
(f) Memerlukan proses *backup* dan *restore*.

(ii) *Server* biasa bermaksud *server* yang digunakan untuk memberikan perkhidmatan kepada pengguna di UUM tetapi tidak mempunyai ciri seperti yang terkandung pada *server* kritikal.

9.3 Hak Milik

Semua server yang diperolehi untuk atau bagi pihak UUM adalah menjadi hak milik UUM.

9.4 Tanggungjawab

(i) Pemilik

Melantik pentadbir sistem yang mempunyai kemahiran untuk menguruskan *server* tersebut. Pemilik juga mesti memastikan *server* tersebut didaftarkan dengan UUMIT

bagi tujuan keselamatan, meminimakan gangguan perkhidmatan serta dapat memastikan apa-apa makluman kepada pengguna dapat disalurkan dengan betul.

(ii) Pentadbir Sistem

Memastikan *server* diurus dan ditadbir dengan betul serta memenuhi keperluan pemilik *server* dan polisi yang berkuatkuasa. Pentadbir sistem adalah bertanggungjawab sepenuhnya ke atas keselamatan data dan sistem di dalam *server*.

9.5 Polisi Am

9.5.1 Perolehan

(i) Semua perolehan server baharu perlu dirujuk kepada Jawatankuasa Penilai Spesifikasi/Jawatankuasa Perolehan/Jawatankuasa Teknikal UUMIT mengikut mana yang berkenaan terlebih dahulu untuk tujuan penyelarasan.

(ii) Spesifikasi *server* untuk tujuan perolehan perlu mendapat pengesahan dan kelulusan Jawatankuasa Penilai Spesifikasi/Jawatankuasa Perolehan/Jawatankuasa Teknikal UUMIT mengikut mana yang berkenaan.

(iii) Semua perolehan *server* PTJ diurus dan dilaksanakan oleh PTJ mengikut prosedur perolehan UUM.

(iv) Semua perolehan *server* PTJ adalah menggunakan peruntukan yang perlu disediakan oleh PTJ masing-masing.

9.5.2 Penempatan

(i) Penempatan *server* perlu mengambil kira keperluan operasi berdasarkan empat (4) kriteria iaitu:
   (a) Reka bentuk dan kompleksiti sistem;
   (b) Keselamatan dan kerahsiaan maklumat;
   (c) Keperluan pemprosesan dan prestasi capaian;
   (d) Halangan perundangan.

(ii) *Server* kritikal mesti ditempatkan di Pusat Data UUM *(Private Cloud)* yang telah dilengkapi dengan kriteria seperti berikut:

   (a) Lokasi yang selamat dan hanya boleh dicapai oleh staf atau individu yang dibenarkan sahaja.

   (b) Mempunyai sistem dan peralatan 'backup' seperti media yang mencukupi untuk menyimpan data-data di dalam *server* secara berkala mengikut

tempoh tertentu.

(c) Mempunyai peralatan *Uninterruptible Power Supply (UPS)* dengan masa minimum beroperasi 30 minit jika terputus bekalan elektrik dan perlindungan daripada kilat serta menyokong penutupan *(shut down) server* secara automatik untuk mengelakkan kerosakan.

(d) Memasang 'generator set' yang bersesuaian bagi memastikan server masih terus berfungsi apabila berlaku gangguan bekalan elektrik.

(e) Mempunyai sistem pencegah kebakaran.

(f) Pengudaraan yang mencukupi dan suhu hendaklah terkawal di dalam had suhu yang diperlukan untuk *server*.

(iii) *Server* biasa boleh diletakkan di PTJ dengan syarat mendapat kebenaran daripada UUMIT dan memenuhi kriteria berikut;

(a) Lokasi yang selamat dan hanya boleh dicapai oleh staf atau individu yang dibenarkan sahaja.

(b) Mempunyai peralatan UPS untuk mengelakkan kerosakan pada *server* jika berlaku gangguan elektrik.

(c) Mempunyai peralatan 'backup' jika wujud keperluan untuk menyimpan data di dalam *server* secara berkala mengikut tempoh tertentu.

(d) Mempunyai sistem pencegah kebakaran.

(e) Pengudaraan yang mencukupi dan suhu hendaklah terkawal di dalam had suhu yang diperlukan untuk *server*.

(iv) *Server* biasa boleh menggunakan kemudahan *Public Cloud* dengan syarat pelaksanaan mendapat persetujuan UUMIT dan selaras dengan pekeliling Dasar Perkhidmatan Pengkomputeran Sektor Awam yang sedang berkuat kuasa.

(v) PTJ adalah bertanggungjawab ke atas mana-mana *server* yang berada di bawah pengawasan PTJ dan ditempatkan di lokasi luar dari Pusat Data UUM.

(vi) PTJ adalah bertanggungjawab ke atas mana-mana *server* yang berada di bawah pengawasan PTJ dan tidak memenuhi syarat penempatan seperti di perenggan 9.5.2. (iii).

