UNIVERSITI TEKNOLOGI MARA
Pejabat Pembangunan Infrastruktur dan Infostruktur

DASAR ICT

Versi 2.0

TEKNOLOGI MAKLUMAT & KOMUNIKASI

Jabatan Infostruktur
Pejabat Pembangunan Infrastruktur dan Infostruktur
Aras 5 & 6 Menara Sultan Abdul Aziz Shah
Universiti Teknologi MARA
Shah Alam, Selangor.

Pusat Kebangsaan ISBN, Perpustakaan Negara Malaysia.
ISBN 978-967-19445-0-9

Dicetak di Malaysia oleh:

PUSAT PERCETAKAN UiTM (UiTM PRINT)
Fakulti Seni Lukis & Seni Reka
Universiti Teknologi MARA
40450 Shah Alam
Selangor Darul Ehsan

Sejarah Dokumen (DOCUMENT HISTORY)

Versi (Revision No.)	Kelulusan (Revision No.)	Tarikh Kuatkuasa (Released Date)
1.0	MAJLIS EKSEKUTIF UNIVERSITI (MEU)	14 Mac 2018
1.0	LEMBAGA PENGARAH UNIVERSITI (LPU)	2 Julai 2018
2.0	MAJLIS EKSEKUTIF UNIVERSITI (MEU)	23 Disember 2020

PRAKATA NAIB CANSELOR

Assalamualaikum warahmatullahi wabarakatuh dan salam sejahtera,

Perkhidmatan ICT dan penggunaan teknologi digital kini sudah menjadi satu keperluan kepada semua warga di Universiti Teknologi MARA (UiTM). Tidak hanya memfokuskan kepada kumpulan pengurusan dan professional malahan dengan norma baharu yang terpaksa kita lalui kini menyaksikan kepentingan dan keperluan bagi semua warga dalam penggunaan ICT.

Digitalisasi menjadi satu elemen penting dalam salah satu fokus strategik KPT 2021, iaitu memperkasakan Agenda Pendigitalan Pendidikan yang juga selari dengan hasrat YAB Perdana Menteri, Dato' Sri Ismail Sabri Yaakob bahawa penyampaian perkhidmatan perlu berteraskan teknologi digital dan revolusi industri 4.0 selaras dengan harapan serta cabaran.

Dokumen Dasar ICT Versi 2.0 yang dikeluarkan oleh Jabatan Infostruktur ini merupakan satu panduan rujukan oleh setiap warga UiTM. Ianya penting bukan sahaja sebagai satu rujukan tetapi juga sebagai panduan amalan terbaik dalam pelaksanaan dan penggunaan ICT di UiTM yang mengikut garis panduan yang ditetapkan.

Saya amat berharap agar pelaksanaan dasar ini menjadi satu aspirasi baharu dan seterusnya ibarat kata pepatah, "bertanjak baharu tinjau" yang membawa maksud membuat sesuatu pekerjaan haruslah mengikut aturan.

Akhir kata, saya ingin mengucapkan setinggi-tinggi tahniah dan terima kasih khususnya kepada pasukan Dokumen Dasar ICT UiTM Versi 2.0 ini daripada Jabatan Infostruktur, Pejabat Pembangunan Infrastruktur dan Infostruktur. Semoga dengan penghasilan dokumen ini dapat dimanfaatkan oleh seluruh warga UiTM khasnya dan pihak luar yang lain amnya.

Profesor Ts. Dr. Hajah Roziah Mohd Janor
Naib Canselor

KATA-KATA ALUAN
KETUA TEKNOLOGI MAKLUMAT (CIO)

Assalamualaikum warahmatullahi wabarakatuh dan salam sejahtera.

Alhamdulillah dengan berkat keizinan dan keberkatan-Nya, dokumen Dasar ICT UiTM Versi 2.0 telah berjaya dihasilkan dan telah diluluskan oleh Majlis Eksekutif Universiti (MEU) pada 23 Disember 2020. Dokumen Dasar ICT ini telah melalui proses semakan setelah pertama kali ianya dikeluarkan pada 14 Mac 2018 yang lalu. Dokumen ini merupakan satu panduan dan sumber rujukan utama kepada warga UiTM terhadap pematuhan peraturan yang telah dinyatakan sebagai Dasar ICT UiTM.

Jika dilihat dari segi perkembangan teknologi ICT masa kini, tidak dapat dinafikan bahawa ianya telah melalui satu fasa perubahan yang pantas. Justeru, bagi memastikan setiap warga cakna terhadap arus perubahan ini, pendedahan yang berterusan terhadap teknologi ICT perlu diberikan di samping pelaksanaan dan penggunaannya yang mematuhi dasar serta garis panduan yang telah ditetapkan.

Dasar ICT yang dikeluarkan oleh Jabatan Infostruktur ini merupakan satu rujukan yang meliputi semua sumber dan kemudahan ICT UiTM. Ianya terpakai kepada semua pengguna ICT di UiTM termasuk pembekal serta pihak lain yang berkaitan. Selaras dengan fungsinya yang menyatakan tentang amalan terbaik penggunaan ICT di UiTM, dokumen ini akan dikemas kini dari semasa ke semasa bagi memastikan ianya kekal relevan dengan perubahan masa dan teknologi serta berpandukan kepada garis panduan yang dikeluarkan oleh agensi pusat seperti Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) dan Jabatan Perkhidmatan Awam (JPA).

Diharapkan dengan wujudnya dokumen Dasar ICT ini, semua warga UiTM akan sentiasa terus berusaha bagi memastikan ianya dipatuhi demi mewujudkan persekitaran ICT yang terjamin dan selamat.

Akhir kata, setinggi-tinggi penghargaan dan ucapan terima kasih kepada Jabatan Infostruktur, Pejabat Pembangunan Infastruktur dan Infostruktur dan seluruh warga kerja yang terlibat secara langsung mahupun tidak langsung dalam menghasilkan dokumen Dasar ICT ini. Semoga usaha murni yang berterusan ini akan memberi manfaat kepada semua warga UiTM.

Profesor Dato' Ts. Dr. Hj. Mohd Fozi Ali

KANDUNGAN

KANDUNGAN

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 dan kamera.
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 *(Information Technology)* merangkumi produk, peralatan dan perkhidmatan yang digunakan untuk menyimpan, mencapai, memanipulasi, menghantar dan menerima data dalam bentuk digital.
ICTSO	*ICT Security Officer.* Pegawai yang bertanggungjawab terhadap keselamatan hal berkaitan ICT.

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.

GLOSARI & AKRONIM

Internet Protocol (IP)	***Internet Protocol (IP)*** adalah protokol 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.
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* ICT 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 tersebut.
Pengguna	Staf, pelajar, pembekal, pelanggan atau pihak-pihak luar yang berurusan dengan UiTM yang menggunakan perkhidmatan ICT di UiTM.
Pengurusan ICT	Pihak yang menyelia dan mentadbir perihal ICT di peringkat PTJ/ Bahagian.
PNC	Penolong Naib Canselor.
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.
Persekitaran ICT	Perkakasan, perisian, rangkaian, aplikasi dan/atau perkhidmatan ICT.
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.
PPTM	Penolong Pegawai Teknologi Maklumat.
Private IP	Alamat IP yang dikhaskan untuk rangkaian dalaman seperti LAN dan MAN dan tidak disebarkan ke Internet.
Produk	Merangkumi perkakasan ICT, Perisian dan Sistem Aplikasi.
PTJ	PTJ atau Pusat Tanggungjawab bermaksud jabatan, fakulti, pejabat, pusat, kampus kota, kampus negeri di UiTM.
PTM	Pegawai Teknologi Maklumat.
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.
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 rotoc.
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 protocol 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.

