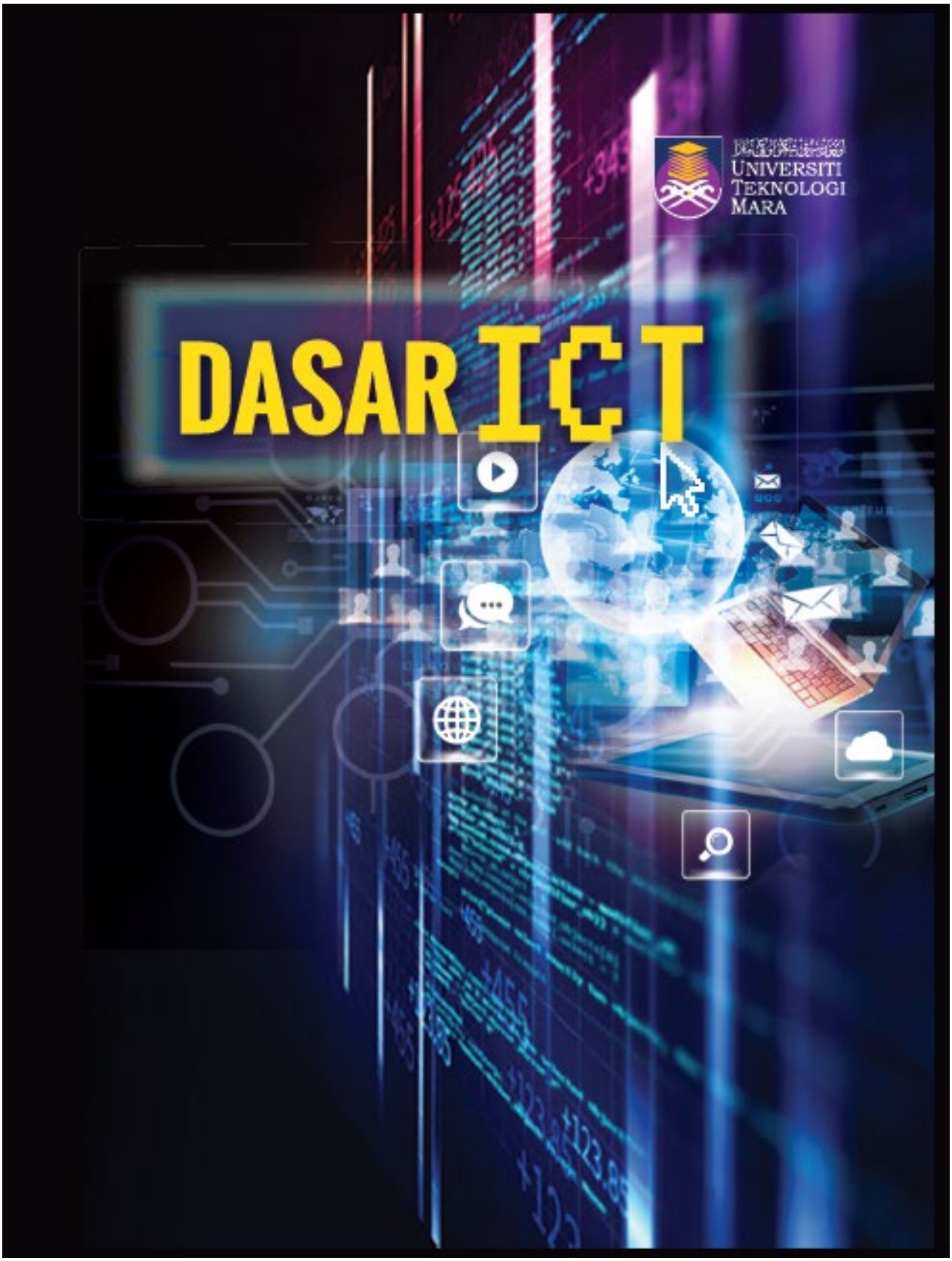

UNIVERSITI
TEKNOLOGI
MARA
DASAR ICT

UNIVERSITI
TEKNOLOGI
MARA

DASAR ICT

UNIVERSITI TEKNOLOGI MARA

Pejabat Infrastruktur dan Infostruktur
Aras 5 & 6, Menara SAAS
Universiti Teknologi MARA
Shah Alam, Selangor

1 April 2018

PRAKATA **NAIB CANSELOR**

Assalamualaikum warahmatullahi wabarakatuh dan Salam sejahtera

Alhamdulillah dengan berkat keizinan dan keredhaanNya dokumen Dasar ICT UiTM telah berjaya dihasilkan dan telah diluluskan oleh MEU pada 14 Mac 2018. Dokumen Dasar ICT ini memainkan peranan sebagai panduan dan sumber rujukan utama kepada warga UiTM terhadap pematuhan peraturan yang telah dinyatakan sebagai Dasar ICT UiTM. Semoga warga UiTM akan sentiasa terus berusaha bagi memastikan apa yang terkandung dalam dokumen Dasar ICT ini dapat dipatuhi dengan berkesan sehingga mencapai matlamat yang dihasratkan.

Cabaran ICT di masa kini semakin meluas dengan perubahan teknologi yang pantas, segala isu dan masalah mengenai ICT perlu ditangani secara rasional di semua peringkat di UiTM. Pelaksanaan pematuhan Dasar ICT ini akan dilakukan secara berperingkat bagi memenuhi keperluan semasa dan masa hadapan Universiti Teknologi MARA. Tindakan perlu diambil bagi mengenal pasti, meneliti dan menangani isu-isu ICT supaya perancangan dan pelaksanaan semua program dan projek ICT dapat dilaksanakan dengan lancar dan berkesan. Faktor penting yang akan menentukan kejayaan tersebut adalah menerusi kerjasama dan sokongan pengurusan dan warga UiTM dalam mematuhi Dasar ICT.

Dasar ICT ini meliputi semua sumber dan kemudahan ICT UiTM dan adalah terpakai bagi semua pengguna ICT di UiTM termasuk pembekal serta pihak lain yang menggunakan kemudahan ICT UiTM. Dasar ICT ini merupakan satu dokumen yang akan dikemaskini dari semasa ke semasa selaras dengan perubahan masa dan teknologi serta berdasarkan kepada arahan dan garis panduan terkini yang telah dikeluarkan oleh agensi pusat seperti MAMPU dan JPA. Dengan adanya Dasar ICT UiTM ini nanti, diharapkan semua warga UiTM akan mendapat manfaat dan keselamatan ICT akan lebih terjamin.

Akhir kata, terima kasih dan setinggi-tinggi penghargaan kepada Infostruktur, Pejabat Pembangunan Infastruktur dan Infostruktur dan seluruh warga kerja yang terlibat secara langsung atau tidak bagi menghasilkan dokumen Dasar ICT ini yang dapat dilaksanakan dengan sempurna dan jayanya. Semoga usaha murni ini akan memberi manfaat kepada semua warga UiTM.

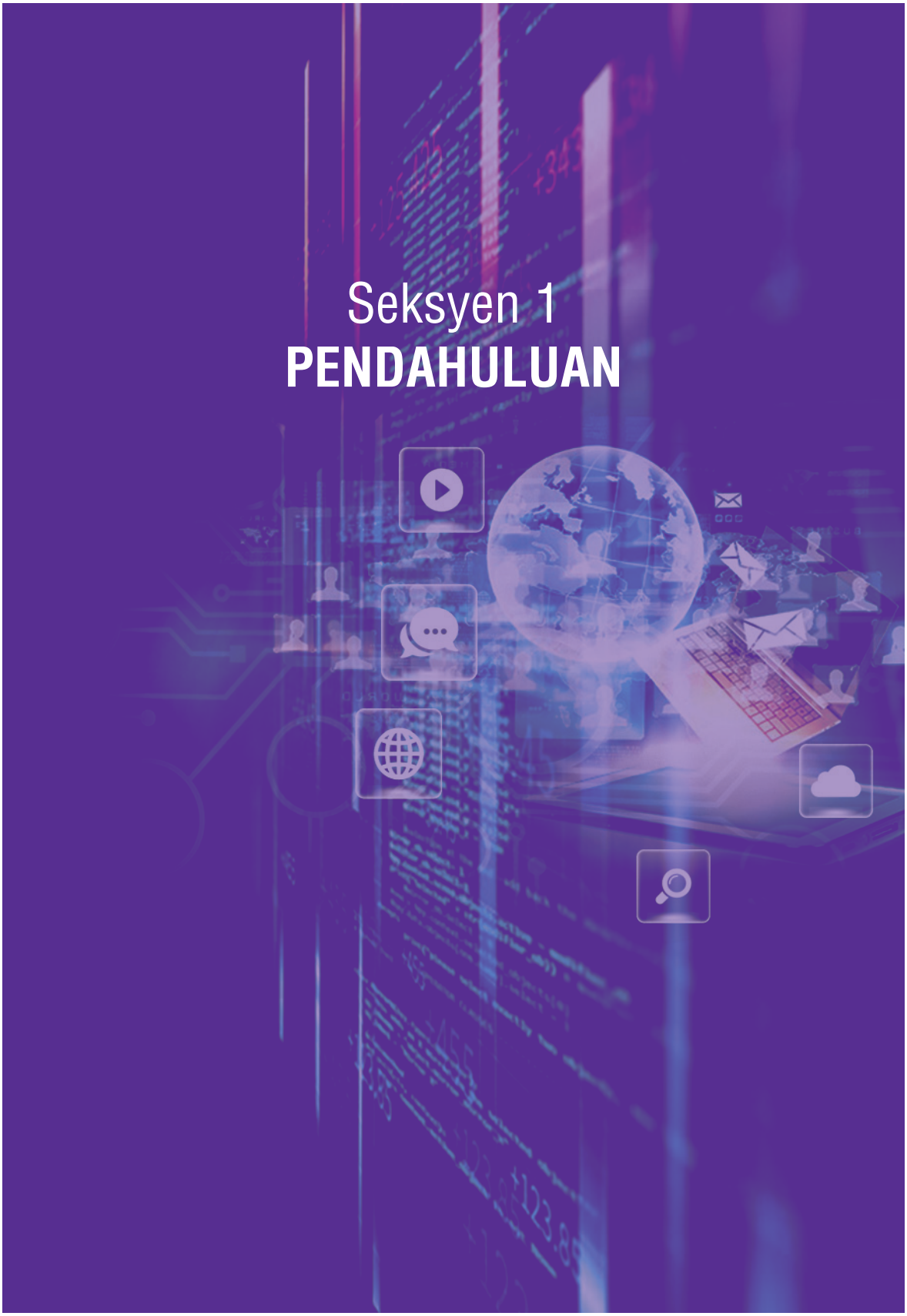
Sekian dan wassalam.

YBHG. PROFESSOR EMERITUS DATO' DR. HASSAN SAID

KANDUNGAN

Seksyen 1

PENDAHULUAN



1. PENGENALAN

Dokumen Dasar ICT Universiti Teknologi MARA merupakan sebuah dokumen yang menggariskan peraturan penggunaan aset dan kemudahan ICT UiTM dengan cara yang betul. Ia mesti dibaca dan dipatuhi oleh setiap pengguna kemudahan ICT universiti.

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

1.1 Penyataan Dasar

Dasar ICT UiTM diwujudkan untuk memastikan penggunaan sumber dan aset ICT universiti oleh semua warga universiti, dari segi infrastruktur, sistem aplikasi, kemudahan ICT serta data, adalah mengikut peraturan dan undang-undang demi menjadikan persekitaran ICT UiTM berkualiti tinggi dan selamat bagi melindungi dan menjamin keselamatan aset universiti. Semua warga UiTM dikehendaki mematuhi Dasar ini.

1.2 Tujuan

Tujuan dasar ini adalah untuk memaklumkan peraturan-peraturan yang perlu dipatuhi oleh semua pengguna aset dan sumber ICT Universiti, sama ada dari kalangan warga universiti atau pihak luar, untuk mengguna kemudahan yang diberikan secara berhemah dan menjaga keselamatan aset ICT dari segi perkakasan, perisian dan maklumat.

1.3 Skop

Dasar ini meliputi semua aset dan kemudahan ICT yang digunakan seperti maklumat (contoh: fail, dokumen, data elektronik), perisian (contoh: sistem aplikasi, perisian desktop dan perisian kolaborasi) dan fizikal (contoh: Pusat Data, PC, server, peralatan komunikasi, media storan dan lain-lain). Dasar ini adalah terpakai kepada semua pengguna sumber ICT Universiti termasuk pihak ketiga. Sumber ICT yang dimaksudkan ialah:

a. Perkakasan ICT

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

b. Perisian

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh, perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat, e-mel dan kolaborasi kepada UiTM;

c. Perkhidmatan

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

d. Data atau Maklumat

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

e. Infrastruktur ICT

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

f. Manusia

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

g. Premis Komputer Dan Komunikasi

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara (a) hingga (f) di atas. Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

Skop ancaman atau insiden Keselamatan ICT ialah:

a. Pelanggaran Dasar (*Violation of Policy*)

Penggunaan aset ICT bagi tujuan membocorkan maklumat dan/atau mencapai maklumat yang melanggar Dasar Keselamatan ICT;

b. Penafian Perkhidmatan (*Denial of Service*)

Ancaman ke atas keselamatan sistem komputer di mana perkhidmatan pemprosesan maklumat sengaja dinafikan terhadap pengguna sistem. Ia melibatkan sebarang tindakan yang menghalang sistem daripada berfungsi secara normal termasuk *denial of service* (DoS), *distributed denial of service* (DDoS) dan *sabotage*;

c. Pencerobohan (*Intrusion*)

Mengguna dan mengubahsuai ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak. Ia termasuk capaian tanpa kebenaran, pencerobohan laman web, melakukan kerosakan kepada sistem (*system tampering*), pindaan data (modification of data) dan pindaan kepada konfigurasi sistem;

d. Pemalsuan (*Forgery*)

Pemalsuan dan penyamaran identiti dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/ espionage*) dan penipuan (*hoaxe*s);

e. Spam

Pesanan yang dihantar namun tidak dikehendaki oleh penerimanya yang mana sekiranya dihantar secara berulang-kali dalam satu masa boleh menyebabkan kesesakan rangkaian dan tindak balas menjadi perlahan;

f. Malicious Code

Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya;

g. Harrassment/Threats

Gangguan dan ancaman melalui pelbagai cara samada medium komunikasi atau isyarat yang mempunyai motif untuk menyebabkan sebarang kehilangan atau kerosakan;

h. Attempts/Hack Threats/Information Gathering

Percubaaan (sama ada gagal atau berjaya) untuk mengakses sistem atau data tanpa kebenaran termasuk *spoofing, phishing, probing, war driving* dan *scanning*; dan

i. Kehilangan Fizikal (*Physical Loss*)

Kehilangan capaian dan kegunaan disebabkan kerosakan, kecurian dan kebakaran ke atas aset ICT yang berpunca dari aktiviti pencerobohan.

1.4 Penafian

UiTM menyediakan saluran elektronik untuk penyaluran maklumat dan bukannya penerbit. Oleh ICT, melainkan ia adalah penerbitan rasmi universiti, UiTM tidak bertanggungjawab terhadap bahan atau komunikasi yang dibuat oleh satu atau lebih individu melalui *World Wide Web*, internet, atau rangkaian sosial; perkongsian fail; atau pengiriman melalui e-mel; atau sebarang tindakan yang dibuat

melalui persekitaran maya. Walau bagaimanapun, dalam keadaan tertentu, Universiti boleh bertindak terhadap aduan mengenai bahan atau komunikasi tersebut.

