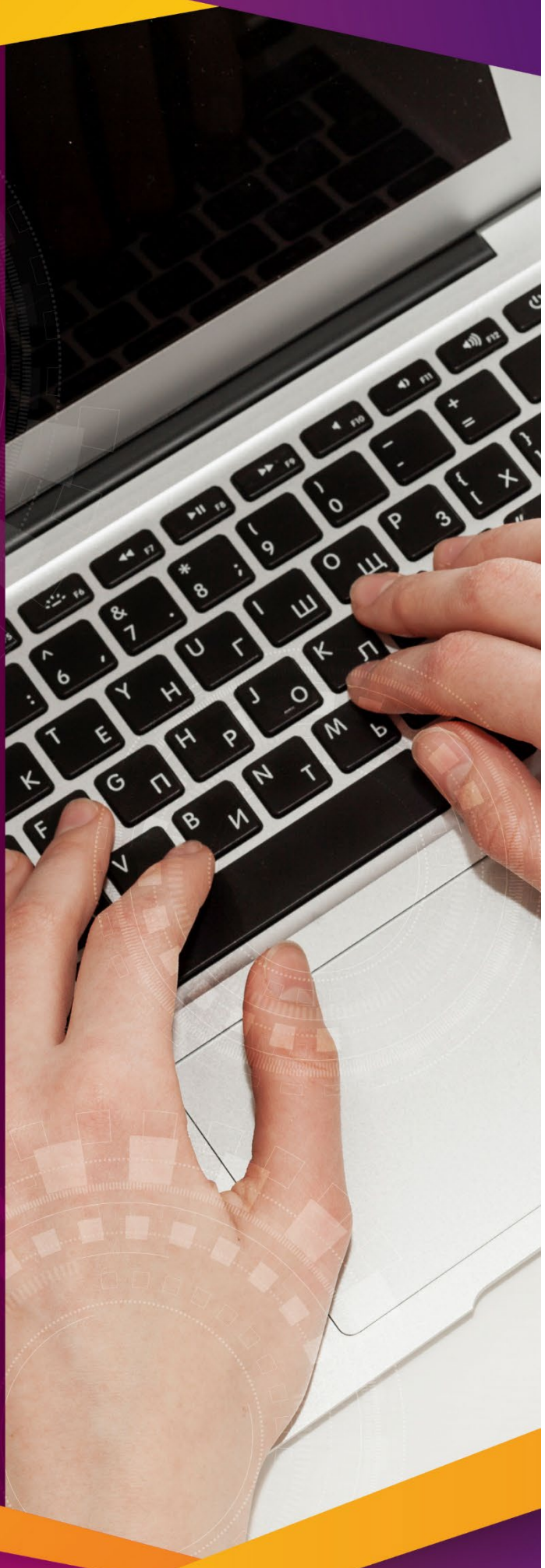
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

DASAR ICT UTeM

Versi 2.0



ISI KANDUNGAN

REKOD PINDAAN DOKUMEN

Versi	Keterangan Pindaan	Kelulusan	Tarikh Kuat Kuasa
2.0	Pengemaskinian Dasar ICT 2.0 selaras dengan perubahan Standard MS ISO/IEC 27001:2022	Mesyuarat Lembaga Pengarah Universiti (LPU) Bilangan 8 /2025	28 Ogos 2025

DASAR UTAMA

1.0 PENDAHULUAN

1.1 Pejabat CDO bertanggungjawab menyediakan perkhidmatan ICT secara menyeluruh di samping melaksanakan tugasnya dalam membangunkan, melaksanakan dan menyelenggarakan infrastruktur dan infostruktur ICT dengan memastikan penggunaan ICT dalam kalangan pengguna di tahap yang maksimum dan berkualiti.

1.2 Dalam menyokong perlaksanaan pelan strategik maka setiap projek ICT yang akan dilaksanakan hendaklah memberikan suatu impak yang besar dan menyeluruh kepada pengguna. Maka setiap pencapaian dan perancangan perlu mengambil kira pelan strategik universiti dan pelan strategik yang melibatkan ICT.

1.3 Selaras dengan tanggungjawab tersebut, Dasar Utama ini disediakan untuk dijadikan panduan kepada pengurusan UTeM dalam membuat sebarang keputusan berkaitan perancangan, keselamatan dan pembangunan ICT UTeM.

1.4 Dasar Utama ini terdiri kepada tujuh (7) bab seperti di bawah:

Bab 1: Dasar Pengurusan ICT

Dasar ini menerangkan secara umum aspek pengurusan organisasi dan pembangunan ICT UTeM melalui JPICT.

Bab 2: Dasar Perkakasan

Dasar ini bertujuan untuk memastikan pengurusan perkakasan dan perisian automasi yang melibatkan tanggungjawab pengguna dan PTj diuruskan dengan lebih baik. Dasar ini juga adalah berkaitan perolehan, pengagihan dan skop penyelenggaraan, baik pulih, pelupusan serta agihan semula perkakasan.

Bab 3: Dasar Server

Dasar ini bertujuan untuk menerangkan tentang peraturan yang perlu dipatuhi serta memberikan panduan berkaitan pengurusan server di UTeM.

Bab 4: Dasar Rangkaian

Dasar ini merangkumi penyediaan, penggunaan dan pengoperasian merangkumi rangkaian UTeM, penyambungan rangkaian, penyelenggaraan rangkaian dan penyambungan telefon.

Bab 5: Dasar Aplikasi

Dasar ini bertujuan memastikan sistem aplikasi yang dibangunkan adalah efisyen serta mempunyai kebolehpercayaan yang tinggi bagi menyokong pengurusan dan pentadbiran, pengajaran dan pembelajaran, penyelidikan dan sebagainya.

Bab 6: Dasar Akauntabiliti

Dasar ini menyatakan tanggungjawab pihak yang terlibat dengan penggunaan kemudahan ICT berkenaan ciri-ciri keselamatam maklumat, capaian maklumat, pematuhan data dalam rangkaian dan pengurusan maklumat sulit.

Bab 7: Dasar Keselamatan Siber

DKS ini disediakan dengan tujuan untuk melindungi kerahsiaan, integriti, dan ketersediaan data dan maklumat di UTeM merangkumi arahan, peraturan, garis panduan, dan amalan yang ditetapkan untuk melindungi data dan maklumat daripada capaian yang tidak sah, kehilangan, atau pendedahan yang tidak dibenarkan.

2.0 TAFSIRAN, AKRONIM DAN INTERPRETASI

2.1 TAFSIRAN

(a) Dalam Dasar Utama ini melainkan jika konteksnya menghendaki makna yang lain:

Pernyataan	Definisi
akaun pengguna	satu kaedah bagi membenarkan seseorang pengguna untuk membuat capaian terhadap sesuatu sistem. Kebiasaannya akaun pengguna melibatkan penggunaan kata nama dan kata laluan seperti akaun e-mel, portal, sistem dan rangkaian
Akta 605	Akta Badan-Badan Berkanun (Tatatertib dan Surcaj) 2000 termasuklah apa-apa pindaan dan apa-apa perundangan subsidiari di bawahnya
aset ICT	data, maklumat, perkakasan, perisian, aplikasi, dokumentasi dan sumber manusia serta premis berkaitan dengan ICT yang berada di bawah tanggungjawab UTeM
data	ertinya himpunan mentah mengenai sesuatu benda, kejadian, orang atau entiti yang boleh terdiri daripada perkataan, angka atau gambar
Dasar Akauntabiliti	Dasar Akauntabiliti dan Kerahsiaan Maklumat
Dasar Aplikasi	Dasar Sistem Aplikasi
Dasar Pengurusan ICT	Dasar Pengurusan Teknologi Maklumat dan Komunikasi
Dasar Perkakasan	Dasar Perkakasan dan Perisian Automasi Pejabat
Dasar Rangkaian	Dasar Perkhidmatan Rangkaian dan Telekomunikasi
Dasar Server	Dasar Perkhidmatan Server
dokumen	semua himpunan atau kumpulan bahan atau dokumen yang disimpan dalam bentuk media cetak, salinan lembut *(softcopy)*, elektronik, dalam talian,

Pernyataan	Definisi
	kertas lut sinar, risalah atau slaid
insiden Keselamatan	musibah *(adverse event)* yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut
infrastruktur ICT	perkakasan, perisian dan perlesenan
internet	sistem rangkaian komunikasi global yng merangkumi infrastruktur perkakasan dan perisian yang menyediakan sambungan rangkaian global di antara komputer. Internet dalam skop UTeM adalah pekhidmatan rangkaian yang membolehkan pengguna mengakses sumber maklumat di seluruh dunia secara atas talian
intranet	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 UTeM adalah perkhidmatan rangkaian yang membolehkan pengguna mengakses sumber makumat di dalam kampus UTeM secara atas talian
IP	*Internet Protocol* iaitu satu set nombor unik yang diberikan kepada setiap peranti yang terhubung ke rangkaian internet
kampus	(a) Kampus Induk; (b) Kampus Teknologi; (c) Kolej-kolej kediaman; dan apa-apa bangunan atau tempat yang yang diwujudkan oleh UTeM dari semasa ke semasa
kemudahan ICT	perkakasan, peralatan dan perkhidmatan yang berkaitan teknologi maklumat dan telekomunikasi yang disediakan oleh UTeM bagi tujuan pengurusan, pentadbiran, penyelidikan, pengajaran dan pembelajaran serta operasi pengguna

Pernyataan	Definisi
KTP	Kaedah-Kaedah Universiti dan Kolej Universiti (Universiti Teknikal Malaysia Melaka) versi terkini 2024 termasuklah apa-apa pindaan dan apa-apa perundangan subsidiari di bawahnya
kod sumber sistem aplikasi	sebarang 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
LAN	*Local Area Network* iaitu rangkaian komputer yang merangkumi kawasan fizikal yang kecil
maklumat	hasil daripada pengumpulan, pemprosesan dan penganalisaan data yang boleh digunakan untuk membuat sesuatu keputusan
maklumat terperingkat	apa-apa maklumat, data atau kedua-duanya yang dikelaskan sebagai rahsia rasmi di bawah seksyen 2 Akta Rahsia Rasmi 1972 iaitu;- “rahsia” ertinya dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan negara, menyebabkan kerosakan besar kepada kepentingan dan martabat negara Malaysia atau memberi keuntungan besar kepada sesebuah kuasa asing hendaklah diperingkatkan **Rahsia**; “rahsia besar” ertinya dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada negara Malaysia, hendaklah diperingkatkan **Rahsia Besar**; “sulit” ertinya dokumen rasmi, maklumat rasmi dan