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.

PERNYATAAN 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.

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.

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.

SEKSYEN 1

DEFINISI

Seksyen 1 - DEFINISI

1.1 AKTA UNIVERSITI

Akta Universiti Teknologi MARA 1976 (Akta 173).

1.2 DASAR ICT

Dasar ICT adalah satu kenyataan rasmi dan ringkas di peringkat universiti berkaitan teknologi maklumat dan komunikasi (ICT). Ia menjadi asas untuk membuat keputusan dan menyatakan tindakan yang perlu dilaksanakan serta wajib dipatuhi.

1.3 STANDARD

Standard ialah aktiviti, tindakan, undang-undang atau peraturan mandatori yang dirujuk bagi memastikan struktur sokongan dan hala tuju dasar lebih efektif.

1.4 GARIS PANDUAN

Garis panduan ialah penyataan umum sebagai rujukan bagi cadangan pelaksanaan prosedur untuk mencapai objektif dasar.

1.5 PROSEDUR

Prosedur merupakan arahan terperinci yang telah ditetapkan dalam dasar, standard dan garis panduan bagi menyokong pelaksanaan dasar.

1.6 KATEGORI DASAR ICT

Dasar dan garis panduan ICT dikeluarkan dalam tiga kategori utama seperti yang berikut:

a. Pekeliling, iaitu suatu arahan rasmi mengenai sesuatu dasar kerajaan;

b. Surat Pekeliling, iaitu suatu penjelasan tentang pelaksanaan sesuatu dasar yang dinyatakan dalam pekeliling; dan

c. Surat Arahan, iaitu suatu arahan untuk melaksanakan sesuatu perkara secara spesifik tetapi tidak semestinya berdasarkan perkara yang dinyatakan dalam pekeliling atau surat pekeliling.

SEKSYEN 2

TADBIR URUS ICT UiTM

Seksyen 2 - TADBIR URUS ICT UiTM

2.1 PENGENALAN

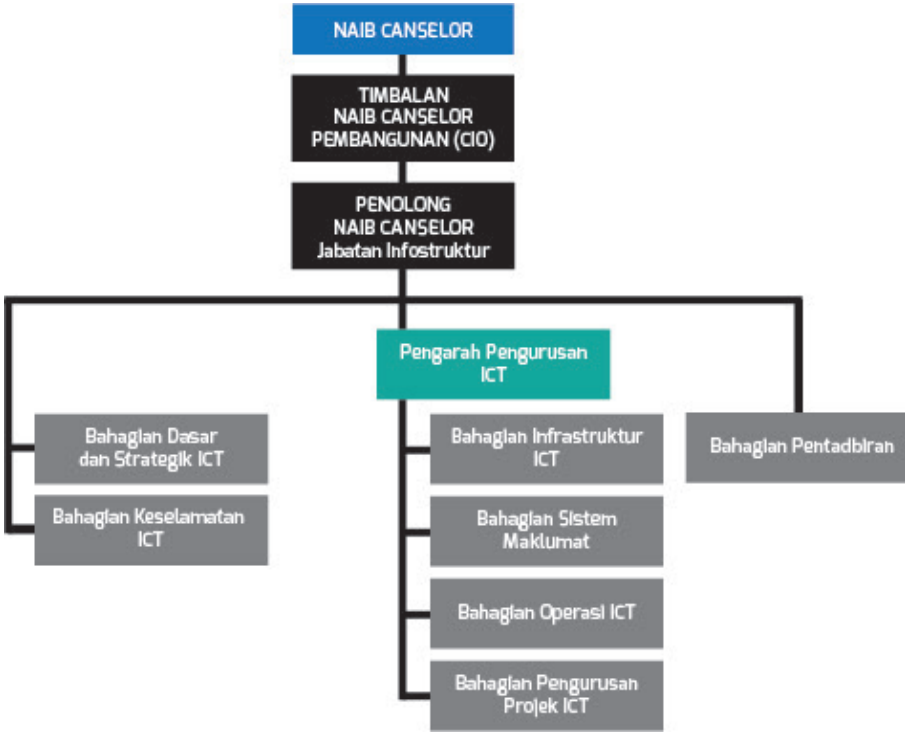
Seksyen ini menerangkan secara umum mengenai tadbir urus dan tanggungjawab terhadap agenda ICT di universiti dalam aspek pembangunan ICT bagi merancang, mengurus, melaksana dan menyelenggara perkhidmatan ICT UiTM menerusi strategi-strategi yang ditetapkan. Skop dasar ini merangkumi:

a. Terma rujukan Ketua Pegawai Maklumat (CIO) yang bertanggungjawab menetapkan Dasar Teknologi Maklumat dan Komunikasi (ICT) dan memantau keberkesanan pelaksanaan ICT di UiTM; dan

b. Menerangkan skop dan fungsi tadbir urus ICT.

2.2 CARTA ORGANISASI ICT UITM

Carta Organisasi Tadbir urus ICT UiTM yang baharu seperti gambar rajah 2-1 berikut menunjukkan hasil penstrukturan semula organisasi ICT UiTM pada 12 Disember 2018.



Gambar Rajah 2-1: Carta Organisasi Tadbir urus ICT

2.3 TADBIR URUS ICT

a. Naib Canselor

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

b. 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 oleh MAMPU dan Surat Edaran Pemakluman Fungsi dan Tugas CIO.

c. Ketua Pegawai Maklumat Bersekutu (*Associate* CIO)

Ketua 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.

d. Pengarah Pengurusan ICT

Pengarah Pengurusan ICT merupakan ketua yang bertanggungjawab menyediakan perkhidmatan ICT kepada UiTM dan memastikan pematuhan kepada Dasar ICT UiTM.

e. Pegawai Keselamatan ICT (ICTSO)

Pelantikan Pegawai Keselamatan ICT adalah memenuhi keperluan Pekeliling Am Bil.3/2000 (Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan) bagi memastikan Dasar Keselamatan ICT UiTM dipatuhi. ICTSO 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) Agensi Keselamatan Siber Negara (NACSA).

f. Pegawai Skim Perkhidmatan Teknologi Maklumat

Pegawai yang bertanggungjawab untuk membangun, mengurus, mengawal, memantau dan menyelenggara kemudahan dan perkhidmatan ICT.

g. Pemegang Taruh

Pemegang Taruh UiTM merupakan individu atau organisasi yang mempunyai kepentingan terhadap UiTM seperti pelajar, ibubapa, masyarakat, industri dan negara amnya.

h. 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 & PEMATUHAN

Seksyen 3 - PENGUATKUASAAN & PEMATUHAN

3.1 PENGENALAN

Seksyen ini memaklumkan kepada pengguna tentang tindakan yang boleh dikenakan kerana melanggar Dasar ICT UiTM. Skop dasar meliputi apa-apa bentuk pelanggaran yang dinyatakan di dalam Dasar ICT UiTM atau mana-mana akta, arahan, pekeliling dan peraturan yang berkaitan.