UiTM berhak memasang perisian atau perkakasan penapisan e-mel dan virus (*e-mail filter* and anti virus) yang difikirkan sesuai. Ianya digunakan untuk mencegah, menapis, menyekat atau menghapuskan mana-mana e-mel yang disyaki mengandungi virus atau berunsur spamming daripada memasuki atau keluar dari server, stesen kerja atau rangkaian UiTM;

UiTM tidak bertanggungjawab terhadap sebarang kerosakan, kehilangan atau sebarang kesan lain kepada maklumat, aplikasi, *mailbox* atau fail yang disimpan oleh pengguna di dalam stesen kerja atau server akibat daripada penggunaan perkhidmatan rangkaian UiTM;

a. UiTM berhak memasang perisian atau perkakasan penapisan e-mel dan virus (e-mail filter and anti virus) yang difikirkan sesuai. Ianya digunakan untuk mencegah, menapis, menyekat atau menghapuskan mana-mana e-mel yang disyaki mengandungi virus atau berunsur spamming daripada memasuki atau keluar dari server, stesen kerja atau rangkaian UiTM;

b. UiTM tidak bertanggungjawab terhadap sebarang kerosakan, kehilangan atau sebarang kesan lain kepada maklumat, aplikasi, mailbox atau fail yang disimpan oleh pengguna di dalam stesen kerja atau server akibat daripada penggunaan perkhidmatan rangkaian UiTM;

c. UiTM tidak bertanggungjawab terhadap pengguna yang menjadi penghantar (sender) atau penerima (receiver) kepada sebarang e-mel yang berunsur spamming atau penyebaran e-mel dengan kandungan tidak beretika;

d. Bagi kes kerosakan e-mel, pentadbir e-mel hanya bertanggungjawab untuk memulihkan kembali (restore) maklumat akaun pengguna dan bukannya kandungan atau mailbox pengguna;

e. Fail yang mempunyai extension .exe, .cmd, .bat, .hta, js, .vb, .mov, .avi, .mp3, .mpeg, .mpg, .wav, .rm, .ram, .rmx, .asf, .wmf, .wmp, .wsf, . wsh, .shs, .scr, .htm, .html, .qsm, .Ink, .wab, .dbx, .rar, .eml dan .zip dan fail yang mempunyai

kapasiti melebihi empat (4) megabyte akan dibuang secara automatik tanpa sebarang notis sekiranya dijumpai dalam tapak yang dihoskan; dan

f. Pentadbir e-mel, dengan kelulusan UiTM, berhak memeriksa dan melihat isi kandungan e-mel dan ruang storan pengguna dari semasa ke semasa atas keperluan audit dan keselamatan.

1.5 Akta Universiti

Akta Universiti Teknologi MARA 1976 (Akta 173).

1.6 Dasar ICT

Dasar ICT adalah suatu ketetapan secara dasar yang telah dipersetujui secara rasmi sebagai asas untuk membuat dan melaksanakan keputusan berkaitan dengan teknologi maklumat dan komunikasi (ICT).

1.7 Prosedur

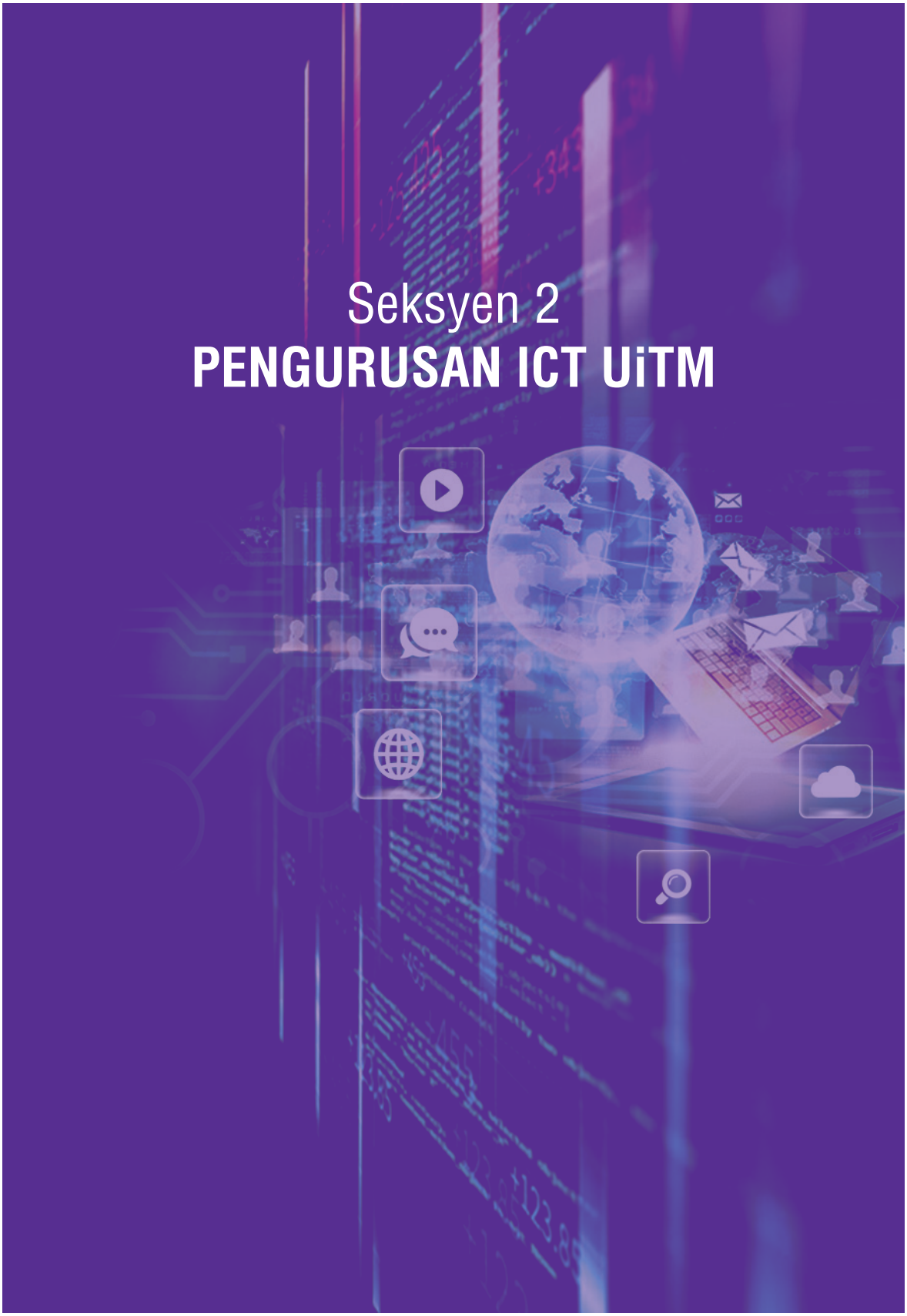
Prosedur merupakan aturan atau tatacara menjalankan sesuatu aktiviti/tugas/kerja bagi memastikan tugas ICT dijalankan dengan betul dan mengikut dasar dan peraturan yang telah ditetapkan.

1.8 Garis Panduan

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

Seksyen 2

PENGURUSAN ICT UiTM



2. PENGURUSAN ICT UiTM

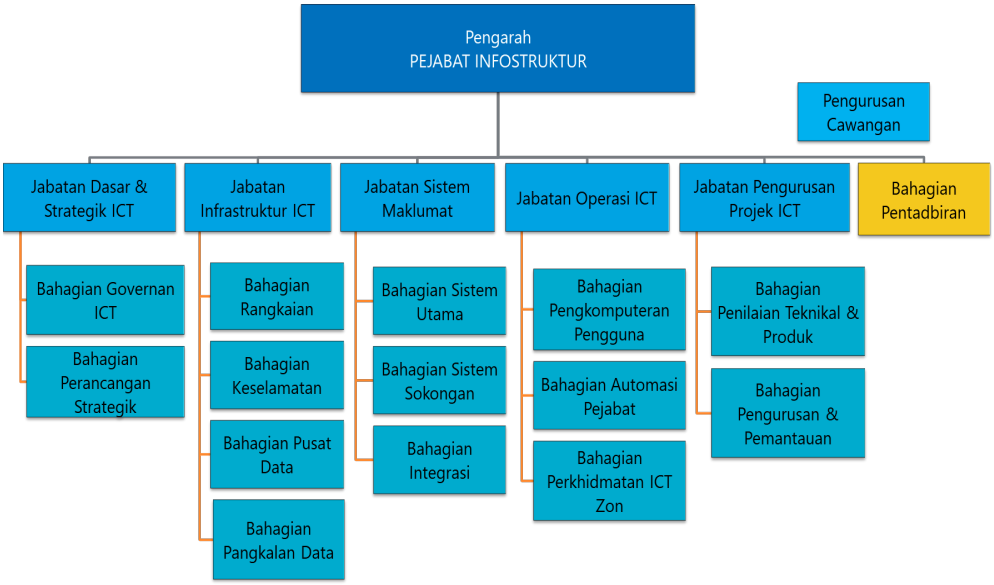
2.1 Tujuan

Menerangkan terma rujukan CIO yang bertanggungjawab menetapkan Dasar Teknologi Maklumat dan Komunikasi (ICT) dan memantau keberkesanan pelaksanaan ICT di UiTM; dan

Menerangkan skop dan fungsi Pengurusan ICT di dalam melaksanakan pengurusan dan pembangunan ICT di UiTM.

2.2 Carta Organisasi ICT UiTM

Carta organisasi Pengurusan ICT seperti Gambar Rajah 2-1 berikut menunjukkan hasil penstrukturan semula organisasi ICT UiTM pada Disember tahun 2016.



Gambar Rajah 2-1: Carta Organisasi ICT Semasa (Pengurusan ICT)

2.3 Naib Canselor

Naib Canselor hendaklah bertindak sebagai Ketua Eksekutif, pentadbir dan pegawai akademik universiti. Naib Canselor hendaklah memastikan semua peraturan dipatuhi dan dikuatkuasakan.

Peranan dan tanggungjawab Naib Canselor UiTM adalah seperti berikut:

a. Memastikan pelaksanaan ICT Universiti berlandaskan Pelan Strategik ICT UiTM;

b. Memastikan semua pengguna mematuhi Dasar ICT UiTM terkini;

c. Merancang semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) agar mencukupi;

d. Merancang penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan; dan

e. Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar ICT UiTM.

2.4 Ketua Pegawai Maklumat (CIO)

Ketua Pegawai Maklumat (CIO) UITM dilantik selaras dengan arahan Ketua Setiausaha Negara rujukan PM(S)18114 Jld. 13(74) bertarikh 22 Mac 2000. Peranan dan tanggungjawab CIO digariskan dalam Buku Panduan Ketua Pegawai Maklumat (CIO) Sektor Awam terkini yang dikeluarkan oleh MAMPU.

Ketua Pegawai Maklumat bertanggungjawab melaksanakan kajian kebolehlaksanaan untuk pelaksanaan teknologi baharu dan memberi pengesyoran bagi pelaksanaan tersebut.

2.5 Pegawai Maklumat Bersekutu (*Associate* CIO)

Pegawai Maklumat Bersekutu merupakan wakil CIO di peringkat pengurusan ICT UiTM bagi menjalankan tadbir urus ICT dan penyampaian maklumat berdasarkan arahan CIO serta berpandukan dasar dan garis panduan yang telah ditetapkan. *Associate* CIO berperanan seperti CIO tetapi dalam skop pengurusan ICT UiTM.

2.6 Pengarah Pengurusan ICT

Pengarah Pengurusan ICT merupakan ketua yang bertanggungjawab menyediakan perkhidmatan ICT kepada UiTM. Pengarah Pengurusan ICT juga memegang peranan sebagai Pegawai Maklumat Bersekutu (*Associate* CIO) dan memastikan pematuhan kepada Dasar ICT UiTM.

2.7 Pegawai Keselamatan ICT (ICTSO)

Pegawai Keselamatan ICT ialah pegawai yang dilantik bagi memastikan Dasar keselamatan ICT UiTM dipatuhi. Beliau bertanggungjawab menjalankan program-program keselamatan ICT termasuk memaklumkan tindakan pencegahan yang perlu dilakukan oleh pengguna ICT serta melaporkan insiden keselamatan ICT kepada CIO dan Pasukan Tindak balas Insiden Keselamatan ICT (GCERT) MAMPU.

2.8 Pegawai Gred Perjawatan Skim Teknologi Maklumat (Skim F)

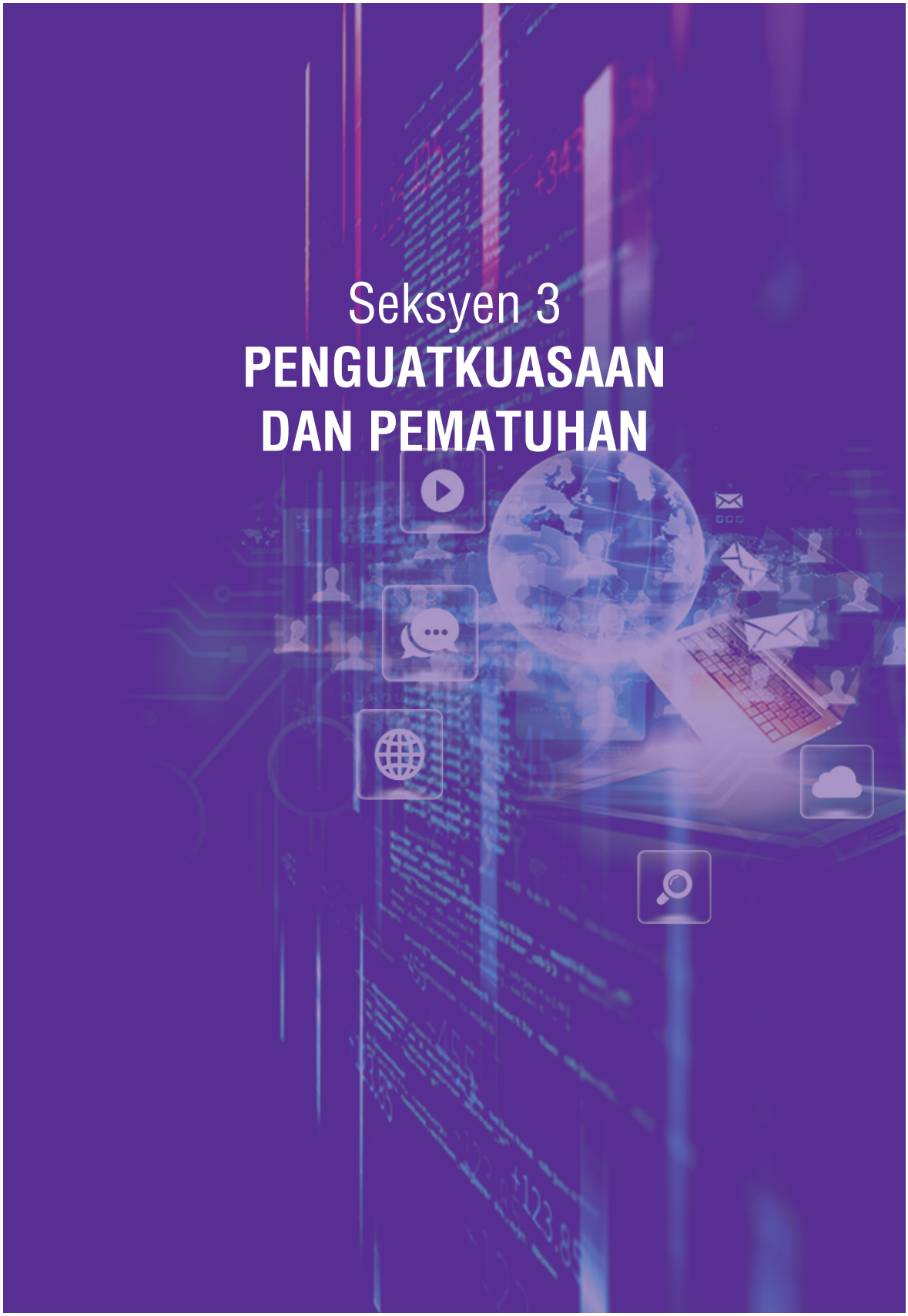
Pegawai yang bertanggungjawab untuk membangun, mengurus, mengawal, memantau dan menyelenggara perjalanan dan fungsi sesuatu sistem atau kemudahan ICT.