Pernyataan	Definisi
	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 hendaklah diperingkatkan **Sulit**; "terhad" ertinya dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan **Rahsia Besar, Rahsia atau Sulit** tetapi berkehendakkan juga diberi satu tahap perlindungan keselamatan hendaklah diperingkatkan **Terhad.**
MAN	*Metropolitan Area Network* iaitu rangkaian komputer yang meliputi suatu kawasan geografi yang agak luas berbanding dengan rangkaian yang diliputi oleh LAN untuk berhubungan ke semua kampus UTeM
pegawai aset	ertinya pegawai dilantik yang menguruskan aset dan stor PTj mengikut peraturan yang telah ditetapkan
Pegawai Pengelas	ertinya pegawai yang dilantik oleh kementerian yang bertanggungjawab terhadap pengajian tinggi di bawah seksyen 2B Akta Rahsia Rasmi 1972
pelan strategik	Pelan Strategik Universiti Teknikal Malaysia Melaka
pembangun sistem	Pegawai Teknologi Maklumat atau Penolong Pegawai Teknologi Maklumat atau individu yang bertanggungjawab membangun dan menyelenggara sesuatu sistem maklumat
pemilik aset	individu atau PTj yang bertanggungjawab untuk aset
pemilik data	individu atau PTj yang bertanggungjawab untuk data di dalam sistem
pemilik projek	pihak yang bertanggungjawab ke atas hampir

Pernyataan	Definisi
	keseluruhan proses kerja projek tersebut. Pemilik projek memainkan peranan utama dalam menentukan keperluan, spesifikasi dan ciri-ciri serahan (produk atau perkhidmatan) yang akan dihasilkan oleh sesuatu projek
pemilik proses	PTj yang bertanggungjawab untuk proses tertentu di dalam sistem yang dibangunkan
pemilik sistem	pihak yang memohon sesuatu sistem maklumat dibangunkan dan memiliki serta mengawal data secara majoriti
pentadbir akses	staf yang dilantik mentadbir akses pengguna untuk sistem maklumat universiti
pentadbir ICT	staf yang bertanggungjawab mengurus, mengawal, memantau dan menyelenggara sesuatu sistem maklumat di bawah seliaannya.
pentadbir rangkaian	staf yang bertanggungjawab mengurus, mengawal, memantau dan menyelenggara operasi dan keselamatan rangkaian universiti
pengurus projek	staf yang bertanggungjawab merancang dan mengurus projek supaya projek berjaya disiapkan mengikut skop, tempoh masa, kos dan kualiti yang telah ditetapkan
pengguna	“pelajar” ertinya seseorang yang mendaftar sesuatu program akademik sama ada sepenuh masa, separuh masa atau siswazah di UTeM; “pihak luar” ertinya mana-mana orang selain staf dan pelajar seperti pembekal, pakar runding dan sebagainya; dan “staf” ertinya mana-mana orang yang diambil kerja oleh UTeM sama ada secara tetap, kontrak,

Pernyataan	Definisi
	sementara, sambilan dan termasuk seseorang yang berkhidmat di UTeM dan di luar UTeM secara pinjaman
pengguna akhir	pengguna yang menggunakan semua sistem yang telah dibangunkan
Pengurus ICT	staf yang menguruskan Pusat Data, Rangkaian dan sumber ICT
perkakasan	keseluruhan komponen jenis fizikal yang dihubungkan secara terus dengan komputer atau sistem yang lain dan merupakan suatu alat yang digunakan sebagai input, aktiviti pemprosesan serta output sesuatu operasi
perisian automasi pejabat	konfigurasi perkakasan komputer, rangkaian dan perisian yang digunakan untuk melaksanakan kerja dengan bijak dan mengoptimumkan tatacara Pejabat sedia ada
PTj	Fakulti/Sekolah/Institut/Pejabat/Pusat atau apa-apa jua nama ia disebut yang ditubuhkan oleh UTeM dari semasa ke semasa termasuk pihak berkuasa UTeM ("PBU") yang tidak mempunyai kuasa kewangan
Private IP	alamat IP yang dikhaskan untuk rangkaian dalaman seperti LAN dan MAN dan tidak disebarkan ke internet
Public IP	alamat IP yang dikhaskan untuk kegunaan rangkaian luar seperti WAN (internet)
server	pelayan (fizikal atau maya) iaitu komputer yang mempunyai keupayaan tinggi yang memberi perkhidmatan berpusat
VPN	*Virtual Private Network* atau Rangkaian Persendirian Maya iaitu perkhidmatan rangkaian yang menggunakan infrastruktur telekomunikasi awam seperti internet bagi membolehkan pengguna yang berada di luar kampus mendapat capaian "UTeM-Net"

Pernyataan	Definisi
	dan menggunakan rangkaian tersebut dalam keadaan selamat
WAN	*Wide Area Network* iaitu rangkaian komputer jarak jauh dan teknologi yang biasanya digunakan untuk menyambungkan komputer atau peranti yang berada pada lokasi yang berbeza (negeri, negara dan benua). WAN dalam skop UTeM adalah sambungan kepada rangkaian internet

2.2 AKRONIM

Singkatan	Nama Penuh
CDO	Ketua Pegawai Digital
JDN	Jabatan Digital Negara, Kementerian Digital
DKS	Dasar Keselamatan Siber
JDN	Jabatan Digital Negara, Kementerian Digital
ICT	*Information and Communication Technology* atau Teknologi Maklumat dan Komunikasi
JPICT	Jawatankuasa Pemandu ICT UTeM
JKICT	Jawatankuasa Keselamatan ICT UTeM
PdP	pengajaran dan pembelajaran
PKPU	Peraturan Kewangan dan Perakaunan Universiti
PPPK	Pusat Perkhidmatan Pengetahuan Dan Komunikasi
PaDtRIOT	Pusat Perkhidmatan Data Raya dan IOT
PPF	Pejabat Pengurusan Fasiliti
UAT	*User Acceptance Test*
UTeM	Universiti Teknikal Malaysia Melaka
UTeM-Net	rangkaian dalaman UTeM

2.3 INTERPRETASI

(a) Mana-mana perkataan dalam bentuk tunggal adalah termasuk juga yang majmuk dan sebaliknya.

(b) Pada bila-bila masa Dasar Utama ini merujuk setiap hari dalam kalendar, apa-apa angka atau nombor tersebut hendaklah dirujuk kepada hari-hari dalam kalendar Gregorian.

(c) Tajuk-tajuk dan tajuk-tajuk kecil dalam Dasar Utama ini dimasukkan bertujuan untuk memudahkan rujukan sahaja dan tidak boleh dibuat pertimbangan dalam mentafsirkan Dasar Utama ini.

(d) Lampiran-lampiran yang dirujuk di dalam Dasar Utama ini (jika ada) hendaklah diambil, dianggap, dibaca dan ditafsirkan sebagai bahagian yang penting kepada Dasar Utama ini**.**

3.0 UNDANG-UNDANG

3.1 Dasar Utama ini hendaklah dibaca bersama dokumen-dokumen berikut:

(a) Akta Universiti dan Kolej Universiti 1971 termasuklah apa-apa pindaan dan apa-apa perundangan subsidiari di bawahnya;

(b) Akta 605;

(c) Akta Jenayah Komputer 1997 termasuklah apa-apa pindaan dan apa-apa perundangan subsidiari di bawahnya;

(d) Akta Rahsia Rasmi 1972 termasuklah apa-apa pindaan dan apa-apa perundangan subsidiari di bawahnya;

(e) Akta Perlindungan Data Peribadi 2010 termasuklah apa-apa pindaan dan apa-apa perundangan subsidiari di bawahnya;

(f) KTP;

(g) Polisi Keselamatan Siber Jabatan Digital Negara; dan

(h) Mana-mana undang-undang, dasar, peraturan, kaedah, garis panduan, pekeliling, arahan dan sebagainya yang berkuat kuasa dari semasa ke semasa

3.2 Dasar Utama ini adalah tertakluk kepada undang-undang, dasar, peraturan, kaedah, garis panduan, pekeliling, arahan dan sebagainya yang berkuat kuasa dari semasa ke semasa.

3.3 Dasar Utama ini adalah tertakluk kepada pindaan oleh pihak UTeM dari semasa ke semasa.

3.4 Sekiranya mana-mana peruntukan di dalam Dasar Utama ini menjadi tidak sah dan tidak boleh dilaksanakan disebabkan sebarang alasan, termasuk dan tidak terbatas kepada peruntukan mana-mana undang-undang yang berkuat kuasa atau disebabkan keputusan mahkamah atau badan lain atau pihak berkuasa yang mempunyai bidang kuasa ke atas Dasar Utama ini, maka hanya peruntukan tersebut sahaja yang terbatal manakala peruntukan-peruntukan yang lain masih sah dan berkuat kuasa.

4.0 TANGGUNGJAWAB PENGGUNA

4.1 Dasar Utama ini menerangkan tanggungjawab pengguna terhadap kemudahan ICT seperti berikut:-

(a) UTeM akan menyediakan kemudahan ICT untuk kemudahan staf dan pelajar bagi menyokong fungsinya.

(b) Semua kemudahan dan perkhidmatan ICT yang disediakan oleh UTeM adalah hak mutlak UTeM dan UTeM berhak menarik balik kemudahan serta perkhidmatan yang diberikan tanpa notis.

(c) Kemudahan ICT yang disediakan oleh UTeM hanya boleh digunakan untuk tujuan yang berkaitan dengan fungsi UTeM. Penggunaan selain daripada itu seperti untuk tujuan peribadi, komersial dan politik adalah tidak dibenarkan.