3.2 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 "*ignorantia juris non excusat*" atau *ignorance of law is not an excuse* adalah terpakai di dalam penguatkuasaan Dasar ICT UiTM.

3.3 PELANGGARAN DASAR

a. Mana-mana pihak yang gagal untuk mematuhi peruntukan dasar ini sama ada dengan niat sengaja atau pun tidak, boleh dikenakan tindakan 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 diambil 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 UiTM hendaklah dibuat secara rasmi kepada CIO/ *Associate* CIO. CIO/ *Associate* CIO boleh melantik satu Jawatankuasa yang terdiri daripada pengerusi dan sekurang-kurangnya dua (2) orang pegawai untuk membuat siasatan dan menyediakan laporan sebelum sesuatu tindakan diambil.

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

3.4 KEPERLUAN PERUNDANGAN

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

i. Akta Badan-badan Berkanun (Tatatertib dan Surcaj) 2000 (Akta 605);

ii. Akta Institusi-institusi Pelajaran (Tatatertib) 1976 (Akta 174);

iii. Akta Universiti Teknologi MARA 1976 (Akta 173);

iv. Akta Rahsia Rasmi 1972 (Akta 88);

v. Akta Komunikasi dan Multimedia 1998 (Akta 588);

vi. Akta Jenayah Komputer 1997 (Akta 563);

vii. Akta Perlindungan Data Peribadi 2010 (Akta 709);

viii. Akta Tandatangan Digital 1997 (Akta 562);

ix. Akta Mesin Cetak dan Penerbitan 1984 (Akta 301);

x. Akta Hak Cipta 1987 (Akta 332);

xi. Akta Tele-Perubatan 1997 (Akta 564);

xii. Akta Aktiviti Kerajaan Elektronik 2007 (Akta 680);

xiii. Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian *Government Computer Emergency Response Team* (GCERT) oleh NACSA bertarikh 28 Januari 2019;

xiv. Surat Pemakluman Pengurusan Maklumat Pegawai Keselamatan ICT (ICTSO) Sektor Awam bertarikh 28 Februari 2019 oleh NACSA;

xv. Surat Arahan MAMPU (MAMPU.BDPICT – 7/22(23) bertarikh 4 Janurari 2010) – Garis Panduan Transisi Protokol Internet Versi 6 (IPV6) Sektor Awam;

xvi. Surat Pekeliling Am Bilangan 3 Tahun 2009: Garis Panduan Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam bertarikh 17 Nov 2009;

xvii. Surat Pekeliling Am Bil. 1 Tahun 2008: Garis Panduan Mengenai Tatacara Memohon Kelulusan Teknikal Projek ICT Agensi Kerajaan yang dikeluarkan oleh MAMPU;

xviii. Arahan Teknologi Maklumat (2007) yang dikeluarkan oleh MAMPU;

xix. Pekeliling Am Bil.4 Tahun 2006: Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;

xx. Pekeliling Am Bil.6 Tahun 2005: Garis Panduan Melaksanakan Penilaian Risiko Keselamatan Maklumat Sektor Awam;

xxi. Pekeliling Am Bil.1 Tahun 2003: Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi Kerajaan;

xxii. Garis Panduan Pengurusan Keselamatan ICT yang dikeluarkan oleh MAMPU, Januari 2002;

xxiii. Pekeliling Am Bil.1 Tahun 2001: Mekanisme Pelaporan Insiden Keselamatan ICT (ICT) yang dikeluarkan oleh MAMPU;

xxiv. Pekeliling Am Bil. 3 Tahun 2000: Dasar Keselamatan ICT Kerajaan yang dikeluarkan oleh MAMPU;

xxv. Pekeliling Am Bil.1 Tahun 2000: Garis Panduan Malaysian Civil Service Link (MCSL) dan Laman Web Kerajaan yang dikeluarkan oleh MAMPU;

xxvi. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan";

xxvii. Pekeliling Am Bil. 6 Tahun 1999: Garis Panduan Pelaksanaan Perkongsian Pintar Antara Agensi-agensi Kerajaan Dalam Bidang Teknologi Maklumat yang dikeluarkan oleh MAMPU;

xxviii. Pekeliling Am Bil. 2 Tahun 1999: Penubuhan Jawatankuasa ICT dan Internet Kerajaan (JITIK) yang dikeluarkan oleh MAMPU; dan

xxix. Akta, Pekeliling, Arahan, Garis Panduan dan Surat Pekeliling yang dikeluarkan dari semasa ke semasa.

SEKSYEN 4

PENGURUSAN & PENYELENGGARAAN DASAR ICT

Seksyen 4 - PENGURUSAN & PENYELENGGARAAN DASAR ICT

4.1 PENGENALAN

Seksyen ini menerangkan tentang komitmen pengurusan ICT dalam pengurusan dan penyelenggaraan pengemaskinian dokumen Dasar ICT berdasarkan keperluan semasa.

4.2 PENGURUSAN DASAR ICT

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

4.3 PENYEBARAN DASAR

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

4.4 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. Kemukakan 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 (2) tahun sekali atau mengikut keperluan semasa.

4.5 PEMAKAIAN

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

SEKSYEN 5

PENGURUSAN PROJEK ICT

Seksyen 5 - PENGURUSAN PROJEK ICT

5.1 PENGENALAN

Seksyen ini menerangkan tentang proses dalam pengurusan projek ICT yang merangkumi fasa permulaan sehingga penamatan projek. Ianya bagi memastikan pelaksanaan pengurusan projek ICT di seluruh UiTM adalah mengikut perancangan dan Garis Panduan Pengurusan ICT UiTM.

5.2 DEFINISI PROJEK ICT

Projek ICT ialah projek pengkomputeran yang melibatkan salah satu atau gabungan kategori projek ICT seperti berikut:

a. **Pembangunan Sistem dan Aplikasi** - pembangunan sistem dan aplikasi menggunakan perisian/ *customization*/ integrasi dan sebagainya;

b. **Peningkatan Persekitaran ICT** - mempertingkatkan atau menaik taraf keupayaan, perubahan dan/atau pertambahan skop/ tempoh, *change request* (CR) persekitaran ICT;

c. **Perluasan persekitaran ICT** - memperkembangkan pelaksanaan dari lokasi sedia ada ke lokasi-lokasi lain atau dengan menambah bilangan pengguna di lokasi yang sama;

d. **Kajian ICT** - projek yang memberi fokus kepada kajian yang menggalakkan inovasi dan berpotensi untuk dilaksanakan serta dapat meningkatkan sistem penyampaian perkhidmatan universiti;

e. **Perancangan Strategik ICT** - pendekatan pengurusan untuk menambahbaik proses seperti penggubalan strategi, polisi, garis panduan, rangka kerja dan sebagainya; dan

f. **Perolehan Infrastruktur ICT** - semua jenis bekalan perkakasan ICT atau perisian sistem, perisian aplikasi dan lesen perisian (pembelian dan pembaharuan).