9.5.3 Pelupusan

Semua *server* yang tidak boleh digunakan lagi sama ada telah rosak atau usang dari segi usia dan teknologi perlu dimaklumkan oleh PTJ kepada UUMIT untuk tujuan pelupusan mengikut prosedur pelupusan UUM.

9.6 Keperluan Mininum Pengurusan *Server*

9.6.1 Pengurusan Semua *Server*

(i) Pentadbir mesti memastikan perisian yang dipasang di *server* mestilah perisian yang berlesen.
(ii) *Server* mestilah mempunyai perisian antivirus dan sentiasa dikemas kini. Pentadbir mesti memastikan pengemaskinian 'patches' sentiasa dibuat pada *server*.
(iii) Hanya servis yang diperlukan sahaja harus dibuka manakala servis lain perlu ditutup.
(iv) Pentadbir mesti memastikan tiada servis penting yang melibatkan rangkaian seperti *Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Lightweight Directory Access Protocol (LDAP), Windows Domain Controller (Active Directory), Novell NDS* digunakan kecuali mendapat kebenaran secara bertulis daripada UUMIT terlebih dahulu.
(v) *Server* tersebut mesti dibuat proses 'backup' data atau sistem jika wujud keperluan untuk menyimpan data atau sistem secara berkala mengikut tempoh tertentu.
(vi) Pentadbir mesti sentiasa membuat semakan ruang storan pada *server*.
(vii) Hanya akaun pengguna/sistem yang sah dan masih digunakan yang perlu wujud di dalam *server.* Mana-mana akaun yang tidak digunakan atau tidak sah mesti dibuang dan direkodkan bagi tujuan audit keselamatan jika perlu.
(viii) Semua kata laluan untuk 'default account' perlu ditukar dan 'default account' yang tidak diperlukan perlu di'disable'.
(ix) Polisi kata laluan yang selamat perlu dilaksanakan pada setiap *server*.
(x) Pentadbir mestilah memastikan tiada capaian oleh pengguna yang tidak dibenarkan ('unauthorised access') kepada *server* berkenaan.
(xi) Pentadbir mestilah memberikan kebenaran capaian yang bersesuaian kepada pengguna masing-masing.
(xii) Pentadbir mestilah memastikan tiada capaian oleh pengguna yang boleh menyebabkan ancaman kepada *server* seperti jangkitan virus, pencerobohan dan sebagainya.
(xiii) Maklumat berkaitan pengguna, rangkaian dan sistem yang kritikal perlu disimpan untuk tujuan audit.

9.6.2 Pengurusan *Server* Kritikal

(i) *Server* tidak boleh digunakan untuk tujuan pengujian atau kajian.

(ii) *Server* mestilah dibuat proses 'backup' data dan sistem. Rekod-rekod 'backup' mesti diarkib bagi tujuan capaian semula.

(iii) Data-data bagi sistem utama mestilah dibuat proses penyalinan untuk tujuan *backup*.

(iv) Pentadbir mesti membuat pemantauan yang rapi bagi memastikan prestasi *server* pada tahap yang baik.

(v) Pentadbir harus menyemak secara berkala tahap keselamatan *server* sama ada dari segi fizikal atau kandungan *server* bagi memastikan tiada apa-apa aktiviti yang tidak dibenarkan dibuat ke atas *server*.

(vi) Rekod-rekod sejarah kata laluan *(password history)* mesti dipantau bagi memastikan kadar tempoh masa penggunaan semula kata laluan lama tidak terlalu dekat. Polisi kata laluan yang selamat perlu dilaksanakan pada setiap komputer server.

(vii) Audit keselamatan pada *server* perlu dibuat secara berkala dan direkodkan bagi memastikan tiada risiko pencerobohan.

BAB 10

DASAR PEMBANGUNAN LAMAN WEB

BAB 10: DASAR PEMBANGUNAN LAMAN WEB

10.1 Tujuan

Menjadi rujukan tentang tatacara pembangunan laman web di UUM sejajar dengan keperluan semasa dan perkembangan ICT.

10.2 Skop

Melibatkan semua pembangunan laman web di UUM, sama ada dibangunkan secara berpusat (oleh Pentadbir Laman Web UUM menggunakan server web utama) atau secara berasingan (oleh Pusat Tanggungjawab (PTJ) mengguna server web PTJ).

10.3 Dasar Pembangunan

(a) Am

(a) Permohonan untuk laman web peribadi staf UUM terutama yang berbentuk ilmiah boleh dibangunkan dengan kelulusan Pengarah UUMIT.
(b) Ketua PTJ, persatuan atau staf UUM adalah bertanggungjawab sepenuhnya terhadap semua kandungan laman web masing-masing.
(c) Pihak UUM tidak akan bertanggungjawab terhadap penyalahgunaan hak harta intelek termasuk hak cipta di dalam kandungan laman web masing-masing.
(d) UUM berhak untuk mengarahkan supaya ditukar atau diubah kandungan laman web yang difikirkan tidak sesuai atas kepentingan UUM.