(d) Pengguna yang menggunakan peralatan ICT peribadi yang dibenarkan di dalam kampus juga tertakluk kepada Dasar Utama ini. Sebarang penggunaan adalah tertakluk kepada undang-undang, dasar, peraturan, kaedah, garis panduan, pekeliling, arahan dan sebagainya yang berkuat kuasa dari semasa ke semasa.

(e) Setiap pengguna hendaklah mematuhi Dasar Utama ini selaras dengan hasrat UTeM untuk mewujudkan pengguna yang beretika dan menghormati pengguna lain.

(f) UTeM bertanggungjawab memastikan pelaksanaan Dasar Utama ini dan syarat yang berkaitan dengan pengguna dan kod etika diamalkan selaras dengan kemudahan di bawah kawalannya.

(g) Ketua PTj bertanggungjawab memastikan Dasar Utama ini dipatuhi oleh staf dan pelajar selaras dengan kemudahan di bawah kawalan dan pengurusannya.

(h) Sekiranya didapati berlakunya sebarang keterdedahan/ketirisan/kebocoran/pencerobohan data atau maklumat semasa menggunakan aplikasi/sistem maklumat universiti termasuk sistem rangkaian universiti, pihak UTeM berhak untuk mengambil tindakan undang-undang terhadap individu atau pihak yang terlibat. Tindakan tersebut termasuk, tetapi tidak terhad kepada prosiding sivil, laporan kepada pihak berkuasa penguatkuasa undang-undang serta tindakan tatatertib dalaman, tertakluk kepada tahap pelanggaran dan kesan terhadap keselamatan maklumat berdasarkan undang-undang keselamatan siber yang berkuatkuasa di Malaysia.

5.0 PEMATUHAN DASAR UTAMA

5.1 Pengguna hendaklah mematuhi Dasar Utama ini. Sebarang pelanggaran terhadap mana-mana atau keseluruhan Dasar Utama ini, boleh dikenakan tindakan di bawah:

(a) Akta 605 bagi staf;

(b) KTP bagi pelajar; atau

(c) undang-undang lain yang berkuatkuasa bagi pihak luar.

5.2 Sebarang aduan berhubung pelanggaran Dasar Utama ini hendaklah dibuat secara bertulis kepada CDO. CDO boleh melantik jawatankuasa siasatan

untuk meneliti laporan dan menentukan sama ada siasatan terperinci perlu dilakukan.

5.3 Jika sabit kesalahan, tindakan akan dikenakan di bawah undang-undang yang berkuatkuasa.

BAB 1: DASAR PENGURUSAN ICT

1.1 TUJUAN

Dasar Pengurusan ICT yang digariskan adalah bertujuan untuk:

(a) Menerangkan terma rujukan Jawatankuasa Pemandu ICT (JPICT) UTeM yang bertanggungjawab menetapkan Dasar Teknologi Maklumat dan Komunikasi (ICT) dan memantau keberkesanan pelaksanaan ICT di UTeM;
(b) Menerangkan peranan Pejabat Ketua Pegawai Digital (CDO) di dalam melaksanakan pengurusan dan pembangunan ICT di UTeM;
(c) Menerangkan terma rujukan Jawatankuasa Keselamatan ICT (JKICT) UTeM;
(d) Menerangkan terma rujukan UTeM-CSIRT.

1.2 JPICT

Keahlian JPICT adalah seperti beirkut:

Jawatan	Keahlian dan TOR
Pengerusi	(a) Naib Canselor
Ahli	(a) Timbalan Naib Canselor (Akademik & Antarabangsa) (b) Timbalan Naib Canselor (Penyelidik & Inovasi) (c) Timbalan Naib Canselor (Hal Ehwal Pelajar & Alumni) (d) Penolong Naib Canselor (Strategik & Kelestarian Global) (e) Ketua Pegawai Operasi (f) Bendahari

Jawatan	Keahlian dan TOR
	(g) Ketua Pustakawan (h) Ketua Pegawai Digital (i) Dekan Fakulti Teknologi Maklumat dan Komunikasi (j) Dekan Fakulti Teknologi dan Kejuruteraan Elektronik dan Komputer (k) Pengarah Pusat Pengurusan Strategik, Kualiti & Risiko (l) Penasihat Undang-undang (m)Pengarah Pejabat Pengurusan Pembangunan (n) Pengarah Pejabat Pengurusan Fasiliti (o) Pengarah Pusat Sumber dan Teknologi Pengajaran
Ahli Turut Serta	(a) Pengarah Pusat Perkhidmatan Data Raya & IoT (b) Pengarah Pusat Perkhidmatan Pengetahuan dan Komunikasi
Terma Rujukan	(a) Menetapkan arah tuju dan strategi untuk **pembangunan dan** pelaksanaan ICT universiti. (b) Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju / strategi ICT universiti. (c) Merancang dan menyelaras pembangunan **dan pelaksanaan** program / projek ICT universiti. (d) Memastikan pembangunan ICT selari dengan pelan strategik universiti. (e) Menilai dan meluluskan projek ICT universiti berdasarkan kepada keperluan sebenar dan dengan perbelanjaan yang berhemat serta mematuhi peraturan-peraturan semasa. (f) Mengikuti dan memantau perkembangan program ICT universiti serta memahami keperluan, masalah

Jawatan	Keahlian dan TOR
	dan isu-isu yang dihadapi dalam pembangunan dan pelaksanaan ICT. (g) Memantau hal berkaitan keselamatan ICT (h) Mengemukakan kertas cadangan perolehan ICT universiti kepada JPICT Kementerian dan JTISA untuk kelulusan teknikal berdasarkan had nilai kelulusan yang ditetapkan (i) Mengemukakan laporan kemajuan projek ICT universiti yang telah diluluskan oleh JTISA kepada JPICT Kementerian mengikut tempoh-tempoh yang telah ditetapkan. (j) Meluluskan garis panduan ICT (tanpa implikasi kewangan)

1.3 PEJABAT CDO

Pejabat CDO diketuai oleh seorang CDO yang dilantik oleh Naib Canselor. Terdapat dua pihak berkuasa universiti (PBU) di bawah Pejabat CDO iaitu PPPK dan PaDtRIot. CDO bertanggungjawab dalam merancang, melaksana, mengurus, memantau dan menyelenggara projek ICT di UTeM merangkumi:

(a) Menyediakan pelan strategik bagi merancang penggunaan ICT dalam menyokong pencapaian visi dan misi UTeM.

(b) Memantap dan menyepadukan proses-proses yang *cross-functional* antara PTj di UTeM bagi menghasilkan sistem penyampaian perkhidmatan yang lebih cekap dan berkesan.

(c) Membangun, mengendali dan mengurus sistem dan infrastruktur ICT yang lebih kukuh dan selamat serta berdasarkan kepada ciri *modular, connectivity, inter-operability* dan *portability.*

(d) Menentukan halatuju sistem aplikasi UTeM bagi mengurangkan masa dan kos pembangunan, pengoperasian dan penyelenggaraan.

(e) Memelihara integriti maklumat, menggalak perkongsian maklumat dan menyediakan mekanisme penyebaran maklumat menerusi ICT kepada pengguna-pengguna yang sah di dalam atau luar UTeM.

(f) Menganggotai jawatankuasa utama yang menggubal dasar dan strategi serta bertanggungjawab terus kepada Naib Canselor.

(g) Mempromosikan penggunaan ICT yang berkesan bagi mencapai matlamat strategik UTeM dan bertindak sebagai agen perubahan dan transformasi.

1.4 JKICT

JKICT adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT UTeM.Keanggotaan JKICT UTeM adalah seperti berikut:

Jawatan	Keahlian dan TOR
Pengerusi	(a) Ketua Pegawai Digital (CDO)
Ahli	(a) Pengarah PPPK (b) Pengarah PaDtRIoT (c) Timbalan Pengarah Infrastruktur ICT PPPK (d) Timbalan Pengarah Infostruktur PPPK (e) Timbalan Pengarah Pengurusan Perkhidmatan ICT PPPK (f) Ketua Bahagian Pengurusan Pusat Data (g) seorang wakil dari Bahagian Pengurusan Akademik, Pejabat Pendaftar (h) seorang wakil dari Sekolah Pengajian Siswazah (i) seorang wakil dari Bahagian Sumber Manusia, Pejabat Pendaftar (j) seorang wakil dari Pusat Pengurusan Strategik, Kualiti dan Risiko

Jawatan	Keahlian dan TOR
	(k) dua (2) orang wakil dari Fakulti Teknologi Maklumat dan Komunikasi.
Terma Rujukan	(a) Memantau tahap pematuhan keselamatan ICT. (b) Memperaku garis panduan, polisi, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam UTeM yang mematuhi keperluan Dasar ICT UTeM. (c) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT. (d) Memastikan Dasar ICT UTeM selaras dengan dasar-dasar ICT kerajaan semasa. (e) Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa. (f) Membincang tindakan yang melibatkan pelanggaran Dasar ICT UTeM. (g) Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang

1.5 UTEM-CSIRT

Keanggotaan UTeM-CSIRT ialah seperti yang berikut:

Jawatan	Keahlian dan TOR
Pengarah	(a) Pengarah PPPK/ PADtRIoT
Pengurus	(a) ICTSO
Ahli	(a) Pegawai Teknologi Maklumat yang dilantik (b) Tiga orang wakil daripada PTj/ Fakulti yang dilantik.
Terma Rujukan	(a) Mengendalikan insiden berdasarkan garis panduan/prosedur yang telah ditetapkan. (b) Memantau, mengesan insiden, menerima dan mengesahkan aduan insiden keselamatan siber, seterusnya mengenal pasti jenis insiden serta menilai impak insiden keselamatan siber. (c) Merekodkan dan menjalankan siasatan awal terhadap insiden yang diterima. (d) Menjalankan penilaian untuk memastikan tahap keselamatan siber dan mengambil tindakan pemulihan serta pengukuhan keselamatan siber supaya insiden baharu dapat dielakkan. (e) Menyebarkan makluman/amaran berkaitan insiden kepada pengguna. (f) Memastikan fail log disimpan sekurang- kurangnya enam bulan di tempat yang selamat.