5.3 KAEDAH PELAKSANAAN PROJEK ICT

Projek boleh dilaksanakan dengan menggunakan pendekatan pelaksanaan projek berikut yang mana lebih bersesuaian mengikut keperluan, peruntukan masa, kewangan dan sumber yang ada.

a. ***In-sourcing*** - Pelaksanaan projek ICT yang menggunakan sumber manusia dan kepakaran dalaman. Pelaksanaan projek selalunya tidak melibatkan transaksi kewangan secara terus di mana kos sumber manusia dikira mengikut emolumen staf yang terlibat.

b. ***Out-sourcing*** - Pelaksanaan projek ICT yang menggunakan perkhidmatan luar sepenuhnya. Ianya melibatkan kos kewangan dan pengurusan kontrak.

c. ***Co-sourcing*** - Pelaksanaan projek ICT yang dilakukan secara bersama menggunakan kepakaran dalaman dan perkhidmatan luar. Ianya melibatkan kos kewangan dan pengurusan kontrak.

5.4 PERINGKAT PENGURUSAN PROJEK ICT

a. **Fasa Permulaan** - Fasa permulaan ialah fasa penting kerana pengurus projek perlu jelas akan skop dan objektif projek serta mendapatkan kelulusan untuk melaksana projek.

b. **Fasa Perancangan** - Fasa kedua ialah fasa untuk memperincikan aspek-aspek tadbir urus dan struktur organisasi projek, pengurusan dan kawalan projek serta pengurusan perolehan dan kontrak termasuk aktiviti-aktiviti dan serahan-serahan projek serta pelan-pelan yang perlu diwujudkan untuk melaksana dan mengawal projek ICT.

c. **Fasa Pelaksanaan & Kawalan** - Fasa untuk melaksanakan semua aktiviti yang dirancang untuk memastikan semua serahan dilaksana mengikut kos, tempoh dan skop untuk mencapai objektif projek.

d. **Fasa Penamatan** - Setelah semua serahan projek selesai dilaksana, projek boleh ditamatkan. Pengurus projek perlu memastikan semua isu/ risiko yang timbul telah diambil tindakan sewajarnya. Projek tidak boleh ditamatkan sekiranya isu masih tidak selesai.

SEKSYEN 6

PENGURUSAN STRATEGIK ICT

6.1 PENGENALAN

Seksyen ini menerangkan tentang pengurusan strategik ICT universiti yang berasaskan kepada dokumen "Panduan Pelan Strategik ICT Sektor Awam Malaysia" oleh MAMPU. Ianya bagi memastikan kaedah pelaksanaan pengurusan strategik ICT universiti adalah mengikut kaedah yang telah ditetapkan oleh Kerajaan.

6.2 METODOLOGI

Panduan Pelan Strategik ICT Sektor Awam Malaysia menetapkan metodologi standard yang mengandungi empat (4) peringkat utama iaitu:

a. Peringkat pertama: Menganalisis Persekitaran Bisnes

Peringkat ini mengandungi penilaian terhadap persekitaran bisnes semasa sebagai asas (*baseline*) kepada perancangan strategik ICT yang memperincikan senibina, konteks bisnes UiTM dan bisnes teras. Rumusan isu dan cabaran termasuk analisa jurang, analisis SWOT dan penyataan faktor kritikal kejayaan mengakhiri peringkat ini sebagai hasil penilaian bisnes semasa.

b. Peringkat kedua: Menganalisis Persekitaran ICT

Peringkat kedua mengandungi penilaian terhadap persekitaran dan senibina ICT semasa di UiTM mengikut lima (5) dimensi ICT iaitu Sumber Manusia, Sistem, Serahan (*Delivery*), Strategi dan Teknologi. Dua grid iaitu grid audit sistem aplikasi semasa dan grid strategik ICT dihasilkan sebagai rumusan penilaian ICT dan bisnes.

c. Peringkat ketiga: Membangun Strategi ICT

Pada peringkat ini, Strategi ICT yang mantap merupakan daya penggerak ke hadapan kepada transformasi UiTM ke arah universiti unggul yang tersohor. Ianya merangkumi:

i. Hala tuju strategik ICT;

ii. Strategi yang digunakan dalam mengenal pasti peluang-peluang ICT; dan

iii. Mengenalpasti potensi dan mengklasifikasi keutamaan peluang.

d. Peringkat keempat: Membangun Pelan Pelaksanaan

Peringkat akhir ini adalah untuk membangunkan Pelan Pelaksanaan peringkat tinggi (*high level implementation plan*) merangkumi strategi pelaksanaan, jadual pelaksanaan dan anggaran kos bagi program ICT yang dikenal pasti.

SEKSYEN 7

KESELAMATAN ICT

7.1 PENGENALAN

Seksyen ini menerangkan tentang penyataan dalam dasar keselamatan ICT yang merangkumi penyataan keselamatan, objektif, skop dan prinsip dalam keselamatan ICT. Ianya bagi memastikan pelaksanaan keselamatan ICT universiti adalah mengikut kaedah yang telah ditetapkan oleh Dasar Keselamatan ICT UiTM (DKICT).

7.2 PENYATAAN KESELAMATAN

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. Keselamatan ICT 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 aset ICT.

Terdapat empat (4) komponen asas keselamatan ICT iaitu:

a. Melindungi maklumat rahsia rasmi dan maklumat UiTM 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 hanya kepada pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

7.3 OBJEKTIF

Objektif utama Keselamatan ICT UiTM adalah seperti berikut:

a. Memastikan kelancaran operasi UiTM dan meminimumkan kerosakan atau kemusnahan;

b. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;

c. Mencegah salah guna atau kecurian aset ICT UiTM;

d. Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan; dan

e. Memperkemaskan pengurusan keselamatan ICT UiTM.

7.4 SKOP

Skop DKICT meliputi:

a. Aset ICT yang terdiri daripada perkakasan, perisian, perkhidmatan, data, maklumat dan manusia;

b. Premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem sokongan lain; dan

c. Kemudahan komunikasi.

7.5 PRINSIP KESELAMATAN ICT

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

a. Akses atas dasar "perlu mengetahui"

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53.

i. Hak akses minimum

Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat.

Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas.

ii. Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Bagi menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

b. Memastikan maklumat tepat dan lengkap;

c. Menentukan maklumat sedia untuk digunakan;

d. Menjaga kerahsiaan kata laluan;

e. Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan ICT yang ditetapkan;

f. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

g. Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.

b. Pengasingan

Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan untuk melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.

c. Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, server, peralatan rangkaian dan peralatan keselamatan ICT hendaklah dapat menjana dan menyimpan log tindakan keselamatan atau audit trail.

d. Pematuhan

DKICT UiTM hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT.

e. Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan pelan pemulihan bencana/kesinambungan perkhidmatan.

f. Saling Bergantungan

Setiap prinsip di atas adalah saling lengkap-melengkapi dan bergantung antara satu sama lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

SEKSYEN 8

PENGURUSAN & PENGGUNAAN INFRASTRUKTUR ICT

Seksyen 8 - PENGURUSAN & PENGGUNAAN INFRASTRUKTUR ICT

8.1 PENGENALAN

Seksyen ini menerangkan tentang peraturan dan tanggungjawab berkenaan perkara-perkara yang berhubung dengan infrastruktur ICT universiti supaya dapat diurus dengan baik dan teratur.