(b) Peranan

(a) Pentadbir Sistem

(i) UUMIT bertanggungjawab menyediakan tapak atau ruang untuk keperluan laman web rasmi UUM, PTJ atau persatuan atau aktiviti rasmi sahaja.
(ii) UUMIT bertanggungjawab untuk memastikan semua laman web yang diletakkan di UUMIT adalah berfungsi dalam keadaan baik.
(iii) Pentadbir sistem berhak menentukan perisian pembangunan laman web dan pangkalan data bagi tujuan pengoptimuman penggunaan dan keselamatan.

(b) *Web Master*

(i) Keselamatan laman web adalah di bawah tanggungjawab PTJ atau persatuan jika melibatkan

penggunaan *server* sendiri atau perkhidmatan *Web Hosting*. UUM juga boleh mengehadkan atau memansuhkan akses kepada mana-mana laman web tersebut jika perlu. Rujuk Bab 3 perenggan 3.7.5 *Web Hosting*

(ii) Setiap PTJ atau persatuan mestilah melantik seorang *web master* yang akan bertanggungjawab mengemas kini isi kandungan laman web masing-masing.

(iii) Laman web UUM dan laman web lain boleh menggunakan sama ada Bahasa Malaysia atau Bahasa Inggeris. Penambahan penggunaan bahasa-bahasa lain adalah digalakkan.

(iv) Semua laman web yang dibangunkan hendaklah mematuhi ciri-ciri identiti korporat UUM seperti yang dinyatakan dalam Manual Identiti Korporat UUM dan mempunyai pautan dengan laman web rasmi UUM.

(v) Kandungan laman web tidak boleh mengandungi maklumat yang menyalahi undang-undang/ peraturan UUM, negeri dan negara. Ini termasuk tetapi tidak terhad kepada maklumat yang berbentuk keganasan, lucah, hasutan, fitnah dan yang boleh menimbulkan atau membawa kepada keganasan, keruntuhan akhlak dan kebencian.

BAB 11

DASAR E-PEMBELAJARAN

BAB 11: DASAR e-PEMBELAJARAN UNIVERSITI UTARA MALAYSIA

11.1 Tujuan

Menjadi rujukan tentang tatacara, prosedur dan pelaksanaan e-Pembelajaran di UUM bagi memastikan pengajaran dan pembelajaran berasaskan e-Pembelajaran mencapai piawaian global.

11.2 Skop

Melibatkan pihak pengurusan UUM, Pusat Pengajaran dan Pembelajaran (UTLC), UUMIT, Kolej, Pusat Pengajian, HEA, pensyarah dan pelajar.

11.3 Objektif

Dasar e-Pembelajaran UUM adalah untuk mencapai objektif berikut:

(i) Memastikan pengajaran dan pembelajaran berasaskan e-Pembelajaran mencapai piawaian global.

(ii) Menjelaskan peranan pihak pengurusan, pensyarah dan pelajar berkaitan e-Pembelajaran UUM.

11.4 Dasar e-Pembelajaran

Dasar ini meliputi aspek berikut:

11.4.1 Polisi Am

(i) UUM mempunyai hak milik ke atas semua isi kandungan yang dimuat naik ke server e-Pembelajaran UUM.

(ii) Apa-apa penerbitan yang bukan milik pensyarah mesti mendapat kebenaran pemilik asalnya terlebih dahulu.

(iii) Apa-apa petikan dari mana-mana buku rujukan/jurnal penyelidikan mesti dinyatakan dengan jelas oleh pensyarah berkenaan. Apa-apa

tindakan atau tuntutan ke atas hak milik oleh pemilik asal penerbitan berkenaan adalah ditanggung oleh pensyarah sendiri dan pensyarah hendaklah menanggung rugi UUM bagi tindakan tersebut.

(iv) Semua pensyarah dan pelajar yang mempunyai akaun dan berstatus aktif di dalam aplikasi e-Pembelajaran merupakan pengguna sah aplikasi e-Pembelajaran UUM.

(v) Kerahsiaan profil pengguna adalah terhad kepada tujuanpengajaran dan pembelajaran.

(vi) Apa-apa penggunaan untuk tujuan lain perlu mendapat kebenaran daripada UUM.

(vii) Kolej/Pusat Pengajian dan pensyarah adalah bertanggungjawab sepenuhnya terhadap aplikasi dan sistem e-Pembelajaran yang tidak diuruskan dan diselenggara oleh UUM.

11.4.2 Pengurusan dan Perkhidmatan UUMIT Terhadap Dasar e-Pembelajaran

(i) Menyedia dan menyenggara infrastruktur, perkakasan, rangkaian, perisian dan khidmat sokongan yang berkaitandengan e-Pembelajaran.