BAB 2: DASAR PERKAKASAN

2.1 TUJUAN

Dasar ini bertujuan memastikan pengurusan perkakasan dan perisian automasi pejabat yang melibatkan tanggungjawab pengguna dan PTj diuruskan dengan lebih baik. Dasar ini juga adalah berkaitan perolehan, pengagihan, skop penyelenggaraan, baik pulih, pelupusan dan agihan semula perkakasan

2.2 SKOP

Dasar ini melibatkan semua perkakasan dan perisian automasi pejabat yang dimiliki, diguna, disewa atau berada di dalam simpanan pengguna, bagi tujuan penggunaan hal-hal berkaitan UTeM sama ada dalam aspek pembelajaran dan pengajaran, penyelidikan ataupun urusan pentadbiran, tidak kira di mana ia berada. Perkakasan dan perisian automasi pejabat merujuk kepada perkakasan dan perisian automasi pejabat yang digunakan untuk membantu tugasan harian pejabat bagi menggantikan lain-lain kaedah manual. Perkakasan dan perisian (termasuk dan tidak terhad kepada) seperti berikut:

(a) Komputer peribadi (*Desktop*).
(b) Komputer riba (*Notebook*).
(c) Pencetak.
(d) Pengimbas.
(e) Sistem Operasi.
(f) Perisian yang dilesenkan oleh UTeM.

2.3 HAK MILIK

(a) Semua perkakasan dan perisian automasi pejabat yang diberi kepada staf untuk tujuan pengajaran, pembelajaran, penyelidikan dan pentadbiran adalah menjadi hak milik UTeM dalam tempoh ia digunakan.

(b) Semua perkakasan dan perisian automasi pejabat di bawah hak milik UTeM tidak boleh dijual, dipinjam, disalin semula oleh sesiapa atau entiti tanpa kebenaran pengurusan UTeM.

2.4 TANGGUNGJAWAB PENGGUNA

Pengguna adalah bertanggungjawab terhadap keselamatan perkakasan dan perisian automasi pejabat di bawah kawalannya. Tanggungjawab pengguna adalah seperti berikut:

(a) Pengguna tidak berhak mengganggu dengan apa jua cara sekalipun perkakasan dan perisian automasi pejabat yang bukan berada di bawah kawalannya termasuklah mengguna atau mengambil tanpa kebenaran, menceroboh dan mencuri perkakasan atau aksesorinya.

(b) Sebarang penggunaan secara gunasama *(sharing)* adalah menjadi tanggungjawab bersama pengguna-pengguna terbabit.

(c) Pengguna secara peribadi bertanggungjawab untuk membaca, memahami dan mematuhi peraturan dan pelesenan bagi setiap perisian automasi pejabat yang digunakan.

(d) Pengguna tidak dibenarkan memuat turun, membuat instalasi dan mengguna perisian automasi pejabat yang boleh mendatangkan kemudaratan dan kerosakan kepada kemudahan yang telah disediakan.

(e) Sebarang instalasi perisian tanpa lesen adalah dilarang dan penyebaran berkaitan dengan perisian tersebut juga adalah dilarang. Sebarang implikasi bagi ketidakpatuhan kepada perkara ini adalah di bawah tanggungjawab pengguna.

(f) Sebarang bentuk permainan komputer tidak dibenarkan kecuali untuk tujuan akademik dan penyelidikan setelah mendapat kelulusan daripada Ketua PTj.

(g) Pengguna tidak dibenarkan membuka bekas *(casing)* perkakasan bagi tujuan meminda, mengubah, mengambil atau membuang komponen dalaman sama ada berlaku kerosakan atau sebaliknya tanpa kebenaran pegawai yang bertanggungjawab.

(h) Sebarang kehilangan, kerosakan atau masalah perkakasan dan perisian automasi pejabat yang berpunca daripada kecuaian adalah menjadi tanggungjawab pengguna. Ia hendaklah dilaporkan kepada pegawai yang bertanggungjawab di PPPK. Sebarang keputusan berkaitan kos penggantian dan pembaikan adalah tertakluk kepada pihak universiti.

2.5 TANGGUNGJAWAB PTj

(a) PTj adalah bertanggungjawab menguruskan urusan perolehan, pengagihan, penggantian, selenggara dan pelupusan berdasarkan PKPU yang berkuatkuasa dari semasa ke semasa.

(b) Pegawai Aset di setiap PTj adalah bertanggungjawab bagi mengemaskini maklumat lokasi bagi perkakasan dan perisian yang terdapat di PTj masing-masing serta menguruskan proses pengesahan asset

2.6 TANGGUNGJAWAB PEJABAT CDO

(a) Menyediakan garis panduan spesifikasi berkaitan perkakasan & perisian berdasarkan maklumat semasa.

(b) Menyedia dan memberikan khidmat sokongan pengguna kepada PTj yang memerlukan.

(c) Menguruskan perolehan yang bersifat berpusat bagi keperluan dan kegunaan PTj.

(d) Memantau agihan perisian sistem operasi dan perisian yang berkaitan yang melibatkan penggunaan secara keseluruhan.

(e) Menyediakan tatacara dan garis panduan dari semasa ke semasa berdasarkan keperluan di peringkat UTeM.

2.7 PEROLEHAN PERKAKASAN DAN PERISIAN AUTOMASI PEJABAT

Pengurusan perkakasan dan perisian automasi pejabat adalah seperti berikut:

(a) Kaedah perolehan setiap perkakasan dan perisian automasi pejabat adalah tertakluk kepada PKPU yang berkuatkuasa dari semasa ke semasa.

(b) Pembelian setiap perkakasan dan perisian hendaklah mengambil kira tempoh jaminan pembekal *(warranty)* sekurang-kurangnya 1 tahun dengan mengambil kira alat ganti, tenaga kerja dan servis *(part, labour & service)* secara *onsite.*

(c) Khidmat nasihat berkaitan perolehan boleh didapati daripada Pejabat CDO bagi menentukan spesifikasi yang bersesuaian berdasarkan keperluan PTj.

(d) Semua perkakasan & perisian automasi pejabat perlu didaftarkan

2.8 PENGAGIHAN KOMPUTER DAN PERKAKASAN

Pengurusan perkakasan dan perisian automasi pejabat adalah seperti berikut:

(a) Kaedah perolehan setiap perkakasan dan perisian automasi pejabat adalah tertakluk kepada PKPU yang berkuatkuasa dari semasa ke semasa.

(b) Pembelian setiap perkakasan dan perisian hendaklah mengambil kira tempoh jaminan pembekal *(warranty)* sekurang-kurangnya 1 tahun dengan mengambil kira alat ganti, tenaga kerja dan servis *(part, labour & service)* secara *onsite.*

(c) Khidmat nasihat berkaitan perolehan boleh didapati daripada Pejabat CDO bagi menentukan spesifikasi yang bersesuaian berdasarkan keperluan PTj.

(d) Semua perkakasan & perisian automasi pejabat perlu didaftarkan

2.9 ASET DAN INVENTORI PERKAKASAN ICT

(a) Menjadi tanggungjawab PTj memastikan kesemua aset dan inventori perkakasan ICT mempunyai pelekat *(tagging)*.

(b) PTj juga bertanggungjawab mengemas kini maklumat aset dan inventori perkakasan ICT yang diperolehi daripada proses pindah milik atau pengagihan semula daripada PTj lain.

(c) Sebarang perubahan maklumat aset dan inventori perkakasan ICT yang berkaitan perlu dikemas kini bagi mengelakkan permasalahan ketika urusan pelupusan.

2.10 PENYELENGGARAAN DAN BAIKPULIH

(a) Semua komputer yang merupakan aset UTeM (komputer peribadi, komputer di makmal, bilik kuliah dan lain-lain) hendaklah diselenggara secara berkala sekurang-kurangnya sekali setahun.

(b) Pengurusan baik pulih kerosakan perkakasan harus dirujuk kepada Pejabat CDO atau PTj yang bertanggungjawab.

(c) PTj boleh merujuk kepada Pejabat CDO bagi sebarang semakan awal atau mendapatkan cadangan untuk menguruskan kerosakan yang dialami sama ada melibatkan perkakasan atau perisian.

2.11 PELUPUSAN

(a) Menjadi tanggungjawab PTj untuk melupuskan aset dan inventori ICT yang telah rosak atau tidak boleh diperbaiki lagi mengikut peraturan yang sedang berkuatkuasa.

(b) PTj boleh merujuk kepada Pejabat CDO bagi mendapatkan cadangan dan nasihat berkaitan dengan teknologi terkini bagi menyokong urusan pelupusan.

2.12 KESELAMATAN PERKAKASAN DAN PERSEKITARAN

Setiap pengguna hendaklah merujuk dan mematuhi DKS bagi perkara yang berkaitan dengan keselamatan perkakasan dan persekitaran

2.13 PENGGANTIAN PERKAKASAN

Pengguna boleh memohon untuk penggantian bagi perkakasan yang telah rosak, usang, atau hilang. Proses dan kebenaran bagi penggantian perkakasan hendaklah dirujuk kepada PTj masing-masing.

BAB 3: DASAR SERVER

3.1 TUJUAN

Dasar ini bertujuan menerangkan tentang peruntukan-peruntukan yang hendaklah dipatuhi serta memberikan panduan berkaitan pengurusan server di UTeM.

3.2 SKOP

Skop bagi dasar ini adalah meliputi kesemua server yang dimiliki oleh UTeM. Kategori server ini dipecahkan kepada (3) kategori iaitu:

(a) Server kritikal iaitu:

(i) Menyimpan data-data penting UTeM.

(ii) Menyokong kesemua sistem aplikasi UTeM.

(iii) Memberikan kesan yang besar kepada operasi universiti sekiranya berlaku sebarang masalah yang tidak diingini kepada server berkenaan.

(iv) Tidak terhad kepada perkara di atas

(b) Server pengajaran dan pembelajaran (PdP) iaitu:

(i) server yang digunakan bagi tujuan PdP bagi sesebuah PTj di UTeM. Server ini adalah penting kepada aktiviti PdP sesebuah PTj namun kegagalan server ini tidak memberikan kesan yang besar kepada operasi UTeM secara keseluruhannya.

(c) Server tidak kritikal iaitu:

(i) server yang tidak memberikan kesan besar kepada operasi UTeM sekiranya berlaku sebarang perkara yang tidak diingini kepada server.