2.9 Pemegang Taruh

Pihak yang berkepentingan terhadap UiTM.

2.10 Pengguna

Pengguna terdiri daripada staf, pelajar, serta pihak ketiga dan mana-mana pihak yang mempunyai ikatan kontrak atau hubungan, sama ada secara bertulis atau tidak, dengan UiTM, yang menggunakan kemudahan ICT universiti.



Seksyen 3
PENGUATKUASAAN DAN PEMATUHAN

3. PENGUATKUASAAN DAN PEMATUHAN

3.1 Pematuhan Dan Keperluan Perundangan

3.1.1 Pematuhan Dasar

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

3.1.2 Pelanggaran Dasar

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

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

c. Pelanggaran dasar ini boleh mengakibatkan tindakan tatatertib, surcaj dan/atau tuntutan sivil di ambil terhadap staf, pelajar serta pihak ketiga. Mereka juga boleh dihalang atau digantung daripada menggunakan atau mendapatkan kemudahan ICT yang disediakan.

d. Sebarang aduan tentang pelanggaran Dasar ICT hendaklah dibuat secara bertulis kepada CIO atau *Associate* CIO. *Associate* CIO boleh melantik satu Jawatankuasa Siasatan untuk meneliti laporan dan menentukan sama ada siasatan terperinci perlu dilakukan. Dalam lantikan tersebut, CIO atau *Associate* CIO akan melantik sekurang-kurangnya dua orang penyiasat teknikal untuk meneliti laporan dan menjalankan siasatan serta membuat keputusan sama

ada siasatan yang lebih terperinci perlu dilaksanakan sebelum sesuatu tindakan di ambil.

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

3.1.3 Keperluan Perundangan

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

1. Akta Badan-badan Berkanun (Tatatertib dan Surcaj) 2000 (Akta 605);
2. Akta Institusi-institusi Pelajaran (Tatatertib) 1976 (Akta 174);
3. Akta Universiti Teknologi MARA 1976 (Akta 173);
4. Akta Rahsia Rasmi 1972 (Akta 88);
5. Akta Komunikasi dan Multimedia 1998 (Akta 588);
6. Akta Jenayah Komputer 1997 (Akta 563);
7. Akta Perlindungan Data Peribadi 2010 (Akta 709);
8. Akta Tandatangan Digital 1997 (Akta 562);
9. Akta Mesin Cetak dan Penerbitan 1984 (Akta301);
10. Akta Hak Cipta 1987 (Akta 332);
11. Akta Tele-Perubatan 1997 (Akta 564);
12. Akta Aktiviti Kerajaan Elektronik 2007 (Akta 680);
13. Akta Universiti dan Kolej Universiti 1971 (Akta 30) Pindaan 2009 [A1342];
14. Surat Arahan MAMPU (MAMPU.BDPICT – 7/22(23) bertarikh 4 Janurari 2010) – Garis Panduan Transisi Protokol Internet Versi 6 (IPV6) Sektor Awam;
15. Surat Pekeliling Am Bil. 1 Tahun 2008: Garis Panduan Mengenai Tatacara Memohon Kelulusan Teknikal Projek ICT Agensi Kerajaan yang dikeluarkan oleh MAMPU;

16. Arahan Teknologi Maklumat (2007) yang dikeluarkan oleh MAMPU;
17. Pekeliling Am Bil.4 Tahun 2006: Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;
18. Pekeliling Am Bil.6 Tahun 2005: Garis Panduan Melaksanakan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
19. Pekeliling Am Bil.1 Tahun 2003: Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi Kerajaan;
20. Garis Panduan Pengurusan Keselamatan ICT yang dikeluarkan oleh MAMPU, Januari 2002;
21. Pekeliling Am Bil.1 Tahun 2001: Mekanisme Pelaporan Insiden Keselamatan ICT (ICT) yang dikeluarkan oleh MAMPU;
22. Pekeliling Am Bil. 3 Tahun 2000: Dasar Keselamatan ICT Kerajaan yang dikeluarkan oleh MAMPU;
23. Pekeliling Am Bil.1 Tahun 2000: Garis Panduan Malaysian Civil Service Link (MCSL) dan Laman Web Kerajaan yang dikeluarkan oleh MAMPU;
24. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
25. Pekeliling Am Bil. 6 Tahun 1999: Garis Panduan Pelaksanaan Perkongsian Pintar Antara Agensi-agensi Kerajaan Dalam Bidang Teknologi Maklumat yang dikeluarkan oleh MAMPU;
26. Pekeliling Am Bil. 2 Tahun 1999: Penubuhan Jawatankuasa ICT dan Internet Kerajaan (JITIK) yang dikeluarkan oleh MAMPU;
27. Pekeliling ICT UiTM;
28. Dasar Keselamatan ICT UiTM; dan
29. Akta, Pekeliling, Arahan, Garis Panduan dan Surat Pekeliling yang dikeluarkan dari semasa ke semasa.

Seksyen 4

PENGURUSAN DAN PENYELENGGARAAN DASAR ICT

4. PENGURUSAN DAN PENYELENGGARAAN DASAR ICT

4.1 Pengurusan Dasar ICT

Pengurusan ICT bertanggungjawab mengurus dasar ICT berdasarkan keperluan semasa dengan dibantu oleh Ketua Pegawai Maklumat (CIO), *Associate* CIO, Pegawai Keselamatan ICT (ICTSO) dan lain-lain pegawai yang dilantik.

4.2 Penyebaran Dasar

Dasar ini perlu disebarkan kepada semua pengguna kemudahan dan aset ICT Universiti termasuk staf, pelajar serta pihak ketiga.

4.3 Penyelenggaraan Dasar

Dasar ICT UiTM tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur berhubung dengan penyelenggaraan Dasar ICT UiTM:

a. Kenal pasti dan tentukan perubahan yang diperlukan;

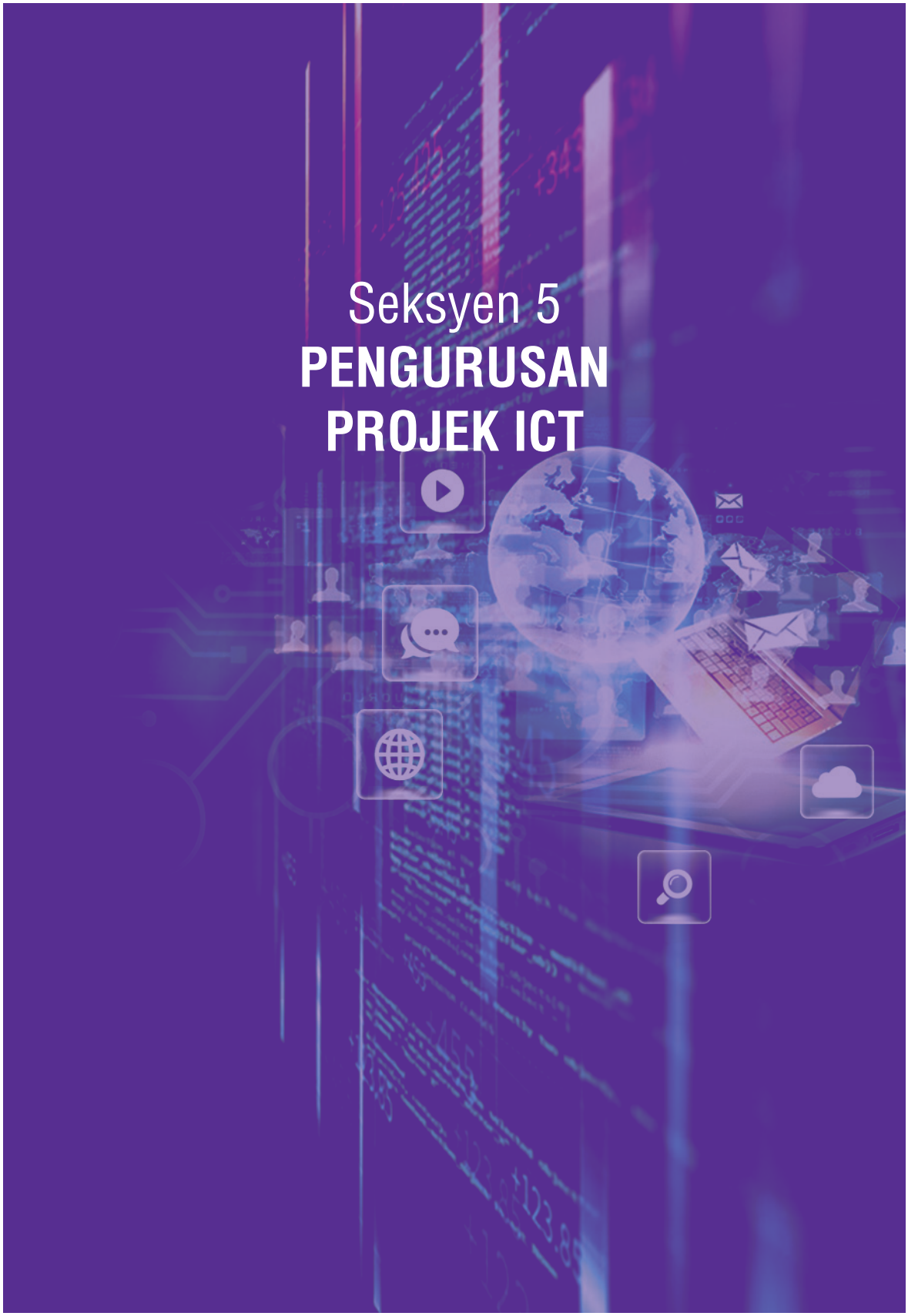
b. Kemuka cadangan pindaan secara bertulis kepada CIO untuk pembentangan dan persetujuan pihak berwajib;

c. Perubahan yang diluluskan mesti dimaklumkan kepada semua pengguna; dan

d. Dasar ini hendaklah dikaji semula sekurang-kurangnya dua tahun sekali atau mengikut keperluan semasa.

4.4 Pemakaian

Dasar ICT UiTM terpakai kepada semua pengguna ICT Universiti tanpa sebarang pengecualian.



Seksyen 5

PENGURUSAN PROJEK ICT

5. PENGURUSAN PROJEK ICT

5.1 Tujuan

Tujuan dasar ini ialah bagi memastikan pelaksanaan pengurusan projek ICT mengikut perancangan yang telah ditetapkan.

5.2 Penggunaan

Pengunaan Dasar Pengurusan Projek ICT hendaklah berasaskan kepada dokumen—"Metodologi PPrISA: Panduan Pengurusan Projek ICT Sektor Awam" daripada MAMPU.

5.3 Pelaksanaan

Pelaksanaan Dasar Pengurusan Projek ICT hendaklah berdasarkan kepada Metodologi PPrISA: Panduan Pengurusan Projek ICT Sektor Awam dan SOP yang telah ditetapkan di dalam MPK Pengurusan ICT Universiti.

Seksyen 6

PERANCANGAN STRATEGIK ICT

6. PERANCANGAN STRATEGIK ICT

6.1 Tujuan

Tujuan dasar ini ialah bagi memastikan kaedah pelaksanaan perancangan strategik ICT Universiti mengikut kaedah yang telah ditetapkan oleh Kerajaan.

6.2 Penggunaan

Pengunaan Pelan Perancangan Strategik ICT Universiti hendaklah berasaskan kepada dokumen Garis Panduan Perancangan Strategik ICT daripada MAMPU.

6.3 Pelaksanaan

Pelaksanaan Pelan Perancangan Strategik ICT hendaklah berdasarkan kepada panduan pelaksanaan perancangan strategik ICT dan SOP yang telah ditetapkan di dalam MPK Pengurusan ICT Universiti.

Seksyen 7

KESELAMATAN ICT

7. KESELAMATAN ICT

7.1 Tujuan

Tujuan dasar ini ialah bagi memastikan kaedah pelaksanaan keselamatan ICT Universiti mengikut kaedah yang telah ditetapkan oleh Kerajaan.

7.2 Penggunaan

Pengunaan dasar keselamatan ICT Universiti hendaklah berasaskan kepada dokumen Dasar Keselamatan ICT UiTM.

7.3 Pelaksanaan

Pelaksanaan dasar keselamatan ICT hendaklah berdasarkan kepada dokumen Dasar Keselamatan ICT UiTM dan SOP yang telah ditetapkan di dalam MPK Pengurusan ICT Universiti.

Seksyen 8

PENGURUSAN DAN PENGGUNAAN INFRASTRUKTUR ICT

8. PENGURUSAN DAN PENGGUNAAN INFRASTRUKTUR ICT

8.1 Tujuan

Tujuan dasar ini adalah untuk menetapkan peraturan dan tanggungjawab mengenai perkara-perkara yang berhubung dengan infrastruktur ICT universiti supaya dapat diuruskan dengan baik dan teratur.

8.2 Pengurusan Rangkaian

Pengurusan rangkaian melaksanakan perancangan, perolehan, penyediaan perkhidmatan, pengoperasian, penyelenggaran perkakasan serta perisian rangkaian untuk perkhidmatan rangkaian UiTM. Rangkaian UiTM merangkumi rangkaian *wired* dan *wireless* yang disediakan oleh UiTM atau pihak-pihak lain.

8.2.1 Kawalan Keselamatan Infrastruktur Rangkaian

Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;

b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran, habuk dan haiwan perosak;

c. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;

d. Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi;

e. *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Rangkaian Pengurusan ICT.

f. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah UiTM;

g. Semua perisian *sniffer* atau *network analyzer* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;

h. Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat UiTM;

i. Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti capaian kepada laman sesawang yang dilarang;

j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan UiTM adalah tidak dibenarkan;

k. Semua pengguna hanya dibenarkan menggunakan rangkaian UiTM sahaja dan penggunaan *modem/ router/switch*/*wireless access point* atau sebarang perkakasan rangkaian bebas adalah dilarang sama sekali tanpa mendapat kebenaran bertulis dari ICTSO; dan

l. Kemudahan bagi *wireless LAN* perlu dipastikan kawalan keselamatan.

3.1.1 Internet atau Intranet

a. UiTM berhak menyediakan dan memasang perisian penapisan kandungan internet dan intranet yang dilayari;

b. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Bahagian/Jabatan;

c. Bahan yang diperolehi dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendaklah dinyatakan;

d. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Bahagian/Jabatan sebelum dimuat naik ke Internet;

e. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang patuh undang-undang hak cipta;

f. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan; dan

g. UiTM berhak menapis, menghalang dan menegah penggunaan mana-mana laman web yang di anggap tidak sesuai.

8.2.3 Kebolehcapaian Pengguna (*User Accessibility*)

8.2.3.1 Rangkaian Setempat (*Local Area Network*)

a. Hanya kakitangan dan pelajar universiti dibenarkan membuat penyambungan ke rangkaian universiti;

b. Pengguna luar perlu mendapatkan kebenaran Pengurusan ICT sebelum membuat capaian ke rangkaian UiTM;

c. Pengguna yang disahkan sahaja dibenarkan membuat capaian ke rangkaian universiti;

d. Penggunaan perisian pengintip (*sniffer*) atau penganalisis rangkaian (*network analyzer*) tidak dibenarkan; dan

e. Status komputer (*IP Address* dan lokasi port) hendaklah disemak setiap tahun oleh Pengurusan ICT untuk memastikan komputer didaftarkan dan berfungsi dengan baik.

8.2.3.2 Rangkaian tanpa wayar (WIFI)

a. Hanya kakitangan dan pelajar UiTM dibenarkan menggunakan rangkaian tanpa wayar UiTM;

b. Pengguna luar perlu mendapatkan kebenaran UiTM secara *online* sebelum menggunakan rangkaian tanpa wayar;

c. Pengguna yang disahkan sahaja dibenarkan membuat capaian ke Rangkaian UiTM; dan

d. Penggunaan perisian pengintip (*sniffer*) atau penganalisis rangkaian (*network analyzer*) tidak dibenarkan.

8.2.4 Pengurusan Alamat IP

Sistem pemberian *IP address* bagi peranti elektronik peribadi adalah menggunakan teknologi DHCP (*Dynamic Host Configuration Protocol*). *IP address* tetap diberikan bagi *server*, peralatan rangkaian dan perkakasan yang dikongsi seperti alat cetak.