(ii) Menjamin keselamatan serta integriti data dalam sistem pengurusan e-Pembelajaran UUM.

(iii) Membuat salinan data setiap semester dan disimpan selama empat (4) tahun.

(iv) Menyediakan sokongan teknikal e-Pembelajaran dalam waktu pejabat.

(v) UUMIT hanya bertanggungjawab terhadap aplikasi dan perisian yang diuruskan oleh UUM.

11.4.3 Peranan dan Tanggungjawab

(i) Peranan Pengurusan UUM

(a) Menetapkan hala tuju, dasar e-Pembelajaran dan memberi komitmen termasuk penyediaan dana dalam pelaksanaan inisiatif e-Pembelajaran di UUM demi kepentingan pemegang taruh.

(b) UUM bertanggungjawab menyediakan satu (1) sistem pengurusan e-Pembelajaran untuk kegunaan seluruh UUM.

(c) UUM melalui Jawatankuasa Pengurusan e-Pembelajaran seperti di **Lampiran C** bertanggungjawab menggubal dasar dan memantau perlaksanaan e-Pembelajaran peringkat UUM.

(d) UUM melalui UTLC berperanan membudayakan e-Pembelajaran dan pembangunan kandungan kursus.

(e) UUM bertanggungjawab memastikan bilik-bilik kuliah dilengkapi dengan kemudahan teknologi e-Pembelajaran dan capaian kepada e-Pembelajaran dalam keadaan sedia diguna.

(ii) Peranan UTLC

(a) Memberi kesedaran dan pendedahan kepada pensyarah mengenai penggunaan e-Pembelajaran bagi tujuan pengajaran dan pembelajaran.

(b) Memastikan pelaksanaan e-Pembelajaran kepada pensyarah UUM.

(c) Menyediakan latihan penggunaan e-Pembelajaran kepada pensyarah dan pelajar UUM.

(d) Memantau dan menyelaras aktiviti e-Pembelajaran dan pembangunan bahan pengajaran dan pembelajaran di setiap kolej.

(e) Menjalankan aktiviti penyelidikan dan pembangunan berkaitan dengan e-Pembelajaran.

(f) Menyediakan garis panduan e-Pembelajaran.

(iii) Peranan *Academic Excellent Development Unit* (AEDU)

Membangunkan polisi dan garis panduan yang berkaitan dengan program akademik.

(iv) Peranan Kolej/Pusat Pengajian

(a) Membentuk jawatankuasa penyelarasan e-

Pembelajaran di peringkat kolej yang diketuai oleh Penolong Naib Canselor bagi memantau pelaksanaan e-Pembelajaran.

(b) Melantik penyelaras e-Pembelajaran di peringkat kolej.

(c) Memastikan pensyarah mempunyai kemahiran teknologi di dalam mengendalikan kursus berasaskan e- Pembelajaran.

(d) Memastikan pensyarah mempunyai integriti akademik di dalam menguruskan e-Pembelajaran.

(e) Menyelaraskan garis panduan e-Pembelajaran yang bersesuaian untuk program masing-masing dengan UTLC.

(f) Memaklumkan kepada pelajar berkenaan kursus e-Pembelajaran melalui taklimat, bengkel dan maklumat lainyang berkaitan.

(g) Menyediakan sokongan, motivasi dan ganjaran yang bersesuaian kepada pensyarah yang aktif dalam penggunaan e-Pembelajaran atau pembangunan bahan PdP digital.

(v) Peranan Pensyarah

(a) Mematuhi dasar dan garis panduan e-Pembelajaran UUM.

(b) Membuat perancangan bagi pembelajaran teradun selari dengan keperluan pelajar dan UUM.

(c) Mereka bentuk pembelajaran selari dengan keperluan pembelajaran dalam talian.

(d) Melaksana pembelajaran teradun mengikut perancangan.

(e) Menggunakan sistem e-Pembelajaran secara berterusan.

(f) Mengoptimumkan aplikasi e-Pembelajaran yang disediakan oleh UUM.

(g) Memantau dan membimbing pelajar dalam penggunaan e-Pembelajaran.

(h) Menghadiri latihan e-Pembelajaran untuk pembangunan profesional.

(i) Membangun dan menyenggara kandungan e-Pembelajaran bagi kursus yang dikendalikan.

(vi) Peranan Pelajar

(a) Mematuhi dasar dan garis panduan e-Pembelajaran UUM.

(b) Meningkatkan kemahiran menggunakan e-Pembelajaran secara berterusan.

(c) Menggunakan bahan pembelajaran secara berterusan.

(d) Mengoptimumkan penggunaan e-Pembelajaran yang disediakan oleh UUM.

(vii) Peranan Penyedia Bahan

(a) Bertanggungjawab sepenuhnya terhadap bahan-bahan yang disumbangkan.

(b) Mengemas kini bahan pembelajaran dari semasa ke semasa.