3.3 HAK MILIK

Semua server yang diperoleh mengikut tatacara perolehan atau sumbangan daripada mana-mana pihak adalah menjadi hak milik UTeM sepenuhnya.

3.4 TANGGUNGJAWAB

Kesemua PTj yang membuat pembelian server adalah bertanggungjawab sepenuhnya kepada server tersebut. Tanggungjawab ini boleh dipecahkan kepada:

(a) Pemilik

(i) Pemilik adalah PTj yang membuat perolehan kepada sesuatu server. Pemilik adalah bertanggungjawab bagi memastikan server di bawah pengawasannya berada di dalam keadaan baik. Pengurusan berkaitan perolehan dan penyelenggaraan server oleh pemilik adalah tertakluk kepada DKS serta undang-undang yang berkuatkuasa dari semasa ke semasa.

(b) Pentadbir Server

(i) Pentadbir Server bertanggungjawab memastikan server diurus, ditadbir dengan betul dan memenuhi keperluan pemilik server serta bertanggungjawab sepenuhnya ke atas keselamatan data dan sistem di dalam server.

3.5 SYARAT PENEMPATAN

(a) Server-server kritikal yang berada di bawah tanggungjawab Pejabat CDO dan berfungsi menguruskan sistem aplikasi universiti hendaklah ditempatkan di Pusat Data UTeM. Server-server ini mesti diletakkan di lokasi yang memenuhi syarat-syarat berikut:

(i) Lokasi yang selamat dan hanya boleh dicapai oleh staf yang dibenarkan sahaja.

(ii) Server perlulah menggunakan saiz dari jenis '*rack-mount*' supaya server tersebut boleh dipasang pada rak server.

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

(iv) Mempunyai peralatan '*Uninterruptable Power Supply*' (UPS) dengan masa minimum beroperasi 5 minit jika terputus bekalan elektrik dan perlindungan daripada kilat serta menyokong penutupan server secara automatik untuk mengelakkan kerosakan.

(v) Memasang generator set sekiranya perlu bagi memastikan server masih terus berfungsi apabila berlaku gangguan bekalan elektrik.

(vi) Mempunyai sistem pencegah kebakaran berasaskan gas (FE-13, FE-77 dan sebagainya).

(vii) Pengudaraan yang mencukupi dan suhu hendaklah terkawal di dalam had suhu yang diperlukan oleh server (20°C – 25°C).

(b) Server kritikal yang tidak ditempatkan di Pusat Data UTeM perlulah mematuhi semua keperluan di atas manakala server tidak kritikal boleh ditempatkan di PTj masing-masing dengan syarat lokasi serta kemudahan yang disediakan adalah bersesuaian serta mampu untuk membolehkan server tersebut berfungsi dengan baik.

(c) PTj dibenarkan untuk menggunakan server luar daripada UTeM-Net bagi tujuan-tujuan rasmi contohnya seperti menggunakan kaedah *cloud computing* bagi pemprosesan data, perkongsian maklumat dan sebagainya. Walau bagaimanapun PTj perlulah membuat permohonan bertulis kepada CDO bagi tujuan tersebut.

(d) PTj juga boleh membuat permohonan secara bertulis kepada CDO untuk menempatkan server tidak kritikal mereka di Pusat Data UTeM. Walau bagaimanapun, segala urusan pengurusan aplikasi pada server tersebut masih lagi di bawah tanggungjawab PTj berkenaan dan Pejabat CDO hanya menyediakan kemudahan fizikal bagi menyokong operasi server tersebut.

(e) Sebarang perkara yang berkaitan dengan aspek keselamatan sesuatu server perlulah dirujuk kepada Dasar Keselamatan Siber.

3.6 PELANGGARAN

Sebarang pelanggaran terhadap mana-mana atau keseluruhan Dasar Server atau Dasar Utama ini yang mengakibatkan salah satu atau lebih perkara-perkara berikut bergantung kepada tahap masalah tersebut:

(a) Bagi masalah keselamatan, server akan ditutup sementara sehingga tahap keselamatan server ditingkatkan ke tahap yang sewajarnya.

(b) Penyambungan server ke rangkaian akan ditutup.

(c) Penutupan operasi server.

(d) Peringatan kepada pemilik dan pentadbir sistem akan dikeluarkan jika didapati server digunakan untuk aktiviti yang bukan berkaitan urusan rasmi UTeM

BAB 4: DASAR RANGKAIAN

4.1 PENGENALAN

Dasar Rangkaian mengandungi beberapa dokumen yang hendaklah dibaca dan dipatuhi dalam penggunaan perkhidmatan rangkaian dan telekomunikasi yang telah disediakan oleh UTeM. Dasar Rangkaian ini juga menerangkan kepada pengguna mengenai tanggungjawab dan peranan mereka dalam memastikan perkhidmatan ini digunakan dengan sebaik mungkin dan melindungi perkhidmatan daripada ancaman dan penyalahgunaan.

4.2 TUJUAN

Menentukan penyediaan, pengurusan, penggunaan dan pengoperasian bagi perkhidmatan UTeM-Net dan kemudahan telekomunikasi UTeM.

4.3 SKOP

4.3.1 UTeM-Net

Sumber rangkaian merangkumi peralatan rangkaian, termasuk (tetapi tidak terhad kepada) seperti *hubs*, *switches*, *routers, access points, perisian rangkaian* dan pengkabelan rangkaian. Perisian aplikasi rangkaian merangkumi perisian sama ada dibeli atau dimuat-turun daripada Internet.

4.3.2 Penyambungan Rangkaian

Penyambungan rangkaian termasuk LAN, MAN dan WAN yang merangkumi kemudahan sambungan Internet dan intranet.

4.3.3 Penyelenggaraan Rangkaian

Penyelenggaraan rangkaian merujuk kepada proses konfigurasi, penjagaan, pemantauan dan pembaikan rangkaian komputer untuk memastikan ia berfungsi dengan baik dan bebas daripada masalah teknikal.

4.3.4 Penyambungan Telefon

Penyambungan talian telefon yang disediakan adalah *IP phone* dan juga *softphone.*

4.4 PENTADBIRAN RANGKAIAN

Pejabat CDO adalah PTj yang bertanggungjawab mengurus, menyelenggara dan memantau rangkaian dan telekomunikasi UTeM.

4.5 HAK MILIK

Semua sumber rangkaian dan telekomunikasi yang diperoleh daripada pihak UTeM adalah menjadi hak milik UTeM.

4.6 KEMUDAHAN RANGKAIAN

Pejabat CDO berhak menarik balik kemudahan penggunaan rangkaian jika pengguna didapati melanggar mana-mana peruntukan berikut:

(a) Kemudahan rangkaian hanya boleh diguna untuk tujuan yang berkaitan dengan urusan kerja rasmi sahaja. Kegunaan peribadi, terutama yang berunsur komersial tidak dibenarkan.

(b) Pengguna tidak boleh menggunakan kemudahan UTeM untuk aktiviti-aktiviti yang bertentangan dengan undang-undang yang berkuatkuasa. Ini termasuk (tetapi tidak terhad kepada) menghantar dan menerima maklumat yang berunsur subversif dan menghantar dan menyebar maklumat terperingkat mengenai UTeM tanpa kebenaran.

(c) Pengguna tidak dibenarkan dalam apa cara sekali pun mengganggu pengguna lain di dalam rangkaian kampus dan Internet. Gangguan ini termasuk (tetapi tidak terhad kepada) menghantar maklumat rambang (*spam*) secara email atau mesej atas talian (*online*) dan lain-lain.

(d) Pengguna tidak boleh memberikan sumber rangkaian di bawah jagaannya termasuk (tetapi tidak terhad kepada) rangkaian tanpa wayar (*wireless*) untuk diguna oleh orang lain walaupun pelajar atau staf UTeM.

4.7 PEYAMBUNGAN RANGKAIAN

Bagi memastikan penyediaan kemudahan rangkaian dan telekomunikasi sentiasa dalam keadaan baik, penyambungan rangkaian hendaklah dilakukan mengikut prosedur berikut:

(a) Perolehan peralatan rangkaian dan penyambungan ke rangkaian kampus UTeM serta talian telekomunikasi perlu mendapat kelulusan Pejabat CDO atau pengurusan UTeM sebelum proses perolehan dilaksanakan. Konfigurasi penyambungan yang hendak dibuat oleh pembekal perlu di bawah pengawasan dan kawalan Pejabat CDO.

(b) Pengguna tidak dibenarkan membuat sebarang penyambungan rangkaian ke rangkaian kampus serta talian telekomunikasi tanpa terlebih dahulu mendapat kebenaran bertulis daripada Pejabat CDO.

(c) Setiap ubah suai serta tambahan bangunan atau bangunan baru yang akan dibina perlu memasukkan keperluan infrastruktur rangkaian dan telekomunikasi yang ditentukan bersama oleh pengguna, Pejabat CDO dan Pejabat Pengurusan Pembangunan. Ia termasuk peralatan aktif dan juga peralatan pasif.

4.8 PENYELENGGARAAN RANGKAIAN

4.8.1 Penyelenggaraan Rangkaian

Bagi menjamin keselamatan dan memudahkan kerja-kerja penyelenggaraan infrastruktur, langkah-langkah berikut hendaklah dipatuhi untuk mengawal keselamatan infrastruktur rangkaian dan komunikasi:

(a) Bagi memastikan talian rangkaian berada dalam keadaan yang baik, kerja-kerja penyelenggaraan hendaklah dilakukan secara berkala sekurang-kurangnya setahun sekali.

(b) Semua peralatan rangkaian seperti *switch*, *modem*, *hub*, *router* dan lain-lain hendaklah diletakkan di tempat yang dikhaskan (rak rangkaian).

(c) Setiap PTj hendaklah memastikan penghawa dingin atau kipas setiap bilik rangkaian berfungsi dengan baik dan melaporkan kepada Pejabat Pengurusan Fasiliti dan Pejabat CDO sekiranya berlaku kerosakan.

(d) Pentadbir Rangkaian hendaklah memastikan bilik rangkaian (*commrack*) hanya boleh diakses atau digunakan oleh pengguna yang dibenarkan sahaja.