8.2 RANGKAIAN

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

a. 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:

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

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

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

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

v. *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Rangkaian;

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

vii. Semua perisian *sniffer* atau *network analyzer* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran pengurusan ICT;

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

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

x. Semua penyambungan rangkaian UiTM perlu mendapatkan kebenaran daripada Pengurusan ICT; dan

xi. Penggunaan *modem/ router/switch/wireless access point* atau sebarang perkakasan rangkaian persendirian adalah dilarang sama sekali.

b. Internet atau Intranet

i. UiTM perlu menyediakan dan memasang perisian *Web Content Filtering* Internet dan Intranet yang dilayari;

ii. Laman sesawang yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh universiti;

iii. Pengguna boleh memuat turun bahan yang dibenarkan serta tidak menyalahi undang-undang;

iv. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan dan ianya di bawah tanggungjawab pengguna; dan

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

c. Kebolehcapaian Pengguna (*User Accessibility*)

i. Hanya staf dan pelajar universiti dibenarkan mengakses ke rangkaian universiti;

ii. Pengguna luar perlu mendapatkan kebenaran Pengurusan ICT sebelum mengakses ke rangkaian UiTM; dan

iii. Penggunaan perisian pengintip (*sniffer*) atau penganalisis rangkaian (*network analyzer*) tanpa kebenaran Pengurusan ICT universiti adalah tidak dibenarkan.

d. Pengurusan Alamat IP

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

e. Sambungan Rangkaian

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

f. *Virtual Private Network* (*VPN*)

Kemudahan penggunaan *VPN* diberikan kepada pentadbir sistem dan rangkaian dengan kebenaran daripada Pengurusan ICT.

g. *Domain* dan *Sub-Domain*

Domain rasmi UiTM adalah www.uitm.edu.my dan penggunaan *sub-domain* hanyalah untuk kegunaan rasmi UiTM.

8.3 MEL ELEKTRONIK

Penggunaan e-mel universiti hendaklah merujuk kepada Garis Panduan Pengurusan ICT dan DKICT. Pengguna bertanggungjawab menjaga integriti sumber dan mematuhi etika penggunaan e-mel dan Internet berdasarkan Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003: Garis Panduan mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan.

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

a. Pengguna tidak dibenarkan memiliki lebih daripada satu (1) akaun e-mel rasmi universiti;

b. Setiap akaun e-mel rasmi individu yang disediakan adalah untuk kegunaan pemilik akaun dan tidak boleh digunakan oleh pihak lain tanpa kebenaran;

c. Pengguna disarankan menukar kata laluan akaun e-mel secara berkala;

d. Pengguna bertanggungjawab ke atas penyelenggaraan termasuk salinan sandar (*backup/archive*) *mailbox* masing-masing;

e. 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;

f. Kandungan e-mel perlu mematuhi Kod Kandungan Komunikasi dan Multimedia Malaysia. Pihak Pengurusan ICT berhak untuk menyekat akses e-mel atas arahan Pengurusan UiTM; dan

g. Kemudahan e-mel akan ditamatkan selepas staf tamat perkhidmatan mengikut tempoh yang ditetapkan.

8.4 TELESIDANG DAN LIVE STREAMING

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

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

a. Telesidang

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

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

iii. Setiap PTJ perlu memastikan kemudahan telesidang yang digunakan untuk tujuan rasmi menggunakan perisian yang dibenarkan dan diperolehi oleh pihak universiti; dan

iv. Kandungan pada semua bahan telesidang perlu mematuhi Kod Kandungan Komunikasi dan Multimedia Malaysia.

b. *Live Streaming*

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

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

iii. Kandungan pada semua bahan *live streaming* perlu mematuhi Kod Kandungan Komunikasi dan Multimedia Malaysia.

8.5 LAMAN SESAWANG

Pemilik laman sesawang mesti mematuhi Dasar Pengurusan Laman Sesawang Universiti dan Garis Panduan Membangun Laman Web dan Tapak *Hosting*. Jawatankuasa Laman Web PTJ bertanggungjawab untuk menjaga integriti sumber dan bahan laman sesawang.

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

a. Pengurusan ICT 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 tapak atau ruang 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 sesawang;

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 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 daripada 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 selepas staf tamat perkhidmatan mengikut tempoh yang ditetapkan; dan

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

8.6 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.

8.7 PUSAT DATA

a. Perkhidmatan

Pusat Data menyediakan perkhidmatan *server* secara maya, storan dan sandaran bagi PTJ di seluruh UiTM selain bertanggungjawab untuk memastikan bahawa data dan maklumat dalam bentuk digital yang dimiliki oleh universiti disimpan dalam infrastruktur yang stabil, sentiasa mudah dicapai dan selamat.
Perkara-perkara yang perlu diberi perhatian adalah:

i. Penggunaan perkhidmatan Pusat Data perlu mendapat kelulusan daripada Pengurusan Pusat Data;

ii. Pengurusan Pusat Data perlu memastikan infrastruktur selamat bagi menjamin keselamatan maklumat universiti; dan

iii. Pentadbir sistem bertanggungjawab melaksanakan penyelenggaraan sistem masing-masing seperti mengemaskini sistem operasi dan perisian-perisian yang digunakan adalah terkini.

b. Prosedur masuk

Pelaksanaan prosedur ini hendaklah merujuk kepada DKICT UiTM. Kemasukan ke Pusat Data dihadkan kepada staf yang dibenarkan mengikut klasifikasi yang ditetapkan seperti berikut:

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

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

iii. Lawatan Pusat Data – Lawatan ke Pusat Data perlu mendapat kebenaran Pengurusan ICT.

8.8 SANDARAN DAN PEMULIHAN (*BACKUP AND RECOVERY*)

Pelaksanaan *backup and recovery* hendaklah merujuk kepada DKICT UiTM. Polisi *backup and recovery* ditentukan melalui persetujuan di antara Pengurusan Pusat Data dan pengguna perkhidmatan pusat data serta merangkumi perkara berikut:

a. Kekerapan *backup*;

b. Jenis *backup* (*full* atau *incremental*); dan

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

Ujian *restore* perlu dilaksanakan bagi memastikan integriti *backup.*

8.9 PENGURUSAN *HIGH-END COMPUTING EQUIPMENT* (*HCE*)

High-end Computing equipment (HCE) boleh didefinisikan sebagai perkakasan ICT berkeupayaan tinggi yang memberikan perkhidmatan berpusat seperti:

a. *Server*;

b. *Storage Area Network* (SAN);

c. *Network Attached Storage* (NAS);

d. *Virtual Tape Library* (VTL);

e. *Tape Library*; dan

f. *Appliances (contoh: security appliances).*

Tanggungjawab dan Hak Milik

a. Semua perkakasan HCE yang diperolehi mengikut tatacara perolehan atau sumbangan daripada mana-mana pihak adalah hak milik UiTM sepenuhnya.