(c) Mematuhi peraturan UUM serta undang-undang berkaitan.

(d) Mematuhi garis panduan proses pembangunan yang ditetapkan.

11.5 Hak Cipta

11.5.1 Hak Cipta Kandungan Kursus

(i) Semua hak cipta bahan pengajaran yang dibangunkan menggunakan kemudahan dan sokongan yang disediakan oleh UUM adalah milik UUM.

(ii) Penggunaan bahan e-Pembelajaran oleh pihak lain perlu mendapat kebenaran UUM.

(iii) Penyedia bahan boleh menggunakan kandungan tersebut untuk kegunaan lain seperti pengajaran di dalam kelas, penyelidikan, penerbitan serta pembentangan dalam seminar.

(iv) Pengedaran bahan kandungan pengajaran dan pembelajaran yang dibangunkan sama ada secara elektronik atau bukan elektronik adalah hak milik UUM.

(v) Penyediaan dan penggunaan bahan kandungan kursus adalah tertakluk kepada undang-undang berkaitan.

11.5.2 Hak Cipta Sistem

(i) Sistem yang dibangunkan oleh UUM dengan pembiayaan dalaman adalah hak mutlak UUM.

(ii) Sistem yang dibeli adalah tertakluk kepada perjanjian dan terma-terma pembelian.

(iii) Pengguna dilarang membuat apa-apa pengubahsuaian terhadap sistem e- pembelajaran.

BAB 12

PEMATUHAN DAN TINDAKAN PENGUATKUASAAN

BAB 12: PEMATUHAN DAN TINDAKAN PENGUATKUASAAN

12.1 Tujuan

Memaklumkan kepada pengguna tentang tindakan yang boleh dikenakan kerana melanggar Dasar ICT UUM.

12.2 Skop

Meliputi apa-apa bentuk pelanggaran yang dinyatakan di dalam Dasar ICT UUM atau mana-mana Akta, Arahan, Pekeliling dan Peraturan yang berkaitan.

12.3 Jenis Pelanggaran dan Tindakan Terhadap Pelanggaran

(i) Jika mana-mana pengguna telah didapati melakukan pelanggaran terhadap kesalahan yang dinyatakan di bawah, maka UUM boleh mengenakan mana-mana satu atau apa-apa gabungan dua atau lebih hukuman seperti berikut:

A. Tindakan Terhadap Pelanggaran Dasar Keselamatan ICT (Bab 3)	
Pelanggaran	**Tindakan**
(a)Akses tanpa kebenaran (b)Melakukan kesalahan vandalisma terhadap perkakasan ICT.	(a) Diberi amaran bertulis oleh Pengarah UUMIT; (b)Pengguna dikenakan penggantungan penggunaan kemudahan ICT di UUM.
B. Tindakan Terhadap Pelanggaran Penggunaan Perisian dan Perkakasan ICT (Bab 4)	
Pelanggaran	**Tindakan**

(a) Memuat turun, mengubah suai, mendedahkan, membuat pemasangan, menghapuskan dan menggunakan perisian yang boleh menyebabkan kerosakan komputerdan Rangkaian UUM; (b) Menjual, menyewa, melesen semula, meminjamkan, menyalin semula, menyebar atau memberi semua perisian hak milik UUM kepada individu atau entiti tanpa kebenaran UUM; dan (c) Apa-apa bentuk permainan komputer (kecuali untuk tujuan pengajaran dan penyelidikan) tanpa kelulusan Ketua PTJ;	(i) Diberi amaran bertulis oleh Pengarah UUMIT; (ii) Pengguna diminta untuk *uninstall* perisian yang tidak berlesen tersebut; (iii) Mengehadkan kapasiti capaian ke rangkaian; (iv) Pengguna dikenakan penggantungan penggunaan kemudahan ICT di UUM.
C. TindakanTerhadap Pelanggaran PenggunaanKemudahan Rangkaian UUM (Bab 5)	
Pelanggaran	**Tindakan**
(a) Pengguna menggunakan peralatan WiFi *booster* untuk menarik signal WiFi. (b) Menyambung peranti elektronik termasuk tetapi tidak terhad kepada komputer peribadi atau *notebook* dan *hub* atau *switch* peribadi atau modem ke	(a) Diberi amaran bertulis oleh Pengarah UUMIT; (b) Digantung kemudahan penyambungan rangkaian; (c) Mengehadkan kapasiti capaian ke rangkaian.