(e) *Rack*, *switch*, *router*, *access point*, *modem* dan kabel rangkaian yang dipasang tidak boleh dialihkan kedudukannya melainkan mendapat kebenaran daripada Pejabat CDO. PTj yang berkenaan hendaklah menghantar salinan pelan susun atur yang baru (jika berlaku perubahan) ke Pejabat CDO untuk makluman dan pengemaskinian dokumentasi.

(f) Maklumat setiap peralatan rangkaian hendaklah direkodkan oleh Pegawai Aset ke dalam borang Daftar Aset dan didokumenkan untuk tujuan rujukan.

(g) Konfigurasi bagi setiap peralatan rangkaian hendaklah disimpan dan didokumentasikan. Sebarang perubahan konfigurasi pada peralatan hendaklah dimaklumkan dahulu kepada Pejabat CDO.

4.8.2 Pemberian Alamat IP

Atas sebab-sebab keselamatan dan kawalan kualiti rangkaian, pemberian alamat IP adalah tertakluk kepada syarat-syarat yang ditetapkan oleh Pejabat CDO dari semasa ke semasa.

BAB 5: DASAR APLIKASI

5.1 TUJUAN

Dasar ini bertujuan memastikan sistem aplikasi Universiti yang dibangun,diselenggara dan digunakan adalah efisien serta mempunyai kebolehpercayaan yang tinggi bagi menyokong urusan pengurusan dan pentadbiran, PdP, penyelidikan dan sebagainya

5.2 SKOP

Skop dasar ini merangkumi semua aktiviti yang berkaitan dengan pembangunan dan penyelenggaraan sistem aplikasi yang melibatkan semua pihak berkepentingan mengikut klasifikasi sistem, pengurusan dan peranan pengguna, proses pengujian bagi menjamin kualiti dan keselamatan sistem.

5.3 CIRI-CIRI SISTEM APLIKASI

Semua sistem aplikasi yang dibangunkan dan yang ditambahbaik adalah mematuhi ciri-ciri berikut:

5.3.1 Integrasi *(Integrated)*

Sistem aplikasi yang dibangunkan dan yang ditambahbaik akan diintegrasikan sepenuhnya di antara satu sistem dengan sistem yang lain agar kemasukan data berlaku pada satu tempat sahaja (*one single entry*) dan data tersebut akan disalurkan kepada sistem-sistem aplikasi yang lain.

5.3.2 Mesra Pengguna *(User Friendly)*

Sistem aplikasi yang dibangunkan dan yang ditambahbaik perlu

menitikberatkan dan mengambil kira berkenaan dengan rekabentuk antaramuka yang lebih mesra pengguna dan mudah difahami.

5.3.3 Dinamik *(Dynamic)*

Sistem aplikasi yang dibangunkan dan yang ditambahbaik akan direka cipta agar bersifat dinamik supaya ianya mudah diubahsuai mengikut keperluan semasa.

5.3.4 Capaian

Kebanyakan sistem aplikasi yang dibangunkan dan yang ditambahbaik adalah berasaskan web yang mana ianya memudahkan pengguna untuk mencapai sistem aplikasi pada bila-bila masa dan di mana-mana sahaja dengan syarat mempunyai capaian internet.

5.3.5 Kawalan Capaian

Kawalan capaian menu adalah mengikut tahap atau kumpulan pengguna yang telah ditetapkan oleh pemilik sistem. Keadaan ini akan dapat mengawal sebarang aktiviti yang tidak diingini atau penyalahgunaan sistem.

5.3.6 Ketepatan Maklumat

Sistem aplikasi yang dibangunkan dan yang ditambahbaik adalah sangat membantu untuk mendapatkan sebarang maklumat yang diperlukan. Pemilik sistem perlu mengetahui peranannya supaya data-data dan maklumat yang diperlukan adalah terkini, tepat dan mempunyai kebolehpercayaan yang tinggi.

5.3.7 Automasi *(Automation)*

Sistem aplikasi yang dibangunkan dan yang ditambahbaik adalah bertujuan untuk mengautomasikan dan mengurangkan proses manual di mana ianya merangkumi proses-proses secara atas talian bermula daripada proses permohonan, pengesahan, kelulusan dan sebagainya. Ia juga merangkumi *alert* dan *trigger* secara automatik yang dijalankan oleh sistem dengan dibantu peralatan seperti Kad Pintar (*smartcard*), Pengimbas Kodbar (*Barcode Reader)* dan sebagainya.

5.3.8 Kepintaran *(Intelligent)*

Semua sistem aplikasi yang dibangunkan adalah merupakan integrasi pemikiran dan kepakaran individu atau kumpulan tertentu dalam sesuatu bidang. Segala formula, prosedur, polisi dan kekangan akan disepadukan dengan sistem-sistem tersebut, yang mana UTeM akan menggunapakai cara-cara dan pendekatan terbaik dalam pembangunan dan penyelenggaraan sistem. Sistem-sistem yang dibangunkan akan menjurus ke arah kecekapan dan keberkesanan pentadbiran, PdP, penyelidikan dan perundingan serta memberi ilmu pengetahuan (*knowledge*) agar ianya dapat memberi manfaat kepada organisasi.

5.3.9 Penggunaan Tanpa Kertas *(Paperless)*

Capaian maklumat secara atas talian (*online access*) adalah sangat penting bagi memastikan data-data yang dicapai adalah yang terkini dan dapat dicapai dengan cepat. Tanpa kertas juga akan memastikan setiap tahap kerja akan dapat diselesaikan dengan cepat dan segera bermula dari proses permohonan sehinggalah kepada proses pengesahan. Segala komunikasi seperti memo, mesyuarat, pekeliling, pengumuman dan sebagainya akan dijalankan secara atas talian atau tanpa kertas.

5.4 PEMBANGUNAN SISTEM APLIKASI

5.4.1 Pembangunan Sistem Aplikasi Secara Dalaman (*In-House Development*)

Pemilik Sistem hendaklah membuat permohonan rasmi kepada Pejabat CDO bagi sebarang permohonan sistem aplikasi baharu yang akan dibangunkan secara dalaman (*in-house*). Pemilik Sistem juga hendaklah menyediakan *Standard Operating Procedure* (SOP) yang lengkap dan menyatakan skop keperluan dengan jelas. Pejabat CDO akan meneliti dan membuat kajian yang sewajarnya bagi pembangunan sistem aplikasi yang dipohon. Pembangunan sistem aplikasi haruslah mengikut proses pembangunan sistem. **(Sila Rujuk:** Garis Panduan Membangun dan Menyelenggara Sistem Maklumat**)**

5.4.2 Sistem Aplikasi Daripada Kerajaan Persekutuan / Agensi Kerajaan Persekutuan

Semua sistem aplikasi yang dibekalkan oleh Kerajaan Persekutuan/Agensi Kerajaan Persekutuan hendaklah dimaklumkan kepada Pejabat CDO untuk diteliti dan diselaraskan sebelum sistem tersebut boleh digunakan oleh pengguna. Penyelarasan ini hendaklah dilaksanakan bagi memastikan sistem aplikasi yang dibekalkan boleh dilaksanakan mengikut kesesuaian di peringkat UTeM. Implikasi dari segi keserasian data, keselamatan data, pelaksanaan melalui rangkaian UTeM serta keupayaan integrasi sistem berkenaan dengan sistem-sistem aplikasi lain yang sedia ada akan diteliti.

5.4.3 Sistem Aplikasi Daripada Pihak Ketiga (*third party*)

Pembangunan perisian secara *outsource* hendaklah diselia dan dipantau sentiasa oleh pemilik sistem. Aspek teknikal hendaklah dikawal selia oleh Pejabat CDO. Klausa mengenai pemindahan teknologi (*Transfer of Technology*) dan penyerahan serta pemilikan *source code* dari pembekal kepada Pejabat CDO hendaklah dinyatakan dalam dokumen kontrak. Ini bagi

memastikan kerja-kerja penyelenggaraan dapat dikawal selia oleh Pejabat CDO. Pihak ketiga hendaklah menyediakan dokumentasi manual pengguna dan dokumentasi sistem yang lengkap dan terkini kepada Pejabat CDO.

5.4.4 Penyelenggaraan Sistem

Sebarang penambahbaikan atau perubahan sistem yang diperlukan oleh Pemilik Sistem hendaklah dimaklumkan kepada Pejabat CDO berkaitan perubahan yang ingin dilaksanakan. Ini adalah bertujuan untuk pengurusan dan pemantauan dengan lebih berkesan. Pejabat CDO akan meneliti dan membuat kajian yang sewajarnya bagi penambahbaikan sistem aplikasi yang dipohon. **(Sila Rujuk: Garis Panduan Membangun dan Menyelenggara Sistem Maklumat)**

5.5 PENGURUSAN DAN PERANAN PENGGUNA

5.5.1 Pemilik Data

Kumpulan Pengguna	Peranan Pengguna
Pemilik data	(i) Bertanggungjawab untuk memasukkan, mengemaskini, dan menghapus data di dalam sistem mengikut keperluan. (ii) Memastikan data yang telah dimasukkan ke dalam sistem adalah data yang betul dan tepat. (iii) Bertanggungjawab terhadap setiap aspek keselamatan data; (iv) Memastikan setiap data dikemaskini bagi memastikan kesahihan data. (v) Pengemaskinian data dalam sistem hanya boleh dilakukan oleh pemilik data sahaja. (vi) Melaporkan sebarang masalah atau kerosakan terhadap data yang berada di luar had capaian

Kumpulan Pengguna	Peranan Pengguna
	sebagai pemilik data kepada khidmat bantuan pengguna Pejabat CDO. (vii) Menjaga kerahsiaan, integriti dan akauntabiliti data.