b. PTJ yang membuat perolehan HCE adalah bertanggungjawab sepenuhnya kepada perkakasan tersebut. Tanggungjawab ini boleh dipecahkan kepada:

   i. Pemilik adalah PTJ yang membuat perolehan kepada perkakasan HCE bertanggungjawab bagi memastikan perkakasan berada di dalam keadaan baik; dan

   ii. Pentadbir Sistem bertanggungjawab untuk mengurus dan mentadbir perkakasan.

c. Pengurusan perkakasan HCE perlu mengikut amalan terbaik seperti yang terdapat dalam Garis Panduan Pengurusan ICT.

d. PTJ bertanggungjawab untuk memantau perkakasan HCE dari sebarang kerosakan dan membuat proses pemulihan secepat mungkin.

e. Pentadbir sistem bertanggungjawab untuk memastikan perkakasan dilengkapi dengan ciri-ciri keselamatan.

f. Jika perkhidmatan perkakasan HCE sudah tidak diperlukan lagi, PTJ bertanggungjawab untuk menghentikan operasi perkakasan tersebut sehingga ia dilupuskan.

g. PTJ bertanggungjawab untuk melupuskan perkakasan HCE yang sudah usang dan tidak digunakan lagi.

SEKSYEN 9

PENGURUSAN PERKAKASAN & PERISIAN ICT

9.1 PENGENALAN

Seksyen ini menerangkan tentang tanggungjawab pengguna dan pihak UiTM berkaitan 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 peribadi (PC), komputer riba (*notebook*), pencetak (*printer*), tablet PC dan pengimbas (*scanner*), perkakasan rangkaian komputer, perkakasan pusat data (*server, storage*), *External Hard Disk*, Aksesori komputer (*mouse,keyboard*).

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

a. Hak Pemilikan

i. 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;

ii. Bagi perkakasan ICT, maklumat pemilik mestilah direkodkan; dan

iii. Perkakasan tersebut tidak dibenarkan untuk dijual, disewa, dipinjam, disebar, diberi kepada individu atau organisasi tanpa kebenaran pengurusan UiTM.

b. Pengagihan Perkakasan ICT

Agihan perkakasan ICT hendaklah mengikut Garis Panduan Pengurusan ICT terkini.

c. Geran Perkakasan ICT

Pembelian perkakasan ICT Secara Geran hendaklah mengikut Garis Panduan Pengurusan ICT terkini.

d. Peminjaman Perkakasan ICT

Peminjaman perkakasan ICT hendaklah mengikut Garis Panduan Pengurusan ICT terkini.

e. Baikpulih dan Penyelenggaraan Perkakasan ICT

i. Baikpulih dan selenggaraan perkakasan ICT tertakluk kepada Pekeliling Bendahari mengenai Tatacara Pengurusan Aset Alih UiTM;

ii. Sokongan penyelenggaraan perkakasan ICT PTJ perlu diselaras oleh Pengurusan ICT bagi tujuan pemantauan dan inventori; dan

iii. Sebarang isu teknikal yang dihadapi dalam penggunaan perkakasan ICT perlu dimajukan melalui saluran bantuan perkhidmatan ICT yang disediakan.

f. Pelupusan Perkakasan ICT

i. Pelupusan perkakakasan ICT adalah tertakluk kepada Pekeliling Bendahari mengenai Tatacara Pengurusan Aset Alih UiTM; dan

ii. Data di dalam perkakasan ICT adalah tanggungjawab pengguna dan hendaklah dihapuskan sebelum pelupusan/pemulangan mengikut Dasar Keselamatan ICT UiTM untuk mengelakkan daripada disalahgunakan oleh pihak yang tidak bertanggungjawab.

g. Tanggungjawab Pengguna

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

h. Tanggungjawab Pihak Ketiga

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

i. Kehilangan Perkakasan ICT

Kehilangan perkakasan ICT hendaklah mengikut Pekeliling Bendahari mengenai Tatacara Pengurusan Aset Alih Universiti Teknologi MARA (Kehilangan) terkini.

9.3 PERISIAN ICT

Perisian ICT adalah perisian yang digunakan untuk menyokong sistem penyampaian perkhidmatan universiti merangkumi pengajaran dan pembelajaran, penyelidikan, dan pentadbiran UiTM.

UiTM tidak akan bertanggungjawab terhadap sebarang penggunaan perisian ICT tanpa lesen.

Semua perisian yang dibekalkan oleh UiTM tidak boleh dijual, disewa, dipinjam, disalin semula, dilesenkan semula, disebar atau diberi kepada individu atau organisasi tanpa kebenaran pengurusan UiTM.

a. Tanggungjawab Pengguna

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

b. 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 bagi perkakasan dan perisian ICT mestilah mematuhi prosedur perolehan UiTM seperti Pekeliling Bendahari, Pekeliling Perbendaharaan, Pekeliling Naib Canselor dan lain-lain pekeliling yang boleh diterima pakai.

SEKSYEN 10

PENGURUSAN SISTEM APLIKASI & INTEGRASI

Seksyen 10 - PENGURUSAN SISTEM APLIKASI & INTEGRASI

10.1 PENGENALAN

Seksyen ini menerangkan tentang pengurusan sistem, aplikasi dan integrasi ICT universiti. Ianya bagi memastikan bahawa pengurusan sistem, aplikasi dan integrasi ICT adalah berdasarkan *Enterprise Architecture* universiti dan selari dengan hala tuju strategik universiti.

10.2 KATALOG SISTEM

Semua sistem dan aplikasi universiti perlu didaftar oleh pemilik sistem kepada pihak pengurusan ICT-merujuk kepada Garis Panduan Pengurusan ICT.

10.3 PEMILIKAN SISTEM

Setiap sistem dan aplikasi yang dibangunkan mesti mempunyai pemilik yang bertanggungjawab ke atas proses kerja sistem yang dibangunkan.

10.4 PERMOHONAN PEMBANGUNAN

Setiap permohonan pembangunan sistem dan aplikasi baharu atau perubahan terhadap sistem dan aplikasi sedia ada kepada versi terbaharu mesti dimajukan secara rasmi kepada Pengurusan ICT.

10.5 PEMBANGUNAN SISTEM

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

10.6 KAWALAN CAPAIAN SISTEM

Kawalan capaian kepada sistem dan aplikasi ditentukan oleh pemilik sistem dan perlu mematuhi Dasar Keselamatan ICT UiTM.

10.7 INTEGRASI SISTEM DAN DATA

Setiap permohonan integrasi perlu mendapatkan kebenaran daripada pemilik sistem dan aplikasi terlebih dahulu sebelum sebarang proses integrasi dilaksanakan. Semua proses integrasi data sistem dan aplikasi adalah tertakluk kepada Garis Panduan Pengurusan ICT.

10.8 KUALITI DATA DAN MAKLUMAT DALAM SISTEM

Pemilik sistem dan aplikasi bertanggungjawab ke atas kesahihan data dan maklumat.

10.9 DOKUMENTASI SISTEM DAN APLIKASI

Setiap pembangunan sistem dan aplikasi perlu mempunyai dokumentasi merujuk kepada Garis Panduan Pengurusan ICT.