8.2.5 Sambungan Rangkaian

Pemasangan sistem rangkaian hanya boleh dibuat oleh dan dengan kebenaran dan pemantauan Pengurusan ICT.

8.2.6 *Virtual Private Net*work (VPN)

Hak akses melalui VPN ditentukan oleh Pengurusan ICT berdasarkan permohonan dan justifikasi.

8.2.7 *Domain* dan *Sub-Domain*

Domain rasmi UiTM ialah www.uitm.edu.my.

Penggunaan *domain* dan *sub-domain* hanyalah untuk kegunaan rasmi UiTM dan perlu menggunakan *domain* yang telah ditetapkan oleh UiTM.

Sub-domain yang ingin dipaparkan perlu mendapatkan kelulusan Pengurusan ICT.

8.3 Mel Elektronik

Pengguna e-mel universiti mesti mematuhi dasar dan Garis Panduan Pengurusan ICT Universiti, bertanggungjawab untuk menjaga integriti sumber dan mematuhi keperluan etika penggunaan e-mel dan internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"–dan mana-mana undang-undang bertulis yang berkuat kuasa.

Perkara-perkara yang perlu dipatuhi dalam pengendalian e-mel adalah seperti berikut:

a. Pengguna individu tidak dibenarkan memohon dan atau memiliki lebih daripada satu (1) akaun e-mel atau alamat e-mel Universiti pada satu-satu masa pada pelayan yang didaftarkan;

b. Setiap alamat e-mel yang disediakan adalah untuk kegunaan pemilik e-mel dan tidak boleh digunakan oleh pihak lain sama ada dengan kebenaran atau tanpa kebenaran.

c. Pengguna disarankan menukar kata laluan akaun e-mel secara berkala. Penggunaan kata laluan yang sukar diramal oleh penggodam adalah digalakkan;

d. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul;

e. Pengguna bertanggungjawab ke atas pengemaskinian dan penggunaan mailbox masing-masing dan bertanggungjawab ke atas *mailbox* masing-masing untuk memastikan ruang storan mencukupi;

f. Pengguna perlu membuat salinan sandar *(backup/archive)* terhadap e-mel masing-masing;

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

h. Kandungan e-mel perlu mematuhi undang-undang yang berkuatkuasa dan kod kandungan Komunikasi dan Multimedia Malaysia. Pihak Pengurusan ICT berhak untuk menyekat akses e-mel atas arahan Pengurusan Atasan Universiti;

i. Pengguna hendaklah log keluar atau tutup *browser* yang digunakan setelah sesi capaian akaun e-mel selesai bagi mengelakkan akaun e-mel diceroboh; dan

j. Kemudahan e-mel akan ditamatkan 6 bulan selepas staf tamat perkhidmatan.

Dasar Mel Elektronik ini perlu dibaca bersama dengan Dasar Keselamatan ICT.

8.4 Telesidang dan Live Streaming

Pengguna Telesidang dan *Live Streaming* mesti mematuhi dasar dan Garis Panduan Pengurusan ICT Universiti, dan bertanggungjawab untuk menjaga integriti sumber dan bahan telesidang.

Perkara-perkara yang perlu dipatuhi dalam pengendalian perkhidmatan telesidang dan *live streaming* adalah seperti berikut:

8.4.1 Telesidang

a. Setiap PTJ perlu melantik seorang pegawai yang terlatih untuk mengurus dan mengendalikan sesi dan peralatan telesidang;

b. Setiap PTJ yang ingin menggunakan perkhidmatan telesidang perlu membuat permohonan dan memaklumkan kepada pengurusan ICT sebelum setiap sesi telesidang dibuat;

c. Pengurusan ICT perlu menyediakan jalur lebar khusus untuk perkhidmatan telesidang bagi menjamin kualiti perkhidmatan;

d. Setiap PTJ perlu memastikan sistem telesidang yang diperolehi sesuai (*compatible*) dengan sistem telesidang universiti;

e. Agensi luar dan PTJ yang tidak mempunyai kelengkapan peralatan telesidang perlu menggunakan perisian yang disediakan; dan

f. Kandungan pada semua bahan telesidang perlu mematuhi Undang-undang yang berkuatkuasa dan kod kandungan Komunikasi dan Multimedia Malaysia. Pihak Pengurusan ICT berhak untuk menamatkan sesi atas arahan Pengurusan Atasan Universiti.

8.4.2 Live Streaming

a. Setiap PTJ yang ingin menggunakan perkhidmatan *live streaming* perlu membuat permohonan dan memaklumkan kepada pengurusan ICT sebelum setiap sesi *live streaming* dibuat;

b. Pengurusan ICT perlu menyediakan jalur lebar khusus untuk perkhidmatan *live streaming* bagi menjamin kualiti perkhidmatan;

c. Hebahan masa dan pautan *live streaming* bagi acara universiti perlu dibuat oleh PTJ yang dipertanggungjawabkan; dan

d. Kandungan pada semua bahan *live streaming* perlu mematuhi undang-undang yang berkuatkuasa dan kod kandungan Komunikasi dan Multimedia Malaysia. Pihak Pengurusan ICT berhak untuk menamatkan sesi atas arahan Pengurusan Atasan Universiti.

8.5 Laman Sesawang

Pemilik laman sesawang mesti mematuhi dasar dan Garis Panduan Pengurusan ICT Universiti, bertanggungjawab untuk menjaga integriti sumber dan bahan laman sesawang.

Perkara-perkara yang perlu dipatuhi dalam pengendalian laman sesawang adalah seperti berikut:

a. Universiti menyediakan tapak atau ruang, untuk laman sesawang rasmi PTJ;

b. Hanya laman sesawang rasmi PTJ yang boleh dipautkan dalam laman sesawang rasmi Universiti;

c. Semua laman sesawang rasmi PTJ mesti mempunyai pautan dengan laman utama UITM;

d. Kemudahan hos yang diberikan hanya untuk pembangunan laman sesawang sahaja. Pihak Universiti berhak untuk menarik balik kemudahan hos jika didapati sebaliknya;

e. Pemilik laman sesawang bertanggungjawab sepenuhnya terhadap semua kandungan. Pihak Universiti tidak akan bertanggungjawab terhadap kandungan dan sebarang penyalahgunaan hakcipta yang dilakukan oleh pemilik laman web;

f. Pihak Universiti berhak menentukan perisian pembangunan laman sesawang bagi tujuan penggunaan dan keselamatan;

g. Keselamatan maklumat dan penyiaran adalah di bawah tanggungjawab PTJ dan perlu mengambil kira aspek keselamatan daripada pencerobohan pihak luar;

h. Kandungan pada semua bahan laman sesawang perlu mematuhi Undang-undang yang berkuatkuasa dan kod kandungan Komunikasi dan Multimedia Malaysia. Pihak Pengurusan ICT berhak untuk menyekat akses laman sesawang atas arahan Pihak Pengurusan Universiti;

i. Aktiviti *spamming* yang berpunca dairpada laman sesawang jabatan tidak dibenarkan. Pihak Pengurusan ICT berhak untuk menyekat akses kepada laman sesawang tersebut sehingga isu selesai;

j. Pemilik laman sesawang perlu membuat salinan sandar *(backup)* terhadap laman sesawang masing-masing;

k. Pengurusan ICT tidak bertanggungjawab ke atas sebarang kerosakan atau kehilangan maklumat pada laman sesawang sehingga menyebabkan berlakunya kegagalan capaian maklumat;

l. Kemudahan laman sesawang individu akan ditamatkan 6 bulan selepas staf tamat perkhidmatan; dan

m. Dasar laman sesawang ini perlu dibaca bersama dengan Dasar Keselamatan ICT UiTM dan Dasar Pengurusan Laman Sesawang Universiti.

8.6 Pengurusan Makmal Komputer

a. Pengurusan makmal komputer adalah tertakluk kepada aktiviti UiTM atau aktiviti yang dibenarkan oleh PTJ sahaja; dan

b. Pengurusan makmal komputer hendaklah merujuk kepada Garis Panduan Pengurusan ICT UITM.

8.7 Pusat Data Pengkomputeran Awan (*Cloud Computing*)

Memastikan keselamatan penggunaan pengkomputeran awan di kalangan warga UiTM.

Pengkomputeran Awan adalah perkhidmatan sumber-sumber ICT yang dimayakan tanpa penyediaan infrastruktur di pihak pengguna.

Perkara-perkara yang perlu diberi perhatian adalah:

a. Skop dasar ini merangkumi public could, private cloud dan hybrid cloud;

b. Penggunaan dan penyediaan perkhidmatan pengkomputeran awan perlu mendapat kelulusan daripada Jawatankuasa Pemandu ICT UiTM;

c. Pengkomputeran awan hendaklah dipastikan selamat bagi menjamin keselamatan maklumat universiti; dan

d. Pengurusan dan keselamatan pelaksanaan pengkomputeran awan adalah dipertanggungjawabkan kepada pengguna sepenuhnya.

8.8 Pengurusan Masuk ke Pusat Data

Kemasukan ke Pusat Data dihadkan kepada staf yang dibenarkan mengikut klasifikasi yang ditetapkan seperti berikut:

a. *Controlling Access* - Staf ICT yang bertugas di Pusat Data;

b. *Escorted Access* – Staf atau vendor yang perlu memasuki Pusat Data untuk menjalankan tugas perlu diiringi oleh staf Pusat Data; dan

c. Lawatan Pusat Data – Lawatan ke Pusat Data tidak dibenarkan sama sekali melainkan mendapat kebenaran Pengarah Pengurusan ICT.

Penyataan lengkap boleh dirujuk kepada Dasar Keselamatan ICT UiTM (Bidang 05 Keselamatan Fizikal dan Persekitaran).

8.9 Pengurusan *Backup* dan *Recovery*

a. Pentadbir sistem mesti menentukan keperluan backup sistem di bawah pengurusan masing-masing dari segi:

   i. Kekerapan backup.

   ii. Jenis backup (*full* atau *incremental*)

   iii. Tempoh pengekalan backup (*retention period*).

   iv. Bilangan generasi *backup.*

b. Pentadbir sistem mesti menjalankan ujian *restor*e bagi memastikan integriti *backup*.

Penyataan lengkap boleh dirujuk kepada Dasar Keselamatan ICT UiTM (Bidang 06 Pengurusan Operasi dan Komunikasi).

8.10 Pengurusan *Server*

a. Pengurus Pusat Data mesti menyimpan maklumat terkini *server* (fizikal atau *virtual*) di bawah pengurusannya yang merangkumi:

   i. Sistem operasi.

   ii. Lesen perisian yang beroperasi pada *server*.

   iii. Sistem aplikasi yang beroperasi pada *server.*

   iv. Pentadbir sistem yang beroperasi pada *serve*r.

   v. Prosedur kecemasan.

   vi. Pelan *backup* dan *recovery server*.

   vii. Pelan pemulihan bencana *server.*

b. Pengurus Pusat Data dan Pentadbir Sistem bertanggungjawab memastikan pengurusan penyelenggaraan perkakasan ICT di Pusat Data & Pusat Pemulihan Bencana dilakukan;

c. Penempatan server di Pusat Data mestilah mendapat kelulusan Pengurus Pusat Data. Penyataan lengkap boleh dirujuk kepada Dasar Keselamatan ICT UiTM(Bidang 06 Pengurusan Operasi dan Komunikasi); dan

d. Kawalan fizikal pusat data dan pusat pemulihan bencana mesti mengambil perhatian terhadap perkara berikut:

   i. Pusat data dan pusat pemulihan bencana ditempatkan di tempat yang bebas daripada risiko bencana seperti banjir, gegaran, kekotoran, kebakaran dan sebagainya.

   ii. Suhu hendaklah terkawal di dalam had yang ditetapkan dan mempunyai kitaran udara yang baik.

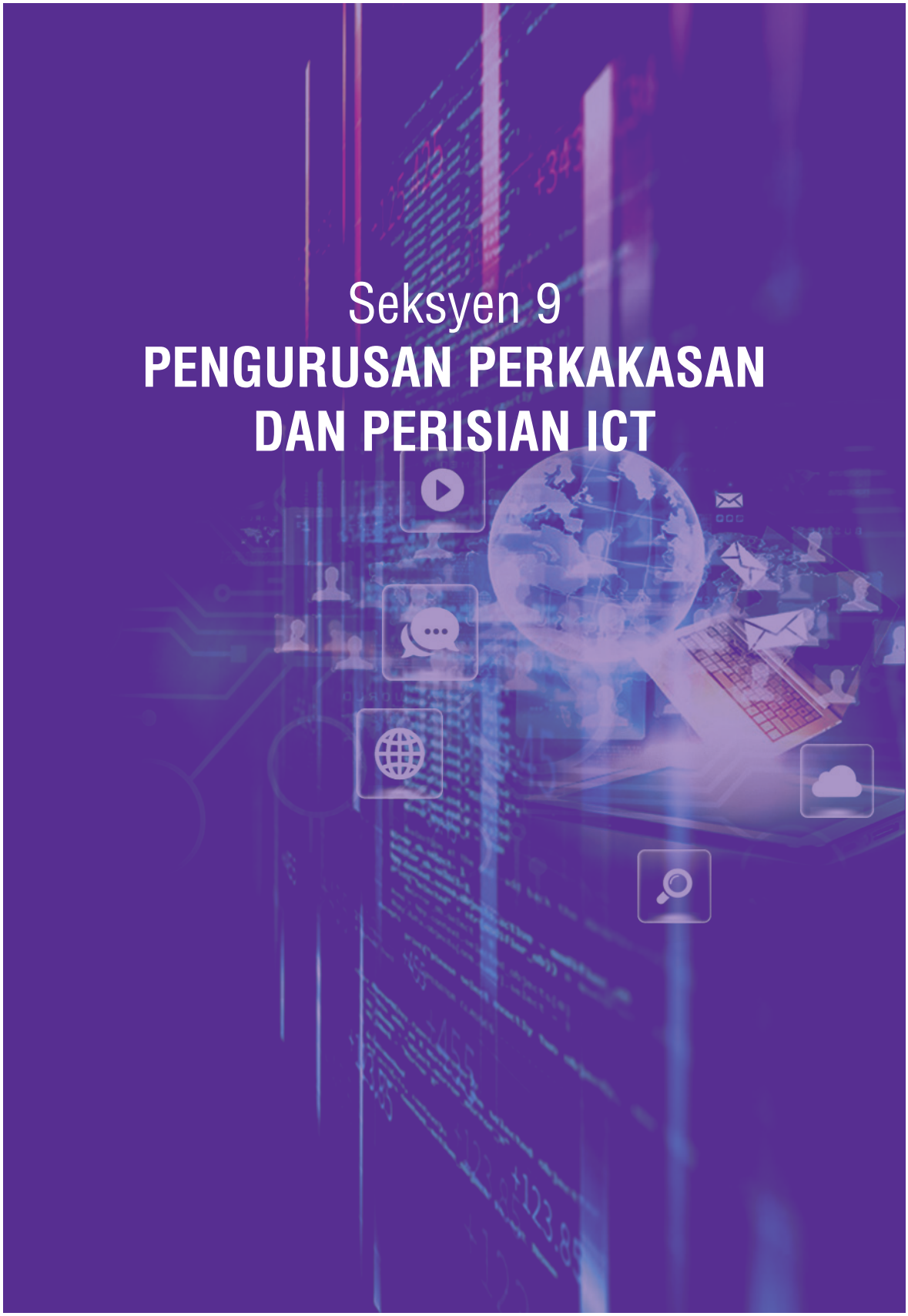
   iii. Memasang *Uninterruptible Power Supply* (UPS) dengan minimum 15 minit masa beroperasi jika terputus bekalan elektrik.

   iv. Menerima bekalan elektrik berkualiti (bekalan elektrik yang bebas daripada *voltage sag, voltage swell* dan *transient overvoltages*).

v. Memasang *generator* sebagai alat bantuan (*backup*).