5.5.2 Pemilik Proses

Kumpulan Pengguna	Peranan Pengguna
Pemilik proses ialah PTj yang bertanggungjawab untuk proses tertentu di dalam sistem yang dibangunkan. Contohnya: (i) Sistem Maklumat Pelajar (SMP) – Bahagian Pengurusan Akademik, Pejabat Pendaftar dan Pejabat Bendahari; (ii) Sistem Maklumat Kewangan Bersepadu (SMKB) – Pejabat Bendahari; (iii) Sistem Maklumat Pasca Siswazah (SMPS) – Sekolah Pengajian Siswazah; (i) Sistem Maklumat Sumber Manusia (SMSM) – Pejabat Pendaftar; dan (ii) *University Research Information System* (URIS) – Pusat Pengurusan Penyelidikan & Inovasi (CRIM).	(i) Bertanggungjawab dalam membekalkan carta alir proses kerja, dasar, prosedur dan lain-lain dokumen yang berkaitan bagi setiap proses dalam keseluruhan sistem. (ii) Mengadakan perbincangan untuk mewujudkan proses kerja dengan pihak pembangun sistem. (iii) Mengadakan perbincangan bagi mengkaji proses sedia ada bagi tujuan pelaksanaan di dalam pembangunan sistem. (iv) Mengadakan bengkel pemurnian proses kerja bersama dengan pemilik proses dan pembangun sistem, sekiranya perlu. (v) Setiap PTj harus melantik seorang *champion* bagi mengkoordinasi kesemua proses yang ada di dalam PTj berkenaan.

5.5.3 Pemilik Sistem

Kumpulan Pengguna	Peranan Pengguna
Pemilik sistem harus mempunyai kriteria berikut: (i) Berkeupayaan untuk menjadi koordinasi projek. (ii) Berpengetahuan dan berpengalaman. (iii) Kreatif dan Inovatif.	(i) Membuat permohonan pembangunan dan penambahbaikan kepada Pejabat CDO. (ii) Menyediakan maklumat dan merangka carta alir proses kerja. (iii) Mengadakan bengkel pemurnian dan semakan sistem aplikasi sedia ada bagi tujuan memantapkan lagi sistem tersebut, sekiranya perlu. (iv) Menentukan jawatankuasa sistem di peringkat PTj terdiri daripada pemilik proses dan pengguna. (v) Menyemak dan mengesahkan skop. (vi) Mengenalpasti pihak yang terlibat dan isu-isu yang akan timbul dalam proses kerja dan melaksanakan pengurusan perubahan. (vii) Mengenalpasti dan mengesahkan format input/output; (viii) Menyemak, memberi maklumbalas dan pengesahan ke atas dokumen kajian keperluan pengguna. (ix) Memberi maklumbalas dan cadangan ke atas reka bentuk yang dibentangkan; (x) Menguji dan mengesahkan fungsi setiap modul yang dibangunkan bersama pasukan teknikal Pejabat CDO dan pengguna sistem. (xi) Mempromosikan pelaksanaan sistem kepada pengguna sasaran.

Kumpulan Pengguna	Peranan Pengguna
	(xii) Menentukan pengguna dan kategori atau tahap capaian pengguna sistem aplikasi. (xiii) Menguruskan senarai pengguna yang akan terlibat dalam latihan pengguna. (xiv) Menguatkuasakan penggunaan sistem di kalangan pengguna. (xv) Memantau pelaksanaan dan keberkesanan sistem secara berterusan. (xvi) Memaklumkan sebarang masalah dan keperluan peningkatan sistem kepada pembangun sistem. (xvii) Memastikan proses kerja semasa selaras dengan proses kerja pengkomputeran yang baharu dan memaklumkan kepada pembangun sistem untuk melakukan penambahbaikan sistem aplikasi. (xviii) Melaksanakan perbincangan berterusan di antara pihak pemilik proses dan pembangun sistem melalui siri mesyuarat /perbincangan mengikut keperluan

5.5.4 Pengguna Akhir *(End User)*

Kumpulan Pengguna	Peranan Pengguna
Pengguna akhir	(i) Menggunakan sistem aplikasi mengikut etika dan tatacara yang ditetapkan. (ii) Memaklumkan sebarang masalah teknikal berkaitan sistem kepada staf teknikal Pejabat CDO. (iii) Dilarang memanipulasi data dalam apa jua bentuk dan tujuan melainkan mendapat kebenaran bertulis daripada Pemilik Data atau Pemilik Sistem yang mana berkaitan. (iv) Bertanggungjawab menjaga kerahsiaan, integriti dan akauntabiliti data. (v) Mengemukakan cadangan penambahbaikan sistem kepada pemilik sistem bagi membolehkan peningkatan prestasi sistem.

5.6 KESELAMATAN DALAM MEMBANGUNKAN DAN MENYELENGGARA SISTEM APLIKASI

Keselamatan dalam membangunkan dan menyelenggara sistem aplikasi adalah berdasarkan kepada DKS.

5.7 PENGUJIAN SISTEM APLIKASI

(a) Salah satu aspek pembangunan dan penambahbaikan sistem aplikasi ialah pengujian yang dilaksanakan pada beberapa peringkat iaitu pemprograman aturcara sistem aplikasi dan integrasi sistem aplikasi

serta pengujian pengguna. Ia melibatkan pengujian aplikasi baharu, penambahbaikan kepada aplikasi semasa atau pemindahan daripada perkakasan lama kepada baharu. Pengujian perlu bagi memastikan sistem berfungsi mengikut spesifikasi yang ditetapkan.

(b) Bagi menghalang maklumat daripada didedah atau diproses secara tidak sepatutnya, persekitaran yang berbeza untuk pembangunan sistem dan pengoperasian sistem hendaklah diwujudkan. Sekiranya persekitaran berasingan untuk pembangunan sistem tidak dapat dilaksanakan, langkah-langkah berikut hendaklah dilakukan:

(i) menggunakan data '*dummy*' atau '*historical*' untuk tujuan pengujian.

(ii) menghapuskan maklumat yang digunakan semasa pengujian sistem (terutamanya apabila menggunakan *data historical*).

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

(iv) melaksanakan ujian simulasi dengan semua pihak berkepentingan bagi mamastikan sistem beroperasi mengikut keperluan yang ditetapkan.

5.8 HAK MILIK PERISIAN/KOD SUMBER SISTEM APLIKASI

(a) Kod sumber sistem aplikasi merujuk kepada sebarang siri pernyataan yang ditulis dalam bahasa pengaturcaraan komputer yang difahami.

(b) Semua perisian/kod sumber sistem aplikasi adalah menjadi hak milik UTeM bagi perkara-perkara berikut:

(i) Perisian sistem aplikasi yang dibangunkan oleh staf atau pelajar UTeM untuk tujuan pentadbiran, PdP, penyelidikan, perundingan dan lain-lain yang diklasifikasi sebagai keperluan perniagaan UTeM maka ianya adalah menjadi hak milik UTeM.

(ii) Perisian sistem aplikasi yang dibangunkan secara khidmat sumber luaran (*Outsource*) atau *Joint Venture* (*JV*) / di antara UTeM

dengan pihak ketiga di mana UTeM membayar kos pembangunan perisian tersebut.

(c) Semua perisian sistem aplikasi hak milik UTeM boleh dijual, disewa, dilesenkan semula, dipinjam, disebar atau diberi kepada sesiapa atau entiti bagi tujuan pengkomersialan dan perundingan dengan kebenaran bertulis UTeM atau *stakeholders* UTeM.

BAB 6: DASAR AKAUNTABILITI

6.1 TUJUAN

Menyatakan tanggungjawab pihak yang terlibat dengan penggunaan kemudahan teknologi maklumat dan komunikasi di UTeM seperti berikut:

(a) Memelihara dan melindungi maklumat pengguna yang disimpan oleh UTeM yang diklasifikasikan sebagai maklumat terperingkat.

(b) Menyokong usaha UTeM untuk menjaga kepentingan *stakeholder.*

6.2 SKOP

Skop dasar ini meliputi tanggungjawab pengguna dan UTeM berkaitan capaian data atau maklumat.

6.3 CAPAIAN MAKLUMAT TERPERINGKAT

6.3.1 Capaian Maklumat Terperingkat oleh Pentadbir ICT dan Pengurus ICT:

(a) Pentadbir ICT dan Pengurus ICT dibenarkan:-

(i) memantau kegiatan dan aktiviti pengguna dari semasa ke semasa sebagai rutin pemantauan keselamatan ICT; dan

(ii) melaporkan sebarang pelanggaran Dasar ICT kepada JPICT atau mana-mana pihak berkuasa UTeM, sekiranya perlu.

(b) Pentadbir ICT dan Pengurus ICT boleh membuat salinan sama ada dalam bentuk bercetak atau digital semua atau sebahagian kandungan akaun pengguna sebagai pemeliharaan bukti. Pentadbir ICT dan Pengurus ICT dengan kebenaran UTeM boleh mencapai maklumat terperingkat pengguna seperti kandungan e-mel atau fail yang tersimpan dalam akaunnya.

6.3.2 Capaian Maklumat Terperingkat Oleh Pengguna

(a) Pengguna tidak dibenarkan menyimpan data atau maklumat terperingkat di dalam komputer atau akaun pengguna melainkan atas keperluan tugasan rasmi.

(b) Pengguna diberi jaminan bahawa selain daripada perkara yang disebutkan di atas, maklumat terperingkat yang terdapat dalam akaun pengguna tidak akan dicapai oleh sesiapa pun. Sekiranya ada pengguna lain mencapai data atau maklumat pengguna lain tanpa kebenaran, maka individu tersebut telah melanggari dasar ini.

6.4 PEMANTAUAN DATA DALAM RANGKAIAN

Pengurus ICT dibenarkan:-

(a) memantau dan merekodkan data-data yang berada dalam rangkaian sebagai sebahagian daripada rutin penjagaan keselamatan sumber ICT. Peralatan rangkaian seperti *router* atau sistem komputer server yang menggunakan perisian-perisian tertentu mampu merekodkan data-data dalam rangkaian. Jaminan diberi bahawa data-data yang direkod tidak akan didedahkan melainkan jika berlaku kejadian pelanggaran DKS; dan

(b) melaporkan sebarang pelanggaran Dasar ICT kepada JPICT atau mana-mana pihak berkuasa UTeM, sekiranya perlu.

6.5 LARANGAN

(a) Sebarang keperluan data atau maklumat yang ingin dicapai dan diambil bagi tujuan mengguna, menghebah atau untuk tujuan prosedur di mana-mana keperluan yang dikenalpasti, hendaklah dimohon kepada pemilik sistem.