10.10 LATIHAN SISTEM DAN APLIKASI

Setiap sistem dan aplikasi yang dibangunkan perlu diberi latihan kepada pemilik sistem dan pengguna.

10.11 SOKONGAN DAN PENYELENGGARAAN SISTEM DAN APLIKASI

Sistem dan aplikasi yang diselenggara perlu melalui proses ujilari oleh pemilik sistem dan diberi latihan (jika perlu).

10.12 KESINAMBUNGAN BISNES DAN PEMULIHAN BENCANA

Bagi menjamin kesinambungan bisnes dan pemulihan bencana, operasi *backup* dan *restore* mesti dilakukan berdasarkan Dasar Keselamatan ICT UiTM.

10.13 PENAMATAN SISTEM

Pemakluman penamatan sistem dan aplikasi secara rasmi mesti diperolehi daripada pemilik sistem berkenaan. Sistem dan aplikasi yang tidak digunakan lagi akan dikeluarkan daripada persekitaran ICT universiti.

SEKSYEN 11

PENGURUSAN PANGKALAN DATA

Seksyen 11 - PENGURUSAN PANGKALAN DATA

11.1 PENGENALAN

Seksyen ini menerangkan tentang hal ehwal pengurusan pangkalan data bagi meningkatkan kebolehgunaan, kebolehpercayaan, integriti dan kebolehsediaan pangkalan data universiti. Ianya bagi memastikan pengurusan pangkalan data selari dengan hala tuju strategik universiti.

11.2 PENGURUSAN PANGKALAN DATA

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

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

c. Semua pangkalan data mesti diselenggara dan dipantau.

11.3 TADBIR URUS PANGKALAN DATA

Pentadbir pangkalan data dan pentadbir sistem perlu dikenalpasti. Peranan pentadbir pangkalan data adalah seperti yang terkandung dalam Garis Panduan Pengurusan ICT UiTM.

11.4 KEBENARAN CAPAIAN PANGKALAN DATA

Capaian pangkalan data diuruskan oleh pentadbir pangkalan data berdasarkan permohonan. Kawalan capaian terhadap pangkalan data adalah berdasarkan Dasar Keselamatan ICT UiTM.

11.5 SANDARAN DAN PEMULIHAN (*BACKUP AND RECOVERY*)

Semua pangkalan data perlu melaksanakan sandaran secara berjadual. Pengurusan sandaran dan pemulihan pangkalan data adalah berdasarkan Garis Panduan Pengurusan ICT UiTM.

SEKSYEN 12

E-PEMBELAJARAN

Seksyen 12 - E-PEMBELAJARAN

12.1 TUJUAN

Tujuan dasar ini dibentuk adalah sebagai panduan bagi pelaksanaan e-Pembelajaran di universiti. Matlamat utama dasar ini adalah bagi memastikan penggunaan teknologi maklumat dan komunikasi sebagai medium bagi meningkatkan kualiti penyampaian dan pembelajaran. Dasar yang dibentuk ini juga secara tidak langsung bertujuan membangunkan modal insan bertaraf dunia serta menjadikan UiTM sebuah universiti unggul yang berteraskan kesarjanaan dan kecemerlangan akademik.

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

12.2 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;
   vi. Pengurusan dan penyelenggaraan pelayan (*server*) bagi sistem e-Pembelajaran; dan
   vii. Pelaporan keberkesanan sistem e-Pembelajaran.

b. Tanggungjawab pemilik sistem e-Pembelajaran dalam tadbir urus e-Pembelajaran adalah seperti berikut:
   i. Membangun dan mengurus sistem e-Pembelajaran bagi tujuan penyampaian dan pembelajaran;
   ii. Memantau dan menyelaras pembangunan bahan pengajaran dan pembelajaran;
   iii. Menjalankan aktiviti penyelidikan dan pembangunan berkaitan dengan e-Pembelajaran;
   iv. Menyediakan garis panduan e-Pembelajaran; dan
   v. Membuat analitik penyampaian dan pembelajaran dengan mengggunakan kaedah e-Pembelajaran.

c. Tanggungjawab pelaksana sistem e-Pembelajaran dalam tadbir urus e-Pembelajaran adalah seperti berikut:

   i. Memantau dan menyelaras aktiviti e-Pembelajaran;

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

   iii. Memastikan tenaga pengajar dan pelajar mematuhi dasar dan garis panduan e-Pembelajaran universiti;

   iv. Menyediakan bahan tentang penggunaan sistem e-Pembelajaran;

   v. Membuat promosi bagi memastikan kelestarian penggunaan sistem e-Pembelajaran; dan

   vi. Membuat penilaian terhadap keberkesanan penggunaan sistem e-Pembelajaran.

d. 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.

e. 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;

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

   v. Memberi maklum balas untuk meningkatkan mutu sistem e-Pembelajaran.

f. 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.

g. 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.

12.3 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 pengajaran dan pembelalajaran. 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. Penggunaan menyeluruh pada sistem e-Pembelajaran universiti perlu dipertingkatkan dari masa kesemasa bagi memastikan sistem e-Pembelajaran yang disediakan sentiasa terkehadapan.

e. Mempunyai satu mekanisma bagi menangani masalah plagiarisma pada tugas-tugas pelajar.

f. 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.

g. 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.

h. 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

Seksyen 13 - PERISIAN SUMBER TERBUKA

13.1 PENGENALAN

Seksyen ini menerangkan tentang hal ehwal perisian sumber terbuka bagi memastikan penggunaan, perkongsian maklumat dan teknologi yang digunakan adalah mengikut dasar yang ditetapkan.

13.2 PENGGUNAAN

Penggunaan perisian sumber terbuka adalah berdasarkan kepada Dasar Sektor Awam *Open Source Software (OSS) Implementation Guidelines by Malaysian Public Sector Open Source Software (OSS) Initiative* daripada MAMPU.

13.4 PERKONGSIAN MAKLUMAT

Sebarang maklumat atau penemuan dalam penggunaan perisian sumber terbuka digalakkan untuk dikongsi dalam komuniti sokongan.

13.5 TEKNOLOGI

a. Teknologi yang digunakan hendaklah versi yang stabil dan mempunyai komuniti sokongan yang berterusan.

b. Pasukan teknikal haruslah mempunyai kemahiran yang diperlukan mengikut perkembangan teknologi yang terkini.

13.6 PELAKSANAAN

Pelaksanaan perisian sumber terbuka hendaklah berdasarkan kepada panduan pelaksanaan iaitu:

a. Sesuai untuk tujuan penggunaan;

b. Tidak mengganggu sistem penyampaian perkhidmatan universiti;

c. Produk yang digunakan atau dibangunkan berasaskan teknologi perisian sumber terbuka boleh beroperasi dengan lain-lain produk *proprietary*; dan

d. Mengoptimumkan infrastruktur ICT sedia ada dan kepakaran dalaman.

SEKSYEN 14

TEKNOLOGI HIJAU

14.1 PENGENALAN

Seksyen ini menerangkan tentang amalan penggunaan peralatan 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

Perolehan produk ICT digalakkan mempunyai ciri-ciri ICT Hijau yang bertujuan untuk mengurangkan impak negatif operasi ICT terhadap persekitaran.