rangkaian UUM dengan tujuan mencapaisumber ICT yang tidak dibenarkan; dan (c) Menggunakan perisian penggodam komputer atau rangkaian.	
D. Tindakan Terhadap Pelanggaran Peraturan Penggunaan Kemudahan PdP **(Bab 6)**	
Pelanggaran	**Tindakan**
(a) Menggunakan komputer bukan untuk tujuan akademik seperti main *computer game* atau sembang siber (*chatting);* (b) Mengganggu pengguna lain dengan apa cara sekalipun, termasuk menimbulkan rasa aib, marah dan tidak selesa; (c) Menukar kedudukan komputer dan peranti; (d) Melayari laman sesawang yang mengandungi unsur lucah, menghina, menghasut dan memfitnah; (e) Menukar konfigurasi komputer; (f) Menambah dan membuang apa-apaperisian; (g) Menyimpan atau memuat turun maklumat atau data ke dalam cakera keras komputer;	(i) Diberi amaran bertulis oleh Pengarah UUMIT; (ii) Dilarang menggunakan peralatan kemudahan PdP yang ditetapkan; (iii) Ditarik balik kemudahan akaun pengguna (jika ada); (iv) Mengganti atau membayar kos peralatan yang dicuri, hilang rosak atas kecuaian semasa penggunaan; dan (v) Pengguna dikenakan penggantungan penggunaan kemudahan ICT diUUM.

(h) Membawa keluar tanpa kebenaran apa-apa peralatan dari makmal; dan (i) Mencuri peranti dan perkakasan komputer.	
E. Tindakan Terhadap Pelanggaran Penggunaan Kemudahan Internet (Bab 7)	
Pelanggaran	**Tindakan**
(a) Menggunakan akaun e-mel palsu atau menyamar sebagai pihak lain; (b) Menggunakan kemudahan e-mel untuk apa-apa aktiviti yang tidak dibenarkan oleh peraturan UUM dan undang-undang negara; (c) Menggunakan aktiviti *spamming, mail-bombing, phishing* dan atau penyebaran e-mel dengan kandungan tidak beretika kepada individu, *mailing list* atau *discussion group* sama ada di dalam rangkaian UUM atau ke internet; (d) Menyebarkan e-mel yang mengandungi virus; (e) Mengganggu atau menceroboh laman web/media sosial mana-mana jabatan, organisasi di dalam/luar negara; dan (f) Memasuki, menyalin, menciplak, mencetak dan menyebarkan maklumat daripada Internet yang menyalahi undang-undang negara.	(i) Diberi amaran bertulis oleh Pengarah UUMIT; (ii) Mengehadkan kapasiti capaian internet; (iii) Mengehadkan penggunaan e-mel UUM. (iv) Menggantung kemudahan e-mel/Internet

F. Tindakan Terhadap Pelanggaran Capaian dan Kerahsiaan Maklumat (Bab 8)	
Pelanggaran	**Tindakan**
(a) Menggunakan kemudahan ICT untuk menyimpan data atau maklumat sensitif, rahsia atau sulit di dalam komputer atau akaun pengguna tanpa kebenaran; (b) Menggunakan identiti pengguna lain untuk akses kepada maklumat yang tidak dibenarkan; (c) Mencapai data atau maklumat pengguna lain tanpa kebenaran; dan (d) Menyalah guna akses kepada capaian maklumat.	(i) Diberi amaran bertulis oleh Pengarah UUMIT; (ii) ID pengguna dibatalkan; (iii) Digantung kemudahan penyambungan rangkaian; (iv) Menyita kemudahan ICT yang diberikan;
G. Tindakan Terhadap Pelanggaran Penggunaan *Server* (Bab 9)	
Pelanggaran	**Tindakan**
(a) *Server* menimbulkan masalah keselamatan disebabkan oleh kecuaian pentadbir *server*; (b) Server digunakan untuk aktiviti yang menyalahi peraturan UUM.	(i) Diberi amaran bertulis oleh Pengarah UUMIT; (ii) Penyambungan *server* ke rangkaian akan ditutup; (iii) Server akan ditutup;dan (iv) Menyita *server* tersebut.
H. Tindakan Terhadap Pelanggaran Pembangunan Kandungan Laman Web (Bab 10)	
Pelanggaran	**Tindakan**

(a) Membangunkan laman web yang mengandungi kandungan atau pautan kepada maklumat yang menyalahi peraturan UUM dan undang-undang Negara; termasuk tetapi tidak terhad kepada maklumat yang berbentuk keganasan, keruntuhan akhlak dan kebencian.	(i) Diberi amaran bertulis oleh Pengarah UUMIT; ; (ii) Capaian laman web disekat atau ditutup; dan (iii) Menggantung kemudahan tapak laman web kepada *web master*/pemilik laman web.

LAMPIRAN

PENGURUSAN SISTEM APLIKASI

1.0 PENGURUSAN SISTEM KEWANGAN

1.1 TUJUAN

Menjadi rujukan tentang tatacara pengurusan sistem kewangan sejajar dengan keperluan *Standard Accounting System for Government Agency (SAGA)*, keperluan operasi semasa dan perkembangan ICT.

1.2 SKOP

Melibatkan semua pembangun, pentadbir dan pengguna sistem kewangan UUM termasuk tetapi tidak terhad kepada pegawai kewangan dan pegawai teknologi maklumat UUM.