Pengurusan Pusat Data hendaklah merujuk kepada Garis Panduan Pengurusan Pusat Data oleh MAMPU.

Penyataan lengkap boleh dirujuk kepada Dasar Keselamatan ICT UiTM (Bidang 06 Pengurusan Operasi dan Komunikasi).



Seksyen 9

PENGURUSAN PERKAKASAN DAN PERISIAN ICT

9. PENGURUSAN PERKAKASAN DAN PERISIAN ICT

9.1 Tujuan

Tujuan dasar ini ialah bagi menentukan tanggungjawab pengguna dan pihak UiTM mengenai perkara yang berhubung dengan perkakasan dan perisian ICT UiTM supaya dapat diuruskan dengan lebih baik dan teratur.

9.2 Perkakasan ICT

Perkakasan ICT adalah semua perkakasan yang digunakan atau berada dalam simpanan pengguna merangkumi komputer meja (PC), komputer riba (*notebook*), pencetak (*printe*r), *tablet PC* dan pengimbas (*scanne*r), dan diperolehi melalui proses perolehan universiti.

Perkakasan ICT yang dibeli hendaklah mempunyai tempoh jaminan minimum tiga (3) tahun daripada pembekal utama (*manufacturer warranty*).

9.2.1 Hak Pemilikan

a. Semua perkakasan ICT yang diperolehi oleh UiTM menggunakan peruntukan kewangan UiTM atau melalui perjanjian kerjasama atau penyelidikan adalah hak milik UiTM, melainkan dipersetujui sebaliknya di bawah perjanjian itu;

b. Bagi perkakasan ICT yang dicipta, maklumat mengenai semua pencipta asal mestilah dikekalkan; dan

c. Perkakasan tersebut tidak dibenarkan dijual, disewa, dipinjam, disebar atau diberi kepada sesiapa atau entiti tanpa kebenaran pengurusan UiTM.

9.2.2 Pengagihan Perkakasan ICT

Agihan perkakasan ICT hendaklah mengikut prosedur di dalam Garis Panduan Pengurusan ICT UiTM.

9.2.3 Geran komputer

Geran komputer hendaklah mengikut prosedur di dalam Garis Panduan Pengurusan ICT UiTM.

9.2.4 Peminjaman Perkakasan ICT

a. Staf yang membuat peminjaman perkakasan ICT bertanggungjawab sepenuhnya terhadap keselamatan perkakasan yang dipinjam dan tertakluk kepada Garis Panduan Pengurusan ICT Universiti.

b. Pelajar dibenarkan membuat peminjaman perkakasan ICT dengan mendapat surat kebenaran/sokongan dari pensyarah atau pegawai di fakulti/pusat tanggungjawab (PTJ) berkaitan. Perkakasan tersebut adalah di bawah tanggungjawab pelajar dan pensyarah atau pegawai berkenaan.

9.2.5 Baikpulih dan Penyelenggaraan Perkakasan ICT

a. Semua baikpulih dan penyelenggaraan perkakasan ICT hendaklah mengikut prosedur yang ditetapkan;

b. Penyelenggaraan perkakasan ICT perlu diselaras oleh pengurusan ICT bagi tujuan pemantauan dan inventori;

c. Bantuan teknikal/aduan tentang masalah-masalah yang dihadapi dalam penggunaan perkakasan ICT perlu dimajukan kepada sistem *online/helpdesk* aduan Pengurusan ICT; dan

d. Baikpulih dan selenggaraan perkakasan ICT tertakluk kepada Pekeliling Perbendaraan Malaysia mengenai Tatacara Pengurusan Aset Alih Kerajaan semasa.

9.2.6 Pelupusan Perkakasan ICT

a. Pelupusan perkakasan ICT tertakluk kepada Pekeliling Perbendaharaan Malaysia mengenai Tatacara Pengurusan Aset Alih Kerajaan semasa.

b. Maklumat yang berada di dalam perkakasan yang hendak dilupus perlu dihapuskan atau diasingkan seperti dinyatakan di dalam Dasar Keselamatan ICT UiTM.

c. Pelupusan perkakakasan ICT adalah tertakluk kepada prosedur Pejabat Bendahari UiTM dan Pekeliling Perbendaharaan.

9.2.7 Tanggungjawab Pengguna

Pengguna bertanggungjawab sepenuhnya kepada perkakasan ICT yang dibekalkan dari segi penggunaan, keselamatan dan penyelenggaraan.

9.2.8 Tanggungjawab Pihak Ketiga

Semua aktiviti menyedia, mengurus, membekal, menyelenggara perkakasan ICT oleh pihak ketiga dalam premis UiTM perlu diselia oleh staf ICT yang dipertanggungjawabkan.

9.2.9 Kehilangan Perkakasan ICT

Pengguna hendaklah menanggung kosnya sendiri bagi menggantikan perkakasan ICT yang hilang disebabkan kecuaian berdasarkan spesifikasi yang sama atau lebih tinggi.

Pengguna perlu melaporkan segera kepada Polis Bantuan UiTM dan Polis Diraja Malaysia sekiranya perkakasan tersebut hilang atau dicuri dalam tempoh 24 jam kehilangan atau kecurian itu, selaras dengan Pekeliling Bendahari Bil 1/1998 – Aturcara Kehilangan Wang/Harta Benda UiTM bagi peralatan yang dibekalkan oleh UiTM.

9.3 Perisian ICT

Perisian ICT adalah semua perisian yang diperolehi dan digunakan untuk pengajaran dan pembelajaran, penyelidikan, pembangunan sistem, pentadbiran di UiTM atau yang dibangunkan oleh UiTM yang berada dalam simpanan pengguna.

Perolehan dan penggunaan perisian ICT tanpa lesen adalah tidak dibenarkan. UiTM tidak akan bertanggungjawab terhadap sebarang perolehan dan penggunaan perisian ICT tanpa lesen oleh pengguna.

9.3.1 Perisian lesen *perpetual*

a. Semua perisian ICT yang diperolehi oleh UiTM menggunakan peruntukan kewangan UiTM atau melalui perjanjian kerjasama atau penyelidikan dengan lesen *perpetual* adalah hak milik UiTM; dan

b. Perisian tersebut tidak dibenarkan dijual, disewa, dipinjam, disalin semula, dilesenkan semula, disebar atau diberi kepada sesiapa atau entiti tanpa kebenaran pengurusan UiTM.

9.3.2 Perisian lesen *time-based*

a. Semua perisian ICT yang diperolehi oleh UiTM menggunakan peruntukan kewangan UiTM atau melalui perjanjian kerjasama atau penyelidikan, dengan lesen *time-based* boleh digunakan oleh warga UiTM dalam tempoh kontrak;

b. Perisian ini bukan hak milik mutlak UiTM; dan

c. Perisian tersebut tidak dibenar kan dijual, disewa, dipinjam, disalin semula, dilesenkan semula, disebar atau diberi kepada sesiapa atau entiti lain.

9.3.3 Tanggungjawab Pengguna

Pengguna bertanggungjawab sepenuhnya kepada perisian ICT yang dibekalkan dari segi penggunaan, keselamatan dan penyelenggaraan tertakluk kepada Garis Panduan Pengurusan ICT UiTM.

9.3.4 Tanggungjawab Pihak Ketiga

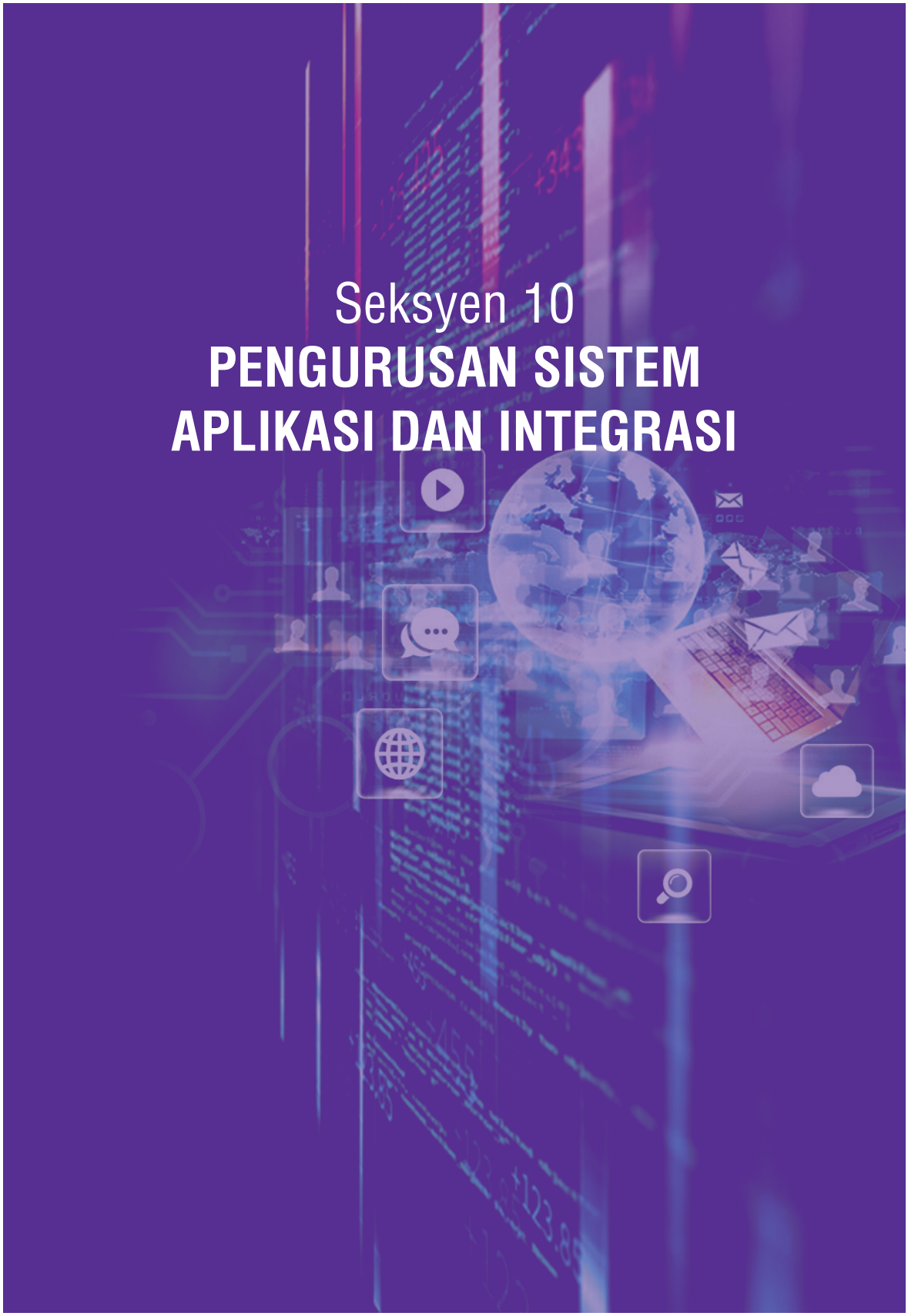
Semua aktiviti menyedia, mengurus, membekal, menyelenggara perisian ICT oleh pihak ketiga dalam premis UiTM perlu diselia oleh staf ICT yang dipertanggungjawabkan.

9.4 Perolehan ICT

Semua perolehan ICT mestilah mematuhi prosedur perolehan UiTM seperti Pekeliling Pejabat Bendahari, Pekeliling Perbendaharaan, Pekeliling Naib Canselor dan lain-lain pekeliling yang boleh diterima pakai.

9.5 Pematuhan Dan Keperluan Perundangan

Tertakluk kepada prosedur yang berkuatkuasa, mana-mana pihak yang gagal untuk mematuhi peruntukan seksyen ini sama ada dengan niat sengaja atau sebaliknya boleh dikenakan tindakan penguatkuasaan bagi tujuan pematuhan di bawah Seksyen 3: Penguatkuasaan dan Pematuhan.



Seksyen 10

PENGURUSAN SISTEM APLIKASI DAN INTEGRASI

10. PENGURUSAN SISTEM APLIKASI DAN INTEGRASI

10.1 Tujuan

Tujuan dasar ini ialah bagi memastikan pengurusan sistem aplikasi dan integrasi adalah berdasarkan *Enterprise Architecture* universiti dan selari dengan hala tuju strategik universiti bagi mengelakkan pertindanan serta memperjelaskan peranan dan tanggungjawab pihak pemilik sistem dan pengurusan ICT, seterusnya meningkatkan kebolehgunaan dan kebolehpercayaan serta integriti dan kebolehsediaan sistem aplikasi dan integrasi.

10.2 Katalog Sistem

Semua sistem aplikasi untuk universiti perlu didaftar oleh pemilik sistem kepada pihak pengurusan ICT.

10.3 Pemilikan Sistem

Setiap sistem yang dibangunkan mesti mempunyai pemilik ke atas sistem yang dilantik semasa pembentukan pasukan projek.

Pemilik hendaklah dari PTJ/jabatan/unit yang bertanggungjawab ke atas proses kerja sistem yang dibangunkan.

10.4 Permohonan Pembangunan

10.4.1 Permohonan Pembangunan Sistem Aplikasi Secara Dalaman (*In House Development*)

Permohonan atau cadangan sistem aplikasi baru untuk kegunaan Universiti atau lebih daripada satu (1) PTJ atau perubahan terhadap sistem aplikasi sedia ada kepada versi terbaru mesti dimajukan secara rasmi kepada Pengarah ICT dan mematuhi prosedur yang telah ditetapkan. Kelulusan dan pendekatan pembangunan projek sistem aplikasi adalah tertakluk kepada hasil kajian yang akan dilakukan.

10.4.2 Pembangunan Daripada Pihak Ketiga (*Outsource*)

a. Permohonan pembangunan mesti dimajukan secara rasmi kepada Pengarah Pengurusan ICT. Dan kelulusan adalah tertakluk kepada hasil kajian yang akan dilakukan.

b. Seliaan dan pemantauan dilaksanakan oleh pemilik

c. sistem manakala aspek teknikal perlu dikawal selia oleh Pengurusan ICT dan pihak teknikal yang berkenaan.

d. Klausa pemindahan teknologi dan penyerahan pemilikan *source code* daripada pembekal kepada teknikal hendaklah dinyatakan dalam kontrak dengan persetujuan pemilik sistem. Pihak ketiga perlu menyediakan dokumentasi teknikal yang lengkap dan terkini seperti yang telah ditetapkan oleh UiTM.

10.5 Pembangunan Sistem

Pembangunan sistem aplikasi, sama ada oleh pihak Pengurusan ICT atau PTJ mesti mematuhi *Enterprise Architecture* universiti dan mematuhi prosedur yang telah ditetapkan.

10.6 Penamatan Sistem

Sistem Aplikasi yang tidak digunakan lagi mesti diarkibkan dan dikeluarkan daripada persekitaran ICT universiti mengikut garis panduan berkaitan. Arahan penamatan sistem aplikasi mesti diperolehi dari pemilik sistem berkenaan.

10.7 Kawalan Capaian Sistem

Kawalan capaian kepada sistem mesti ditentukan oleh pemilik sistem berkenaan dan mesti mematuhi Dasar Keselamatan ICT UiTM.

10.8 Kualiti Data dan Maklumat dalam Sistem

Tanggungjawab ke atas kesahihan data dan maklumat adalah pada pemilik sistem.