14.4 PENGGUNAAN

Garis Panduan Penggunaan ICT Ke Arah ICT Hijau Dalam Perkhidmatan Awam yang disediakan oleh MAMPU dijadikan asas dalam pembudayaan amalan ICT Hijau universiti.

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

PERKHIDMATAN PENGKOMPUTERAN AWAN AWAM

Seksyen 15 - PERKHIDMATAN PENGKOMPUTERAN AWAN AWAM

15.1 PENGENALAN

Seksyen ini menerangkan aspek bagi penggunaan perkhidmatan pengkomputeran awan awam.

15.2 PEMAKAIAN

Dasar ini merangkumi skop semua model perkhidmatan pengkomputeran awan awam (*XaaS*) seperti Perisian sebagai Perkhidmatan *(Software-as-a-Service (SaaS))*, Infrastruktur sebagai Perkhidmatan *(Infrastructure-as-a-Service (IaaS))* dan Platform sebagai Perkhidmatan *(Platform-as-a-Service (PaaS))*.

a. Sebarang penggunaan perkhidmatan pengkomputeran awan awam seperti perkongsian maklumat, pemprosesan data dan sebagainya hendaklah mematuhi segala peruntukan undang-undang, peraturan, pekeliling, polisi dan arahan-arahan yang dikeluarkan dari semasa ke semasa yang dikuatkuasakan oleh Kerajaan Malaysia dan UiTM.

b. Ia juga merangkumi segala data dan maklumat rasmi milik UiTM dalam sistem penyampaian perkhidmatan universiti.

c. Maklumat terperingkat seperti yang digariskan dalam Dasar Pengurusan Maklumat Rasmi Universiti adalah dilarang ditempatkan dalam persekitaran awan awam.

d. Semua warga universiti hendaklah pada setiap masa menjaga dan mengekalkan integriti serta kerahsiaan segala maklumat universiti selari dengan Dasar Pengurusan Maklumat Rasmi Universiti.

15.3 PERANAN

a. Pentadbir

Akaun Pentadbir bagi perkhidmatan pengkomputeran awan awam yang dipakai atau dilanggan hendaklah dimiliki dan diuruskan oleh staf UiTM sendiri.

b. Pengguna

i. Pengguna bertanggungjawab ke atas keselamatan aplikasi dan maklumat yang disimpan dalam persekitaran pengkomputeran awan awam.

ii. Pengguna bertanggungjawab untuk membuat sandaran *(backup)* ke atas data dan maklumat yang disimpan dalam persekitaran pengkomputeran awan awam.

PEGAWAI PENYEDIA DOKUMEN DASAR ICT

1. **Prof. Datin Dr. Noor Habibah Arshad**, Penolong Naib Canselor (Infostruktur)
2. **Puan Hajah Sariani Sarijo**, Pengarah Pengurusan ICT
3. **Prof. Madya Ts. Dr. Nor Shahniza Kamal Bashah**, Ketua Bahagian Dasar dan Strategik ICT
4. **Ts. Maznifah Salam @ Mohd Sahalan**, Ketua Bahagian Keselamatan ICT
5. **Encik Shamsuri Awang Seman**, Ketua Bahagian Infrastruktur ICT
6. **Encik Mohd Hairy Mohamadiah**, Ketua Bahagian Sistem Maklumat
7. **Encik Syamsudin Mudzamil**, Ketua Bahagian Operasi ICT
8. **Puan Hajah Ziraizratul Mohaini Mohamat**, Ketua Bahagian Pengurusan Projek ICT
9. **Encik Gazairi Ghazali**, Ketua Unit Sistem Utama, Bahagian Sistem Maklumat
10. **Encik Zamani Umar Husin**, Ketua Unit Integrasi, Bahagian Sistem Maklumat
11. **Puan Khairunnisa Musa**, Ketua Unit Sistem Sokongan, Bahagian Sistem Maklumat
12. **Puan Nor Azni Abdullah Zawawi,** Ketua Unit Pangkalan Data, Bahagian Sistem Maklumat
13. **Puan Ezabarena Radzi**, Ketua Unit Governan ICT, Bahagian Dasar & Strategik ICT
14. **Ts. Dr. Hajah Kamaliyah Sarjo @ Hj Ahmad**, Ketua Unit Perancangan Strategik ICT, Bahagian Dasar & Strategik ICT
15. **Encik Ahmad Farhan Mohd Fadzil**, Ketua Unit Pusat Data, Bahagian Infrastruktur ICT
16. **Puan Suraya Che Kamal**, Ketua Unit Rangkaian, Bahagian Infrastruktur ICT
17. **Encik Abdul Hadi Milok**, Ketua Unit Pusat Pemulihan Bencana, Bahagian Infrastruktur ICT
18. **Encik Mohd Khanafi Haron**, Ketua Unit Automasi Pejabat, Bahagian Operasi ICT
19. **Ts. Shariza Mohd Said**, Ketua Unit Pengkomputeran Pengguna, Bahagian Operasi ICT
20. **Puan Intan Zuriaty Mujirimi**, Ketua Unit Perkhidmatan ICT Zon, Bahagian Operasi ICT
21. **Encik Kamaruddin Mahad**, Ketua Unit Operasi Keselamatan & Perlindungan Maklumat, Bahagian Keselamatan ICT
22. **Ts. Mohd Firdaus Fairoz Zairolazhar**, Ketua Unit Kawalan & Pematuhan Keselamatan ICT
23. **Ts. Dr. Nur Idora Abdul Razak**, Ketua Unit Penilaian Produk ICT, Bahagian Pengurusan Projek ICT

24. **Ts. Siti Hajar Ismail**, Ketua Unit Pengurusan dan Pemantauan Projek & Kontrak ICT, Bahagian Pengurusan Projek ICT
25. **Puan Siti Sapura Jailani**, Pegawai Teknologi Maklumat Kanan
26. **Puan Faidah Mohammad**, Pegawai Teknologi Maklumat Kanan
27. **Puan Samsuriwati Sohaini**, Pegawai Teknologi Maklumat Kanan
28. **Puan Nik Darwina Ibrahim**, Pegawai Teknologi Maklumat

PENYUNTING

1. **Prof. Madya Ir. Ts. Dr. Hajah Juliana Johari**, Penolong Naib Canselor (Infostruktur)
2. **Ts. Dr. Hajah Kamaliyah Sarjo @ Hj. Ahmad**, Ketua Bahagian Dasar dan Strategik ICT
3. **Puan Ezabarena Radzi**, Ketua Unit Governan ICT, Bahagian Dasar & Strategik ICT
4. **Puan Nik Darwina Binti Ibrahim**, Pegawai Teknologi Maklumat

GRAFIK & REKALETAK DOKUMEN

1. **Encik Jasni Ghani**, Penolong Pegawai Teknologi Maklumat Tertinggi

ISBN 978-967-19445-0-9

9 7 8 9 6 7 1 9 4 4 5 0 9

Jabatan Infostruktur
Aras 5 & 6, Menara Sultan Abdul Aziz Shah
Universiti Teknologi MARA
40450 Shah Alam, Selangor