1.3 PRINSIP

Prinsip yang menjadi asas kepada dasar ini ialah:

i. Akses

(a) Semua pengguna sistem dibenarkan untuk mengakses kepada sistem setelah mendapat kebenaran daripada Jabatan Bendahari melalui permohonan rasmi.

(b) Tahap akses kepada staf adalah berbeza mengikut hierarki dan bidang tugas dan tanggungjawab berkaitan dengan Pengurusan Kewangan.

(c) Pengguna sistem bagi pihak Pusat Tanggungjawab perlu mengemukakan borang pendaftaran pengguna yang telah disahkan oleh Jabatan Bendahari serta mendapat kelulusan penurunan kuasa daripada Naib Canselor sebelum diberi capaian.

(d) UUM perlu melantik dua (2) orang Pegawai Teknologi Maklumat sebagai pentadbir sistem kewangan yang akan menguruskan pentadbiran pengguna. Pegawai

yang dilantik tidak boleh terlibat secara langsung dalam sebarang operasi kewangan UUM.

ii. Akauntabiliti

Staf yang diberi kebenaran untuk mengakses dan mengguna sistem bertanggungjwab di atas tindakan yang dibuat berkaitan dengan tahap akses yang diberikan.

iii. Pengasingan

Tugas untuk mewujud, memadam, mengemas kini, mengubah dan mengesah data hendaklah diasingkan antara pengguna mengikut kesesuaian untuk mengelak kesilapan, kebocoran maklumat atau manipulasi data dan penyelewengan.

iv. Pengauditan

(a) Pengauditan sistem hendaklah dibuat bagi memastikan ketepatan dan kesahihan operasi sistem dan *output* yang dihasilkan.

(b) Rekod pengguna tidak boleh dihapuskan dari pangkalan data meskipun status pengguna adalah tidak aktif bagi tujuan jejak audit.

(c) Sistem kewangan perlu menyimpan jejak audit bagi setiap transaksi yang merangkumi perkara berikut; ID pengguna, tarikh dan masa transaksi, jenis transaksi, modul yang dicapai, masa log masuk dan log keluar.

v. Pemulihan

Pemulihan sistem perlu dilakukan untuk memastikan sistem sedia digunakan pada sepanjang masa. Ianya boleh dilakukan melalui salinan *(backup)* dan menyediakan pelan pemulihan bencana *(Disaster Recovery Plan).*

vi. Pematuhan

Dasar hendaklah dibaca, difahami dan dipatuhi supaya tidak berlaku pelanggaran kepada prosedur yang telah ditetapkan.

1.4 PEMBANGUNAN DAN PELAKSANAAN DASAR

(i) Pelaksanaan Dasar

Pelaksanaan Dasar dibuat oleh Jawatankuasa Pelaksana Dasar ICT Kewangan yang terdiri dari:

(a) Bendahari - Pengerusi
(b) Pengarah UUMIT
(c) Kumpulan Pembangunan Sistem Kewangan
(d) Ketua Unit bagi setiap Modul Sistem Kewangan
(e) Penolong Bendahari - Setiausaha

(ii) Semua pindaan dan cadangan baru mengenai dasar, perubahan dan peruntukan berkaitan sistem perlu dibincang dan diluluskan oleh Jawatankuasa Pelaksana Dasar ICT Kewangan sebelum sesuatu pindaan dibuat.

(iii) Dasar ini perlu disebar kepada semua pengguna sistem yang terlibat secara langsung meliputi:

(a) Pengurusan Tertinggi UUM dan Ketua Pusat Tanggungjawab
(b) Pegawai Pengurusan
(c) Pegawai Sokongan
(d) Pegawai Semakan
(e) Pihak Ketiga (pelajar, staf dan/atau pembekal/kontraktor):

(iv) Modul Sistem Kewangan yang dimaksudkan ialah:
- (a) Sistem Belanjawan
- (b) Sistem Bayaran
- (c) Sistem Terimaan
- (d) Sistem Perolehan
- (e) Sistem Lejar Am
- (f) Sistem Akaun Subsidiari
- (g) Sistem Akaun Pelajar
- (h) Sistem Pinjaman
- (i) Sistem Maklumat Pengurusan
- (j) Sistem Aset dan Inventori
- (k) Sistem Electronic Fund Transfer (eft-BIMB)

1.5 KAWALAN DAN KESELAMATAN

(i) Semua aset yang berkaitan dengan Sistem ICT hendaklah dikawal dan disimpan di tempat selamat untuk mengelak kerosakan dan kehilangan.

(ii) Semua staf yang terlibat di dalam sistem pengurusan kewangan berkomputer hendaklah mengendali maklumat seperti mengumpul, memproses, menyimpan, menukar dan memusnah dengan mengambil kira perkara berikut:

(a) Menghalang pendedahan kepada pihak yang tidak dibenarkan.
(b) Memeriksa maklumat agar ianya tepat dan benar.