10.9 Kesinambungan Bisnes dan Pemulihan Bencana

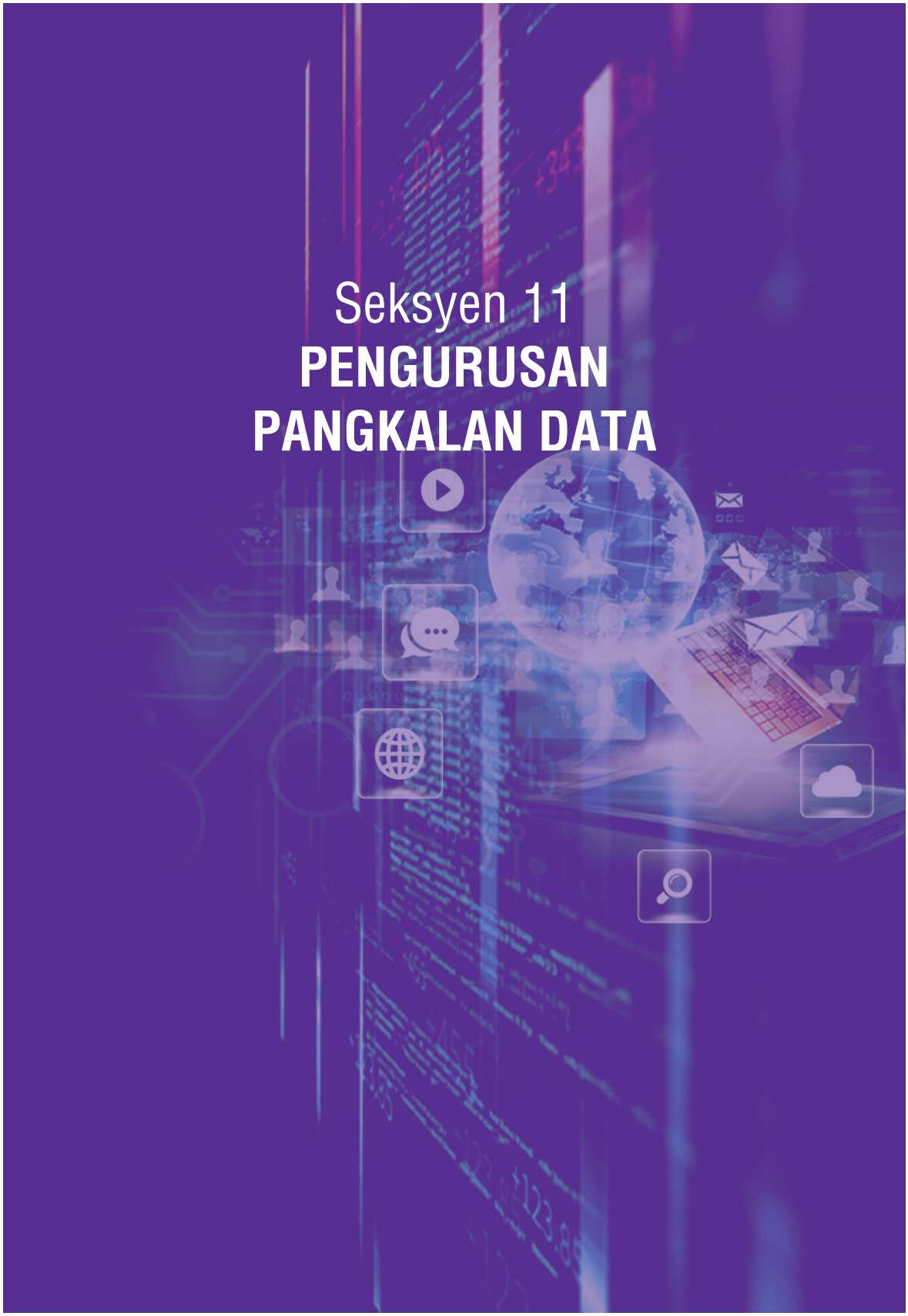
Bagi menjamin kesinambungan sistem dan pemulihan bencana, operasi *backup* dan *restore* mesti dilakukan berdasarkan Dasar Keselamatan ICT UiTM (Bidang 06 Pengurusan Operasi dan Komunikasi).

10.10 Penyelenggaraan, sokongan dan latihan

a. Sistem yang diselenggara mesti diuji sebelum digunakan. Pengguna mesti dimaklumkan dan diberi latihan yang sesuai.
b. Dokumentasi sistem mesti dikemaskini.

10.11 Integrasi Sistem dan Data

Semua proses integrasi data & sistem (sama ada dalaman ataupun kepada agensi luar) perlu menggunakan fasiliti integrasi universiti yang sedia ada. Setiap permohonan integrasi perlu mendapatkan kebenaran daripada pemilik sistem terlebih dahulu sebelum sebarang proses integrasi dilaksanakan.



Seksyen 11

PENGURUSAN PANGKALAN DATA

11. PENGURUSAN PANGKALAN DATA

11.1 Tujuan

Tujuan dasar ini ialah bagi memastikan pengurusan pangkalan data adalah berdasarkan selari dengan hala tuju strategik universiti, seterusnya meningkatkan kebolehgunaan dan kebolehpercayaan serta integriti dan kebolehsediaan pangkalan data.

11.2 Katalog pangkalan data

Semua pangkalan data untuk universiti perlu didaftar oleh pemilik sistem kepada pihak Pengurusan ICT.

11.3 Pengurusan

a. Pemilik pangkalan data bertanggungjawab menyediakan, mengesahkan dan memelihara semua proses dan prosedur seperti dalam dokumen Garis Panduan Pengurusan ICT UiTM;

b. Semua pangkalan data *production* digalakkan mempunyai sokongan penyelenggaraan (*Support Maintenance*) daripada syarikat pengeluar perisian tersebut; dan

c. Pemilihan perisian pangkalan data (DBMS) adalah merujuk kepada Garis Panduan Pengurusan ICT UiTM.

Semua Pangkalan Data mesti diselenggara dan dipantau. Maklumat perlulah didokumenkan untuk rujukan analisis trend dan proses yang berlaku dalam pangkalan data.

11.4 Hak Milik Pangkalan Data – Tadbir Urus

Pentadbir pangkalan data dan pentadbir sistem mesti dilantik. Pelantikan ini mesti didokumenkan, diwar-warkan dan dipantau. Butiran berkaitan hak milik pangkalan data adalah seperti berikut:

a. Semua pangkalan data universiti mesti didaftarkan kepada pihak pengurusan ICT;

b. Pentadbir pangkalan data (DBA) bertanggungjawab untuk merancang, menyediakan, menyelenggara, menaiktaraf, membuat pemulihan dan kawalan terhadap semua pangkalan data *production* dan *non-production*; dan

c. Pentadbir sistem pangkalan data mesti menyelenggara dan mengesahkan inventori dalam pangkalan data seperti yang dinyatakan dalam Garis Panduan Pengurusan ICT Universiti.

11.5 Keselamatan Pangkalan Data

a. Dasar keselamatan dan standard mestilah selaras dengan dasar dan standard yang ditakrifkan dalam Dasar Keselamatan ICT UiTM;

b. Semua pangkalan data *production* dan *non-production* mesti mematuhi kawalan berkaitan capaian data terhadap pangkalan data; dan

c. Pengaturcara perlu mendapatkan kebenaran daripada pentadbir pangkalan data untuk mencapai data dalam pangkalan data *production.*

11.6 Kebenaran Capaian (*Access Privileges*) Pangkalan Data

Pentadbir Pangkalan Data bertanggungjawab terhadap capaian pangkalan data. Kebenaran capaian terhadap pangkalan data mesti dipantau dan diselaraskan dengan Dasar Keselamatan ICT UiTM merangkumi perkara berikut:

a. Menakrifkan proses pengurusan kebenaran capaian terhadap pangkalan data untuk semua pengguna pangkalan data;

b. Pangkalan data yang mengandungi maklumat rahsia besar, rahsia, terhad atau sulit mesti dihadkan kepada pengguna yang dibenarkan sahaja;

c. Mewujudkan prosedur keselamatan untuk menguruskan kebenaran capaian pangkalan data;

d. Mendokumenkan maklumat kebenaran capaian terhadap pangkalan data;

e. Menetapkan tempoh simpanan maklumat permohonan akses kebenaran terhadap pangkalan data;

f. Pemantauan berkala terhadap kebenaran capaian pangkalan data; dan

g. Capaian kepada maklumat ditentukan oleh Pentadbir Sistem berkaitan.

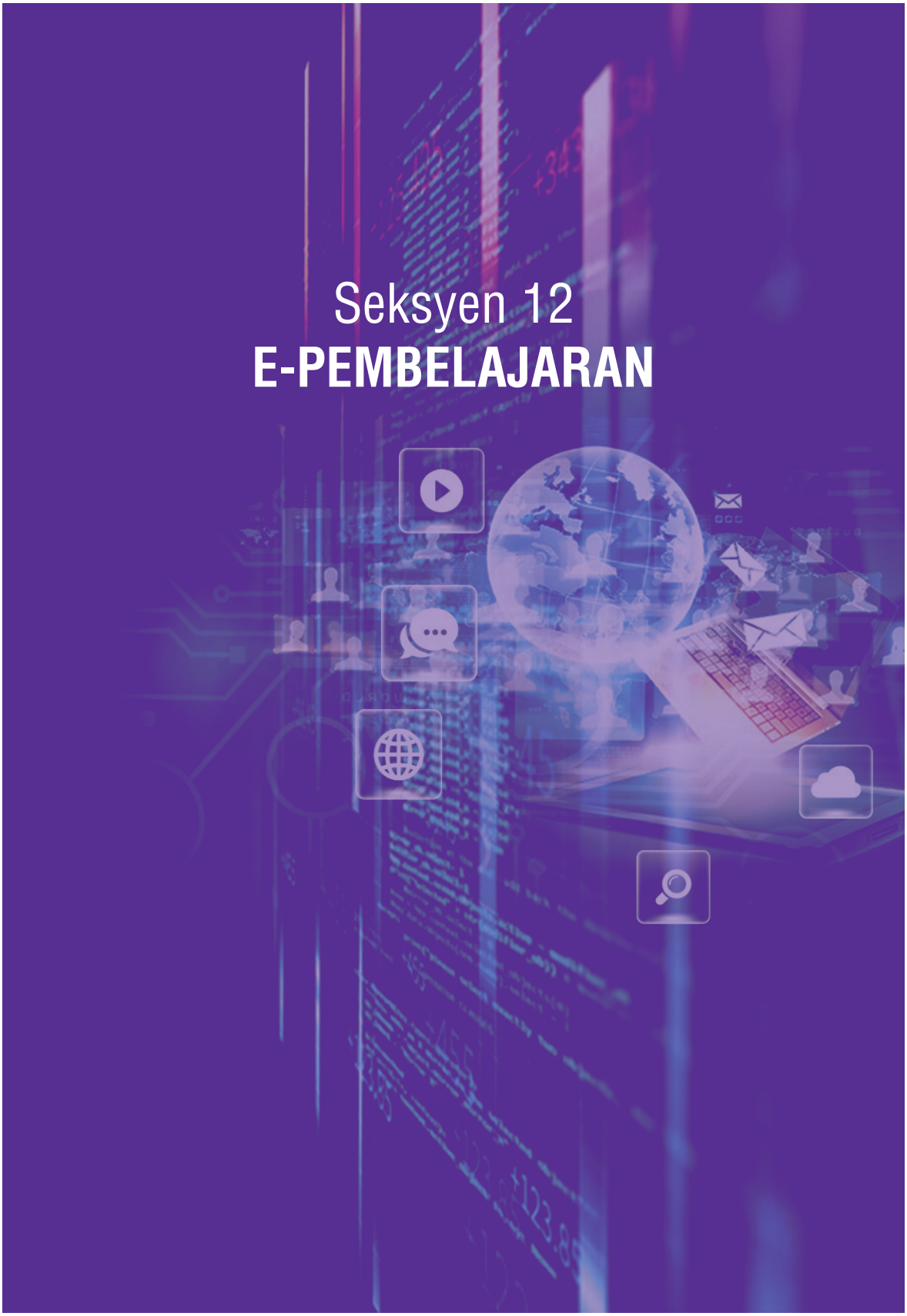
11.7 *Backup* dan *Recovery*

Semua Pangkalan Data *Production,* mestilah mempunyai *backup* yang dijadualkan secara berkala.

Pengurusan Operasi *Backup & Recovery* Pangkalan Data mesti mematuhi Garis Panduan Pengurusan ICT UiTM.

Seksyen 12

E-PEMBELAJARAN



12. E-PEMBELAJARAN

12.1 Tujuan

Tujuan dasar ini ialah menjadi satu panduan bagi pelaksanaan e-Pembelajaran di Universiti. Matlamat utama adalah bagi Universiti untuk menggunakan teknologi maklumat dan komunikasi sebagai alat bagi meningkatkan kualiti pengajaran dan pembelajaran bertujuan membangunkan modal insan bertaraf dunia serta menjadikan UiTM sebuah universiti unggul yang berteraskan kesarjanaan dan kecemerlangan akademik menerusi e-pembelajaran.

12.2 Skop e-Pembelajaran

Skop e-Pembelajaran adalah bentuk instruksi (pengajaran dan pembelajaran) yang dikendalikan menerusi media elektronik bertujuan meningkatkan keberkesanan serta menyokong proses pengajaran & pembelajaran.

12.3 Tadbir Urus e-Pembelajaran

a. Universiti bertanggungjawab menyediakan sumber, latihan dan sokongan berkaitan dengan e-Pembelajaran. Universiti akan menyediakan:

   i. Sistem pengurusan pembelajaran yang lebih praktikal;

   ii. Latihan berkaitan e-pembelajaran secara berterusan;

   iii. Perisian pembangunan e-kandungan terkini;

   iv. Peralatan dan perkakasan audio/video termasuk studio rakaman;

   v. Klinik/Bantuan pembangunan e-kandungan; dan

   vi. Pengurusan dan penyelenggaraan pelayan (*server*) bagi Sistem e-pembelajaran.

b. Tanggungjawab pemilik Sistem e-Pembelajaran dalam tadbir urus e-Pembelajaran adalah seperti berikut:

   i. Memberi kesedaran dan pendedahan kepada tenaga pengajar mengenai penggunaan e-pembelajaran bagi tujuan pengajaran dan pembelajaran;

ii. Memantau dan menyelaras aktiviti e-Pembelajaran pembangunan bahan pengajaran dan pembelajaran;

iii. Menjalankan aktiviti penyelidikan dan pembangunan berkaitan dengan e-Pembelajaran; dan

iv. Menyediakan garis panduan e-Pembelajaran.

c. Peranan Tenaga Pengajar dalam melaksanakan e-Pembelajaran adalah seperti berikut:

i. Mematuhi dasar dan garis panduan e-Pembelajaran UiTM;

ii. Mengoptimumkan aplikasi e-Pembelajaran yang disediakan oleh UiTM;

iii. Membimbing pelajar dalam penggunaan e-Pembelajaran;

iv. Menghadiri latihan e-Pembelajaran untuk pembangunan professional; dan

v. Membangun dan menyelenggara kandungan e-Pembelajaran bagi kursus yang dikendalikan.

d. Peranan Pelajar dalam e-Pembelajaran adalah seperti berikut:

i. Mematuhi dasar dan garis panduan e-Pembelajaran;

ii. Meningkatkan kemahiran menggunakan e-Pembelajaran secara berterusan;

iii. Memuat turun bahan pembelajaran secara berterusan; dan

iv. Mengoptimumkan penggunaan e-Pembelajaran yang disediakan oleh UiTM.

e. Peranan Penyedia Bahan e-Pembelajaran adalah seperti berikut:

i. Bertanggungjawab sepenuhnya terhadap bahan-bahan yang disumbangkan;

ii. Bertanggungjawab mengemaskini bahan pembelajaran dari semasa ke semasa; dan

iii. Bertanggungjawab mematuhi peraturan UiTM serta undang-undang berkaitan.

f. Berikut adalah perihal hak cipta Kandungan Kursus yang dibangunkan khusus untuk e-Pembelajaran dan digunakan di Universiti.

   i. Semua hakcipta bahan pengajaran yang dibangunkan menggunakan kemudahan dan sokongan yang disediakan oleh UiTM adalah milik UiTM;

   ii. Penggunaan bahan e-Pembelajaran bukan untuk tujuan dan/atau faedah UiTM perlu mendapat kebenaran bertulis UiTM; dan

   iii. Penyediaan bahan kursus adalah tertakluk kepada garis panduan yang ditetapkan oleh Universiti.

12.4 Tahap Pelaksanaaan e-Pembelajaran

a. Pelaksanaan e-Pembelajaran untuk akademik adalah melalui kaedah mod pembelajaran teradun atau *Blended Learning*. Merujuk kepada Jawatankuasa CAP e-Learning, KPT, mod Pembelajaran Teradun atau *Blended Learning* (BL) merujuk kepada kursus yang mempunyai campuran pendekatan pembelajaran mod dalam talian (*online*) dan mod pembelajaran bersemuka (*onsite*) dengan 30% - 80% kandungan dan aktiviti kursus dikendalikan secara *online* sama ada menyokong atau menggantikan pembelajaran bersemuka. Sila rujuk Garis Panduan Pelaksanaan Pembelajaran Teradun (*blended learning*) Universiti Teknologi Mara.

b. Bagi menyokong e-Pembelajaran dalam mod BL, UiTM telah menyediakan akses internet yang laju bagi memastikan kelancaran P&P. Tiada sekatan pada bahan-bahan pengajaran dalam talian seperti akses ke *Youtube*. Kemudahan *Wifi/ Hotspot* juga disediakan bagi memastikan aktiviti BL dapat dijalankan tanpa mengira waktu dan lokasi di dalam kampus UiTM.

c. Penggunaan platform atau pelantar untuk e-pembelajaran adalah melalui penggunaan Portal e-pembelajaran rasmi Universiti. Sekiranya perlu menggunakan saluran lain, tenaga pengajar mesti menyediakan pautan (*link*) atau perintah tersirat (*embedded command*) melalui portal rasmi. Tenaga pengajar boleh menggunakan pelantar media sosial dengan syarat mendokumentasikan bukti pengajaran.

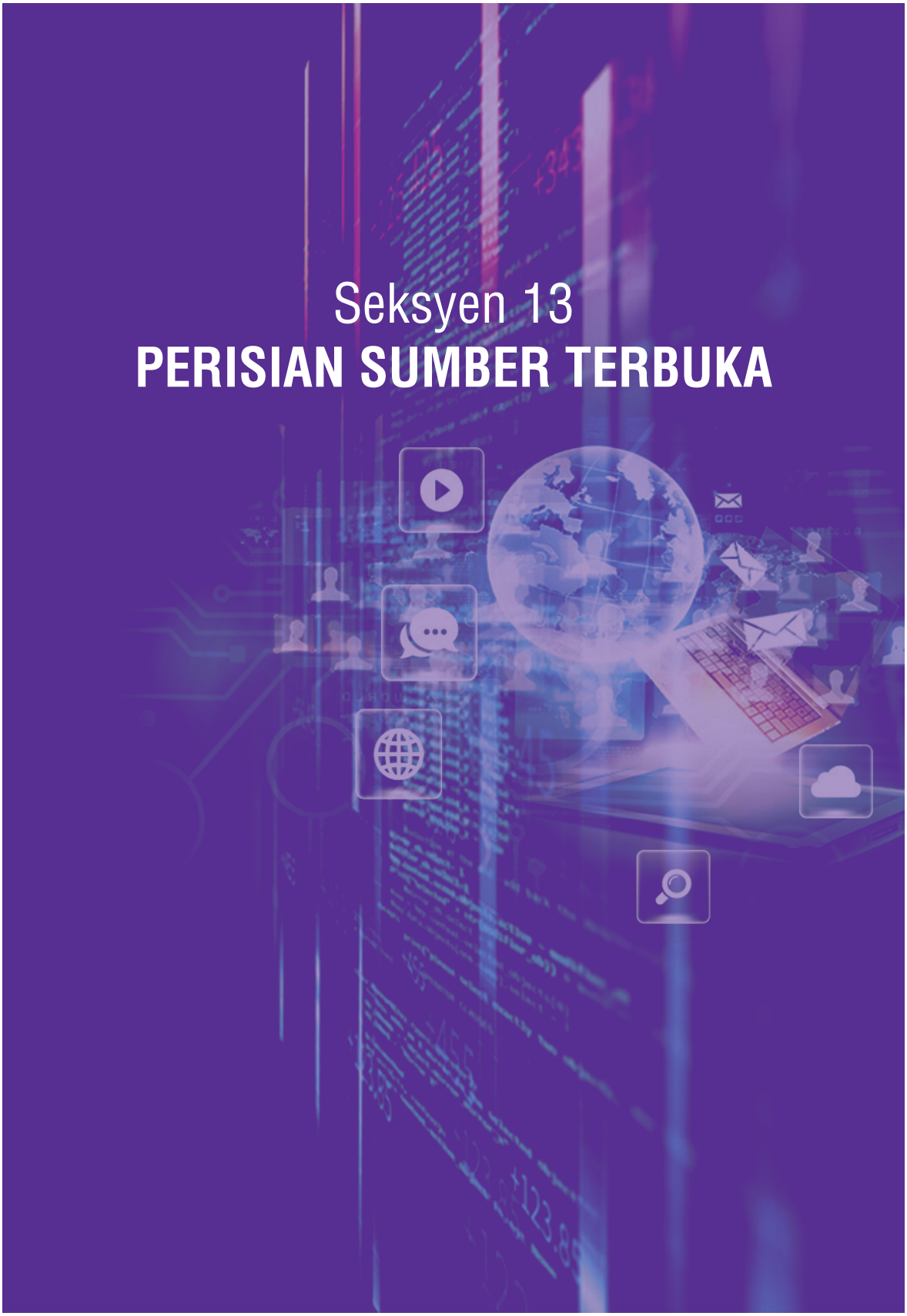
d. Pembangunan bahan e-kandungan kursus berupa aplikasi multimedia standard di kalangan tenaga pengajar adalah amat digalakkan. Pembangunan e-Kandungan ini bertujuan menyokong pelaksanaan Pembelajaran Teradun (*Blended Learning*) di peringkat Universiti melalui penyampaian kandungan silibus berbentuk digital.

e. Pelaksanaan e-Pembelajaran menerima pakai Polisi e-Pembelajaran UiTM, Garis Panduan pelaksanaan pembelajaran teradun (*blended learning*), Garis Panduan Pembangunan e-Kandungan Kursus dan juga Dasar e-Pembelajaran Negara (DePAN). Untuk pernyataan terperinci, sila rujuk dasar dan garis panduan tersebut.

f. Salah satu pendekatan yang digunakan dalam pelaksanaan e-Pembelajaran adalah melalui pembangunan e-Kandungan Terbuka (*Open Courseware*) dan Kursus Terbuka (MOOC).

Seksyen 13

PERISIAN SUMBER TERBUKA



13. PERISIAN SUMBER TERBUKA

13.1 Tujuan

Tujuan dasar ini ialah bagi memastikan penggunaan, perolehan, pemilikan, teknologi, perkongsian maklumat dan pelaksanaan *Open SourceSoftware* (OSS) berjalan lancar.

13.2 Penggunaan

Pengunaan OSS hendaklah berasaskan kepada Dasar Sektor Awam mengenai OSS, *Open Source Software (OSS) Implementation Guidelines by Malaysian Public Sector Open Source Software (OSS) Initiative* daripada MAMPU dan Dasar Keselamatan ICT UiTM.

13.3 Perolehan

a. Perolehan OSS perlu berdasarkan merit, nilai wang, ketelusan, keselamatan dan boleh dikendali serta selaras dengan dasar-dasar perolehan dan mengikut prosedur yang ditetapkan dan/ atau diterimapakai oleh Universiti; dan

b. Perkakasan yang digunapakai menyokong OSS.

13.4 Pemilikan

a. Pemilikan OSS harus merangkumi pelesenan perisian yang membolehkan hak untuk mengunakan dan mengubah suai perisian; dan

b. Perlesenan bagi perisian yang dibangunkan dalam harus serasi dengan lesen GPL, lesen BSD atau lesen GOM berdasarkan kesesuaian.

13.5 Perkongsian Maklumat

a. Mendaftarkan dalam bank pengetahuan semua *OSS solution*.

b. Berkongsi semua sumber OSS yang telah diubahsuai; dan

c. Melaporkan semua masalah dan pepijat.

13.6 Teknologi

a. Teknologi yang digunakan hendaklah mematuhi standard terbuka di seluruh dunia;

b. Teknologi yang diperolehi akan dapat disokong oleh mana-mana pihak lain untuk memastikan sokongan mempunyai kesinambungan.

13.7 Pelaksanaan

Pelaksanaan OSS hendaklah berdasarkan kepada prinsip panduan pelaksanaan iaitu:

a. Sesuai untuk tujuan penggunaan;

b. Kurang gangguan pada pengoperasian;

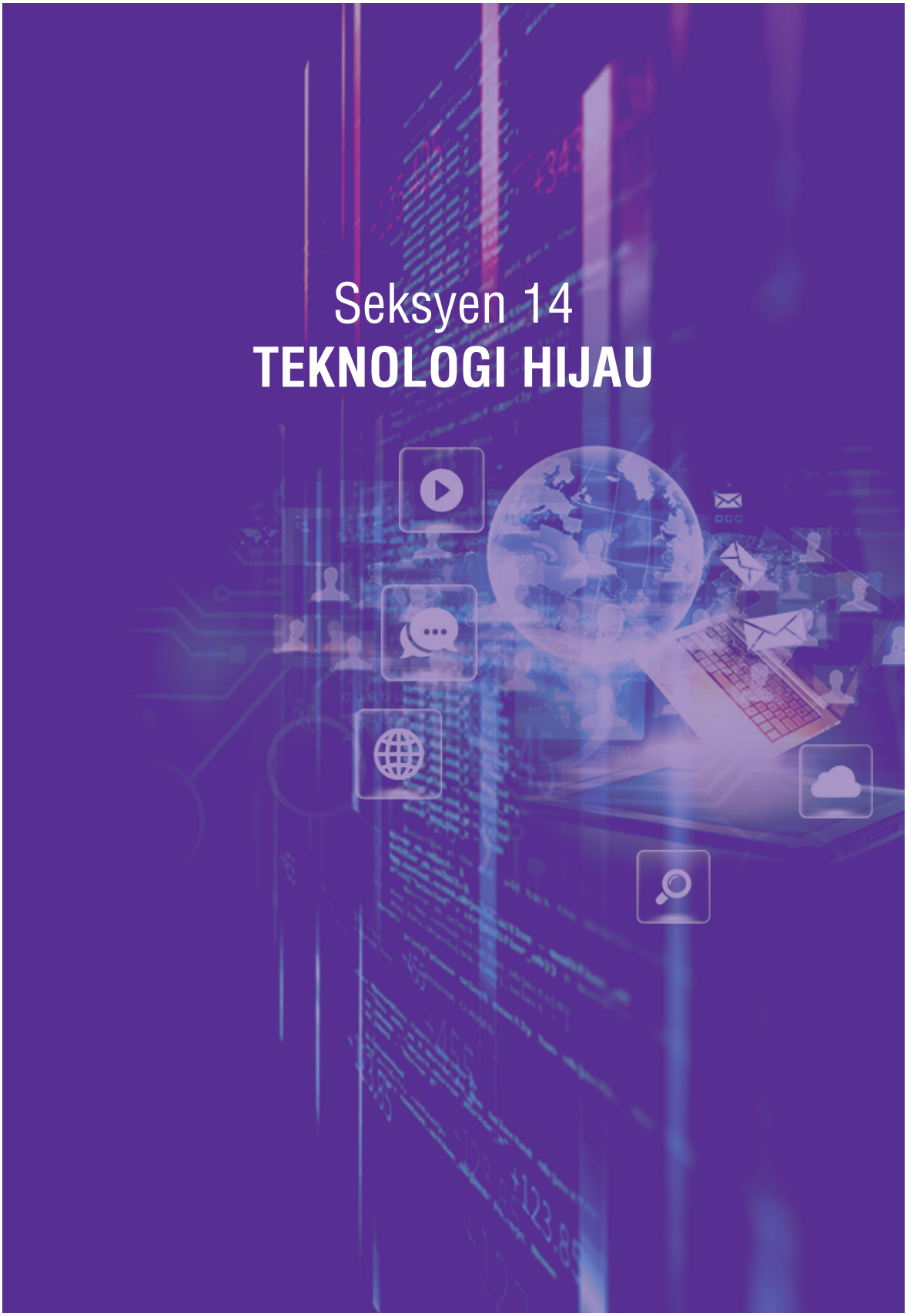
c. Kewujudan bersama sistem proprietari yang lain;

d. Memanfaatkan kemudahan sedia ada, perkakasan, perisian dan kepakaran; dan

e. Tidak didorong atau dikawal oleh perkakasan dan perisian vendor.

Seksyen 14

TEKNOLOGI HIJAU



14. TEKNOLOGI HIJAU

14.1 Tujuan

Tujuan dasar ini ialah bagi penggunaan produk ICT ke arah ICT Hijau bagi menyokong Dasar Teknologi Hijau Negara.

14.2 Pemakaian

Dasar ini merangkumi skop perolehan, penggunaan dan pelupusan produk ICT.

14.3 Perolehan

a. Perolehan produk ICT yang mempunyai ciri-ciri ICT Hijau.

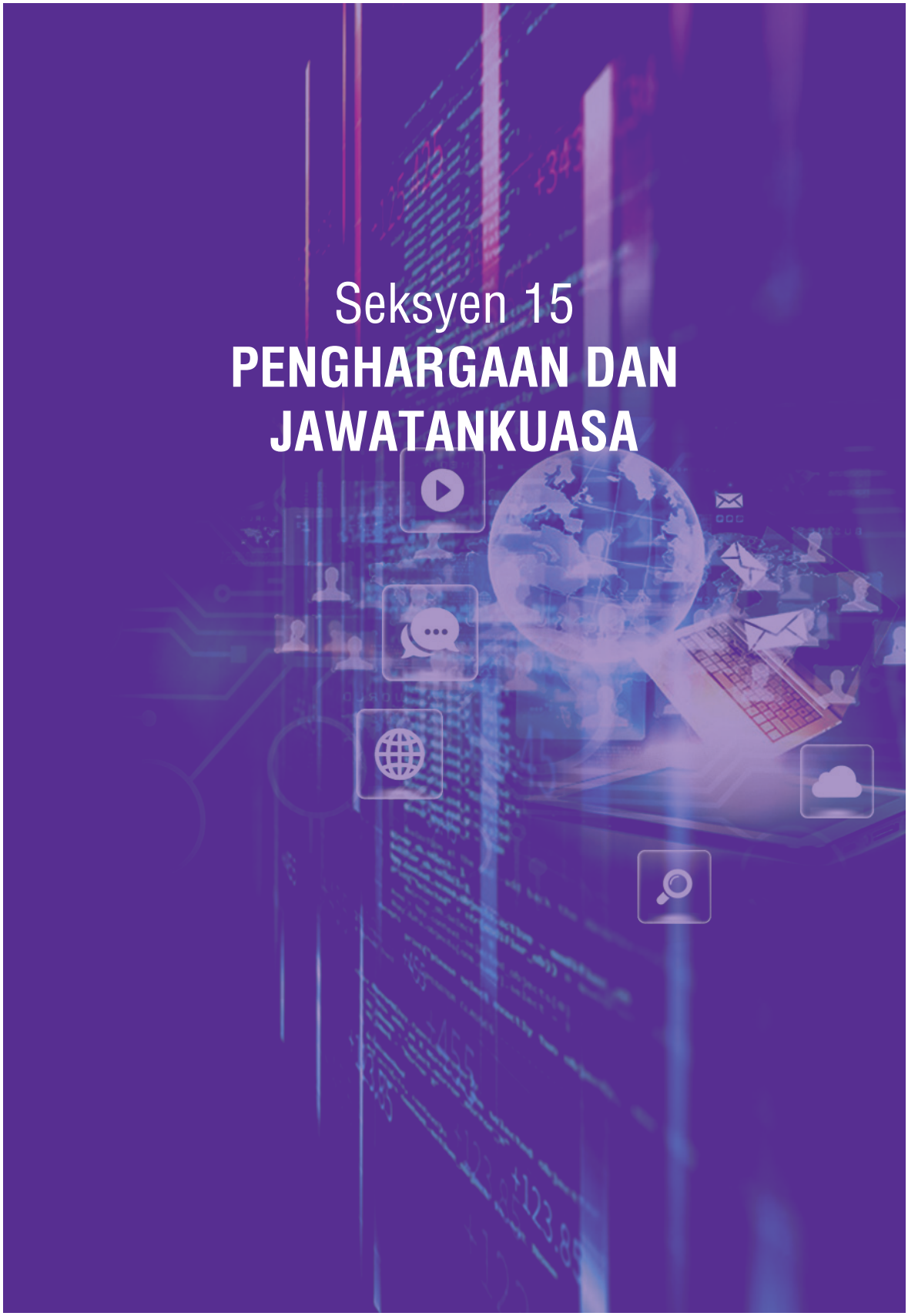
b. Produk ICT yang digunakan digalakkan mempunyai ciri-ciri ICT hijau, *eco-friendly, energy star* dan yang berkenaan dari peringkat negara atau antarabangsa.