(c) Menjaga rahsia kata laluan.
(d) Menjaga rahsia langkah keselamatan ICT diketahui umum.
(e) Memberi perhatian kepada maklumat terperingkat.

(iii) Memastikan fail yang dijana dari sistem kewangan disulitkan *(encrypted)* sebelum dihantar ke bank bagi transaksi *Electronic Fund Transfer* (EFT) dan data gaji.

(iv) Sistem kewangan akan menamatkan sesi secara automatik *(auto logoff)* sekiranya pengguna tidak aktif bagi tempoh 20 minit.

1.6 KESELAMATAN SUMBER MANUSIA

Untuk memastikan risiko seperti kesilapan, kecuaian dan penyalahgunaan sistem kewangan berkomputer perkara berikut perlu dilakukan:

(i) Menunjukkan dengan jelas senarai tugas dan tanggungjawab berkaitan dengan sistem kewangan berkomputer bagi setiap staf.

(ii) Semua insiden keselamatan ICT dipatuhi dengan melapor:
(a) Maklumat yang didapati hilang dan didedahkan kepada pihak luar.
(b) Sistem maklumat diguna tanpa kebenaran.
(c) Berlaku kejadian sistem luar biasa kehilangan fail dan *data corrupted*.
(d) Penyalahgunaan kata laluan.

(iii) Latihan berkala diberi kepada pengguna sedia ada dan wajib diberikan kepada pengguna baharu.

(iv) Tindakan tatatertib kepada staf yang melanggar dasar Pengurusan Sistem Aplikasi.

1.7 KESELAMATAN FIZIKAL

(i) Bilik prosesan utama sistem hanya boleh dimasuki oleh staf yang dibenarkan sahaja.

(ii) Perbekalan kuasa eletrik perlu sedia sepanjang masa supaya kejadian bekalan eletrik terputus tidak akan menjejas prosesan dan rekod kewangan.

(iii) Peralatan yang membantu sistem komputer hendaklah yang berteknologi terkini untuk melicin dan menjamin kecekapan sistem.

(iv) Penyenggaraan secara berkala kepada peralatan komputer perlu disedia supaya operasi dapat berjalan lancar tanpa gangguan.

1.8 KESELAMATAN SISTEM

Untuk memastikan sistem dapat digunakan pada bila-bila masa tindakan berikut perlu dilakukan:

(i) UUM bertanggungjawab menyediakan prasarana yang lengkap bagi menyokong sistem kewangan UUM.

(ii) *Backup* dilakukan oleh UUMIT setiap hujung hari untuk menyimpan data terkini sekiranya berlaku bencana.

(iii) Data kedua disimpan di Pusat Pemulihan Bencana UUM (*DRC*).

(iv) Dokumentasi tentang *'system flow'* dan apa-apa pindaan perlu disedia dan dikemas kini setiap berlaku perubahan kepada prosedur sistem.

1.9 INTEGRASI ANTARA SISTEM

(i) Senarai keperluan untuk melakukan integrasi di antara sistem kewangan dengan sistem lain di UUM mesti dibuat melalui Pemilik Sistem.

(ii) Pemilik Sistem hendaklah memastikan bahawa data-data dari sistem/modul lain adalah *'valid'* sebelum dipindah dan digunakan di dalam Sistem Kewangan.

(iii) Segala pindaan kepada data adalah tidak dibenarkan kecuali mendapat pengesahan dan kelulusan Bendahari.

(iv) Segala pindaan yang tidak melalui sistem yang sebenarnya atau *'breakdown access'* adalah dilarang sama sekali.

(v) Laporan yang diluluskan oleh sistem hendaklah disemak dan disahkan oleh pegawai yang bertanggungjawab kepada sesuatu modul sistem.

(vi) Audit 'trail' bagi setiap proses hendaklah disediakan dan disimpan oleh sistem untuk tindakan susulan jika perlu.

1.10 KAWALAN CAPAIAN

(i) Hanya pengguna yang dibenarkan dan diberi kata laluan dibenarkan memasuki dan mengguna sistem.

(ii) Kata laluan digalakkan ditukar setiap tiga (3) bulan bagi mengelakkan diketahui oleh pihak lain.

(iii) Kata laluan akan dihapuskan atau dipinda sekiranya pengguna bertukar PTJ, tanggungjawab atau berhenti dari perkhidmatan atau bercuti panjang.

LAMPIRAN B

Keanggotaan Jawatankuasa Pengurusan e-Pembelajaran UUM

(i) Pengerusi: TNC Akademik dan Antarabangsa.

(ii) Urus setia: UTLC

(iii) Senarai ahli:

(a) Pendaftar

(b) Bendahari

(c) Ketua Pustakawan

(d) Dekan Pusat Pengajian

(e) Pengarah UTLC

(f) Pengarah HEA

(g) Pengarah Jabatan Pembangunan

(h) Pengarah UUMIT

(i) Pengarah PACE