14.4 Penggunaan

Pengguna hendaklah merujuk garis panduan penggunaan perkakasan dan perisian ICT yang telah ditetapkan iaitu Garis Panduan Penggunaan ICT Ke Arah ICT Hijau Dalam Perkhidmatan Awam yang disediakan oleh MAMPU.

14.5 Pelupusan

Produk ICT yang hendak dilupuskan perlu mengikut tatacara proses pelupusan UiTM dan mengambil kira pemuliharaan alam sekitar serta amalan hijau sama ada ianya masih boleh diguna pakai dan dikitar semula.



Seksyen 15
PENGHARGAAN DAN JAWATANKUASA

PEGAWAI PENYEDIA DOKUMEN DASAR ICT

- **Prof. Datin Dr Noor Habibah Arshad**
  Pengarah Infostruktur

- **Puan Sariani Sarijo**
  Ketua Jabatan Dasar & Strategik ICT

- **Encik Shamsuri Awang Seman**
  Ketua Jabatan Infrastruktur ICT

- **Encik Mohd Hairy Mohamaddiah**
  Ketua Jabatan Sistem Maklumat

- **Dr Shaharudin Ahmad**
  Ketua Jabatan Operasi ICT

- **Puan Hajah Ziraizratul Mohaini Mohamat**
  Ketua Jabatan Pengurusan Projek ICT

- **Dr Nazli Ahmad Aini**
  Ketua Bahagian Penilaian Produk

- **Puan Maznifah Mohd Sahalan**
  Timbalan Ketua Pegawai Teknologi Maklumat

- **En Sajuddin Samad**
  Timbalan Ketua Pegawai Teknologi Maklumat

- **Encik Gazairi Ghazali**
  Timbalan Ketua Pegawai Teknologi Maklumat

- **Encik Syamsudin Mudzamil**
  Timbalan Ketua Pegawai Teknologi Maklumat

- **Ts. Dr. Hajah Kamaliyah Sarjo @ Hj Ahmad**
  Pegawai Teknologi Maklumat Kanan

- **Encik Kamaruddin Mahad**
  Pegawai Teknologi Maklumat Kanan

- **Encik Mohd Khanafi Haron**
  Pegawai Teknologi Maklumat Kanan

- **Puan Shariza Mohd Said**
  Pegawai Teknologi Maklumat Kanan

- **Puan Arfah Jamian**
  Pegawai Teknologi Maklumat Kanan

- **Puan Ezabarena Radzi**
  Pegawai Teknologi Maklumat Kanan

- **Puan Siti Hajar Ismail**
  Pegawai Teknologi Maklumat Kanan

- **Puan Intan Zuriaty Mujirimi**
  Pegawai Teknologi Maklumat Kanan

- **Puan Nor Azni Abdullah Zawawi**
  Pegawai Teknologi Maklumat Kanan

- **Puan Sharina Mohd Nasir**
  Pegawai Teknologi Maklumat Kanan

URUSETIA CETAKAN DOKUMEN

- **Puan Maznifah Mohd Sahalan**
  Timbalan Ketua Pegawai Teknologi Maklumat

- **Nik Darwina Binti Ibrahim**
  Pegawai Teknologi Maklumat

GLOSARI & AKRONIM

Akaun Pengguna	Akaun pengguna merupakan nama pengenalan yang sah dalam sesuatu sistem atau sumber ICT bagi membolehkan seseorang mengakses kemudahan ICT, misalnya e-mel, sistem aplikasi dan akaun rangkaian, mengikut hak akses yang telah ditetapkan. Kebiasaannya akaun pengguna melibatkan penggunaan kata nama dan kata laluan.
Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, *optical disk, flash disk*, CDROM, *thumb drive* untuk sebarang kemungkinan adanya virus.
Aset ICT	Data, maklumat, perkakasan, perisian, aplikasi, dokumentasi dan sumber manusia serta premis berkaitan dengan ICT yang berada di bawah tanggungjawab UiTM.
Backup	Proses penduaan sesuatu dokumen, maklumat, data, pangkalan data, sistem aplikasi dan sebagainya.
Bandwidth	Kelebaran Jalur. Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
BSD	*Berkeley Software Distribution*
CIO	Ketua Pegawai Maklumat (*Chief Information Officer*). Pegawai yang bertanggungjawab terhadap perancangan, pengurusan, penyelarasan dan pemantauan program ICT dan maklumat UiTM.
CRT	*Cathode Ray Tube*
Denial of service	Penafian perkhidmatan.
Dokumen	Semua himpunan atau kumpulan bahan atau dokumen yang disimpan dalam bentuk media cetak, salinan lembut (*soft copy*), elektronik, dalam talian, kertas lutsinar, risalah atau slaid.

Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Satu proses penyulitan data dengan menukar teks biasa (*plain text*) kepada kod yang tidak dapat difahami, iaitu teks cipher. Bagi mendapatkan semula teks biasa tersebut, penyahsulitan atau *decryption* dilakukan.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*), penipuan (*hoaxes*).
GCERT	*Government Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
Generator set (Genset)	Genset adalah sebuah mesin-generator gabungan antara generator elektrik dan sebuah mesin penggerak. Keduanya dipadukan menjadi sebuah alat penghasil elektrik. Operasinya menggunakan bahan bakar petrol, disel, solar atau gas.
GOM	Kegunaan untuk audio, video, kamera dan pemain *movie*
GPL	*General Public License*
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh diakses lebih pantas.
Hub	Hub merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu port kepada semua *port* yang lain.

ICT	Teknologi Maklumat dan komunikasi (*Information and Communication Technology*) merangkumi produk, peralatan dan perkhidmatan yang digunakan untuk menyimpan, mencapai, memanipulasi, menghantar dan menerima data dalam bentuk digital.
ICTSO	*ICT Security Officer* adalah pegawai keselamatan ICT yang bertanggungjawab terhadap keselamatan ICT di UiTM.
ICT Hijau	Amalan dari segi pengeluaran, penggunaan dan pelupusan komputer, server serta alat-alat aksesori seperti monitor, tetikus, pencetak dan peralatan rangkaian secara berkesan dan efektif dengan memberi kesan yang minima atau tiada kesan terhadap alam sekitar. Ini bertujuan untuk mengurangkan penggunaan bahan berbahaya, menjimatkan tenaga elektrik dan memanjangkan jangka hayat penggunaan produk ICT.
Insiden Keselamatan ICT	Musibah (*adverse event*) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut yang mengakibatkan perkhidmatan ICT terjejas atau tidak berfungsi.
Internet	Internet adalah sistem rangkaian komunikasi global. Ia merangkumi infrastruktur perkakasan dan perisian yang menyediakan sambungan rangkaian global di antara komputer. Internet dalam skop UITM adalah servis rangkaian yang membolehkan pengguna mengakses sumber maklumat di seluruh dunia secara atas talian.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intranet	Merujuk kepada jaringan rangkaian dalaman yang menghubungkan komputer di dalam sesebuah organisasi dan hanya boleh dicapai oleh staf atau mana-mana pihak yang dibenarkan. Intranet dalam skop UiTM adalah servis rangkaian yang membolehkan pengguna mengakses sumber maklumat di dalam kampus UiTM secara atas talian.

Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan. Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan. Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code.* Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
IP	*Internet Protocol* (IP) adalah protokol atau prosedur komunikasi utama yang digunakan untuk menyampaikan datagram (paket) dari host sumber (*source*) ke host sasaran (*target*) dalam sistem rangkaian.
Kata laluan atau *password*	Merupakan turutan aksara yang membentuk satu kata rahsia bagi mengesahkan identiti pengguna dalam mencapai sistem atau sumber ICT yang dibenarkan. Ia digunakan bersama akaun pengguna.
Kemudahan ICT	Merujuk kepada perkakasan, perisian, peralatan, rangkaian komunikasi, sokongan dan perkhidmatan yang berkaitan teknologi maklumat dan telekomunikasi yang disediakan oleh UiTM bagi tujuan pengurusan, pentadbiran, penyelidikan, pengajaran dan pembelajaran serta operasi pengguna.
Kod Sumber Sistem Aplikasi	Merujuk kepada sebarang pernyataan yang ditulis dalam bahasa pengaturcaraan komputer yang difahami manusia dan terdapat dalam beberapa fail komputer tetapi kod sumber yang sama boleh dicetak di dalam buku atau dirakam dalam pita.
Kriptografi	Bermaksud adalah satu sains penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak yang tertentu sahaja.

LAN	*Local Area Network.* Rangkaian komputer yang merangkumi rangkaian kawasan setempat. LAN dalam skop UiTM adalah rangkaian UiTM di Shah Alam, kampus negeri dan kampus kota UiTM.
LCD	*Liquid Crystal Display*
Logout	*Log-out* komputer. Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, trojan horse, worm, spyware dan sebagainya.
MAMPU	Unit Permodenan Tadbiran dan Perancangan Pengurusan Malaysia, Jabatan Perdana Menteri
MAN	*Metropolitan Area Network* Rangkaian komputer yang meliputi suatu kawasan geografi yang agak luas berbanding dengan rangkaian yang diliputi oleh LAN. MAN dalam skop UiTM adalah rangkaian yang merangkumi UiTM Kampus Negeri/ UiTM Kampus PFI, dan UiTM kampus kota/satelit.
Media storan	Perkakasan yang berkaitan dengan penyimpanan data dan maklumat seperti disket, kartrij, cakera padat, cakera mudah alih, pita, cakera keras dan pemacu pena.
Modem	MOdulator DEModulator Peranti yang boleh menukar strim bICT digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian internet dibuat dari komputer.
MPK	Manual Prosedur Kerja
OSS	*Open Source Software*
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.

Pelajar	Seseorang yang mendaftar sesuatu program akademik (sama ada sepenuh masa atau separuh masa) di UiTM dan statusnya masih aktif.
Pemilik Sistem	adalah PTJ yang bertanggungjawab kepada proses dan operasi sistem tersebu
Pengguna	Staf, pelajar, pembekal, pelanggan atau pihak-pihak luar yang berurusan dengan UiTM yang menggunakan perkhidmatan ICT di UiTM.
Pengurusan ICT	PTJ yang menyelia dan mentadbir perihal teknologi maklumat seluruh sistem UiTM.
Pengarah Pengurusan ICT	Ketua bagi pengurusan ICT.
Pentadbir Sistem	Pegawai yang bertanggungjawab untuk membangun, mengurus, mengawal, memantau dan menyelenggara operasi dan keselamatan kemudahan ICT.
Peralatan Perlindungan	Peralatan yang berfungsi untuk pengawalan, pencegahan dan pengurusan tampalan seperti *firewall, router, proxy* dan antivirus
Perisian Aplikasi	Ia merujuk kepada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Perisian Sumber Terbuka	Perisian komputer dengan yang kod sumber yang disediakan dan dilesenkan dengan lesen di mana pemegang hak cipta memberikan hak untuk mengkaji, mengubah dan mengedarkan perisian bagi semua orang dan untuk semua tujuan
PFI	*Private Finance Initiative* Konsep pembangunan infrastruktur atau penyampaian perkhidmatan kerajaan atau UiTM yang dibuat, diselenggara dan dibiaya oleh pihak swasta.
Pihak Ketiga	Pihak yang membekalkan atau menerima perkhidmatan kepada atau daripada UiTM. Mereka terdiri daripada pembekal, pakar runding, agensi kerajaan dan sebagainya, yang terlibat secara langsung dengan pengurusan Universiti.

Private IP	Alamat IP yang dikhaskan untuk rangkaian dalaman seperti LAN dan MAN dan tidak disebarkan ke internet.
PPTM	Penolong Pegawai Teknologi Maklumat
PTJ	PTJ atau Pusat Tanggungjawab bermaksud semua jabatan, fakulti, pejabat, pusat, institut, kampus kota, kampus negeri di UiTM.
PTM	Pegawai Teknologi Maklumat di UiTM.
Public IP	Alamat IP yang dikhaskan untuk kegunaan rangkaian luar seperti WAN (internet).
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui internet.
Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan Negara, menyebabkan kerosakan besar kepada kepentingan atau martabat negara Malaysia atau memberi keuntungan besar kepada sesebuah kuasa asing dan hendaklah dikelaskan sebagai Rahsia.
Rahsia Besar	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Negara Malaysia, dan hendaklah dikelaskan sebagai Rahsia Besar.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian internet.
Screen Saver	Imej yang diaktifkan pada skrin komputer apabila ia tidak digunakan dalam satu jangka masa tertentu.
Server	Bermaksud komputer yang mempunyai keupayaan tinggi yang memberi perkhidmatan berpusat.
SOP	*Standard Operating Procedure*
Spam	Pesanan yang dikirimkan melalui peranti elektronik secara bertubi-tubi yang tidak dikehendaki oleh penerimanya. Orang yang melakukan spam disebut spammer. Tindakan spam dikenal dengan nama *spamming*. Bentuk spam yang dikenal secara umum meliputi spam surat elektronik, spam pesanan ringkas, *spam Usenet newsgroup, spam* mesin pencari informasi web (*web search engine spam*), *spam blog, spam wiki*, spam jejaring sosial.

Sulit	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan Negara tetapi memudaratkan kepentingan atau martabat negara Malaysia atau kegiatan kerajaan atau orang perseorangan atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing, dan hendaklah dikelaskan sebagai Sulit.
Switch	Gabungan hub dan *bridges* yang menapis bingkai mengikut segmen rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Teknologi Hijau	Pembangunan dan aplikasi produk, peralatan serta sistem untuk memulihara alam sekitar dan sumber semula jadi dan meminimumkan atau mengurangkan kesan negatif daripada aktiviti manusia.
Terhad	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang dikelaskan sebagai Rahsia Besar, Rahsia atau Sulit tetapi dikelaskan sebagai Terhad.
Threat	Gangguan dan ancaman sama ada melalui sebarang medium komunikasi atau isyarat yang bermotifkan untuk mendatangkan sebarang kerosakan atau kehilangan terhadap sesuatu pihak.
UiTM	Universiti Teknologi MARA yang ditubuhkan di bawah Akta Universiti Teknologi MARA 1976 (Akta 173) dan termasuklah penerima serah hak serta pegawai, kakitangan, pengkhidmat atau wakilnya yang diberi kuasa.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi memberikan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conference	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih orang pada lokasi yang berbeza-beza untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.

Video Streaming	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
VPN	*Virtual Private Network* - Rangkaian Persendirian Maya Servis rangkaian yang menggunakan infrastruktur telekomunikasi awam seperti Internet bagi membolehkan pengguna yang berada di luar kampus mendapat capaian UiTMnet dan menggunakan rangkaian tersebut dalam keadaan selamat.
WAN	*Wide Area Network*. Rangkaian komputer jarak jauh dan teknologi yang biasanya digunakan untuk menyambungkan komputer yang berada pada lokasi yang berbeza (negeri, negara dan benua). WAN dalam skop UiTM adalah sambungan kepada rangkaian Internet.
Warga UiTM	Kakitangan dan pelajar UiTM yang berdaftar.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.