(b) Semua keperluan data atau maklumat terperinngkat hendaklah dinyatakan dengan jelas tujuan penggunaannya semasa permohonan mendapatkan maklumat dilakukan; dan

(c) Maklumat kesihatan hanya boleh diambil oleh Pegawai Perubatan yang bertauliah namun masih tertakluk kepada kelulusan JPICT.

6.6 DATA PERIBADI

(a) Data peribadi berikut boleh diambil bagi tujuan carian direktori staf atau apa-apa tujuan rasmi yang lain:

(i) Nama;

(ii) Gelaran;

(iii) Pusat Tanggungjawab (PTj); dan

(iv) Nombor Telefon (Pejabat).

(j) Hak untuk meminta capaian kepada maklumat peribadi dan hak untuk membuat pindaan atau pembetulan jika terdapat kesilapan hendaklah dimaklumkan kepada pemilik sistem tersebut.

6.7 HAD PENGGUNAAN MAKLUMAT PERIBADI

Had penggunaan data dan maklumat peribadi adalah seperti mana di dalam Notis Perlindungan Data Peribadi yang boleh dicapai di laman sesawang rasmi UTeM.

6.8 PENYELENGGARAAN PENGGUNAAN DATA PERIBADI

(a) Pengguna bertanggungjawab memastikan ketepatan data peribadi sentiasa dikemas kini untuk tujuan yang diperlukan. Maklumat terperingkat hendaklah dikemaskini dari semasa ke semasa mengikut keperluan pemilik sistem.

(b) UTeM bertanggungjawab menjamin keselamatan maklumat yang disimpan dengan mematuhi DKS.

(c) UTeM bertanggungjawab menjamin kerahsiaan data peribadi. Individu yang bertanggungjawab menyimpan, mengumpul atau memproses data mestilah memastikan data peribadi tidak disebarkan kepada pihak lain, selain daripada mereka yang mempunyai hak untuk mengetahui maklumat tersebut.

(d) PTj hendaklah melakukan pertukaran pemilik sistem sekiranya pemilik berpindah atau pertukaran bidang tugas.

BAB 7: DASAR KESELAMATAN SIBER

7.1 PENGENALAN

7.1.1 LATAR BELAKANG

7.1.1.1. DKS ini ialah dokumen yang menetapkan hala tuju dalam usaha memastikan keselamatan data dan maklumat secara menyeluruh di UTeM.

7.1.1.2. DKS ini disediakan dengan tujuan untuk melindungi kerahsiaan, integriti, dan ketersediaan data dan maklumat di UTeM merangkumi arahan, peraturan, garis panduan, dan amalan yang ditetapkan untuk melindungi data dan maklumat daripada capaian yang tidak sah, kehilangan, atau pendedahan yang tidak dibenarkan.

7.1.1.3. DKS ini mentakrifkan kawalan keselamatan yang bersesuaian berdasarkan dasar, pekeliling, garis panduan kerajaan semasa yang berkuat kuasa serta mengikut amalan terbaik keselamatan yang relevan.

7.1.2 OBJEKTIF

7.1.2.1. Objektif Dasar ini adalah:-

(a) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem makklumat daripada kesan kegagalan atau kelemahan dalam aspek kerahsiaan, integriti, kebolehsediaan, dan kesahihan makkumat serta penyangkalan;

(b) Mematuhi keperluan perundangan, peraturan, standard, pekeliling dan prosedur yang sedang berkuat kuasa;

(c) Melaksanakan pengurusan risiko dan insiden keselamatan siber yang lebih berkesan;

(d) Memastikan penyampaian perkhidmatan UTeM pada tahap keselamatan tertinggi yang dapat meningkatkan keyakinan pihak berkepentingan seperti jabatan kerajaan, industri, dan orang awam;

(e) Menjamin kelancaran operasi dan kesinambungan perkhidmatan UTeM dengan meminumkan impak insiden keselamatan maklumat fizikal dan logical;

(f) Memudahkan perkongsian data dan maklumat yang selamat dan terjamin;

(g) Mencegah sebarang penyalahgunaan atau kecurian data dan maklumat kerajaan; dan

(h) Menyediakan asas bagi penambahbaikan yang berterusan dalam pengurusan keselamatan dan pentadbiran teknologi maklumat dan komunikasi.

7.1.3 SKOP

7.1.3.1 DKS ini merupakan panduan utama bagi semua pengguna yang terlibat dalam pengurusan data dan maklumat di UTeM. DKS ini memperincikan peranan, tanggungjawab, arahan, peraturan, garis panduan, dan amalan yang **WAJIB DIBACA, DIFAHAMI dan DIPATUHI** oleh semua pengguna yang terlibat dengan perkhidmatan teknologi maklumat dan komunikasi UTeM.

7.1.3.2 DKS ini juga terpakai untuk perlindungan terhadap semua aset maklumat UTeM, yang meliputi data dan maklumat dalam bentuk digital *(softcopy)* atau bercetak *(hardcopy)*, perkakasan, perisian, infrastruktur ICT, manusia, dan kampus.

7.1.3.3 DKS ini menetapkan keperluan asas seperti yang berikut:

(a) **Kebolehcapaian Data dan Maklumat**: Data dan maklumat mesti dapat dicapai secara berterusan dengan pantas, tepat, mudah, dan boleh dipercayai. Ini adalah penting untuk memastikan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti

(b) **Kerahsiaan dan Kesempurnaan Maklumat**: Semua data dan maklumat hendaklah dilindungi kerahsiaannya dan dikendalikan dnegan baik pada setiap masa untuk memastikan ketepatan serta melindungi kepentingan kerajaan, perkhidmatan, dan masyarakat.

7.1.3.4 Untuk memastikan keselamatan aset maklumat sepanjang masa, DKS ini meliputi perlindungan semua bentuk data dan maklumat kerajaan yang diwujudkan, diproses, disimpan, dihantar, sedang digunakan, diedarkan, disimpan, diselenggara, dihapuskan, dan dimusnahkan serta diarkibkan dalam persekitaran ICT UTeM. Perlindungan ini dilaksanakan melalui sistem kawalan dan prosedur pengendalian yang menyeluruh bagi elemen-elemen yang berikut:

(a) **Data dan Maklumat**: Koleksi fakta dalam bentuk kelas atau mesej elektronik yang digunakan untuk mencapai misi dan objektif jabatan. Contohnya, sistem dokumentasi, prosedur **operasi**, rekod, pangkalan data, dan arkib maklumat.

(b) **Salinan Digital *(Softcopy)***: Fakta dalam bentuk digital yang digunakan untuk mencapai misi dan objektif jabatan, termasuk rekod digital, pangkalan data dan arkib maklumat.

(c) **Salinan Bercetak *(Hardcopy)***: Fakta dalam bentuk bercetak, seperti sistem dokumentasi, prosedur operasi, rekod dan fail-fail.

(d) **Perkakasan *(Hardware)***: Semua aset fizikal yang menyokong pemprosesan dan penyimpanan maklumat, termasuk komputer, *server*, dan peralatan komunikasi.

(e) **Perisian (Software)**: Program dan dokumentasi yang berkaitan dengan sIstem komputer, termasuk perisian aplikasi dan sistem operasi yang digunakan untuk pemprosesan maklumat di UTeM.

(f) **Infrastruktur ICT**: Set lengkap perkakasan, perisian, rangkaian, dan kemudahan yang menyokong pemprosesan, penyimpanan, dan penghantaran maklumat dalam organisasi. Ini termasuk LAN, WAN, sistem kad akses, perkhidmatan pengkomputeran awan, serta kemudahan sokongan seperti bekalan elektrik dan sistem pencegah kebakaran.

(g) **Manusia**: Individu yang memiliki pengetahuan dan kemahiran untuk melaksanakan tugas harian bagi mencapai misi dan objektif UTeM berdasarkan tugas dan peranan masing-masing.

(h) Kampus: Semua kemudahan dan kampus yang menempatkan aset-aset di atas, yang mesti dilindungi dengan ketat untuk mencegah kebocoran rahsia atau kelemahan perlindungan, yang akan dianggap sebagai pelanggaran keselamatan.

7.1.3.5 DKS ini memastikan bahawa setiap aspek di atas diberikan perlindungan yang sewajarnya, meminimumkan risiko dan mengekalkan integriti operasi UTeM.

7.1.4 PERNYATAAN DASAR KESELAMATAN SIBER

7.1.4.1 UTeM komited untuk mengekalkan persekitaran yang selamat bagi aset maklumat dengan melaksanakan kawalan keselamatan siber yang berkesan selaras dengan standard dan rangka kerja keselamatan siber yang ditetapkan dari semasa ke semasa.

7.1.5 PRINSIP KESELAMATAN DATA DAN MAKLUMAT

Prinsip-prinsip keselamatan data dan maklumat yang menjadi asas kepada DKS ini dan perlu dipatuhi ialah seperti yang berikut:

7.1.5.1 **Capaian Atas Dasar Perlu Mengetahui**

Capaian terhadap penggunaan aset data dan maklumat hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar perlu mengetahui sahaja. Ini bermakna capaian hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut.

7.1.5.2 **Hak Capaian Minimum**

Pengguna hendaklah diberikan hak capaian minimum iaitu terhad kepada keperluan untuk menjalankan tugasnya. Hak capaian pengguna hanya diberi pada tahap 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 atau capaian sistem hendaklah dihadkan kepada pengguna yang dibenarkan mengikut peranan dalam fungsi tugas mereka dan kebenaran untuk melaksanakan operasi tertentu berdasarkan peranan tersebut. Hak capaian perlu dikaji mengikut sela masa yang ditetapkan atau **sekurang-kurangnya sekali dalam tempoh setahun.**

7.1.5.3 **Akauntabiliti**

Semua pengguna bertanggungjawab ke atas semua tindakannya terhadap aset maklumat UTeM. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap perlindungan keselamatan yang diperlukan oleh sesuatu sumber/aset maklumat. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem ICT tersebut boleh dipertanggungjawabkan atas tindakan mereka. Akauntabiliti atau tanggungjawab pengguna termasuklah:

(a) Menghalang pendedahan data dan maklumat kepada pihak yang tidak dibenarkan;

(b) Memeriksa dan menentukan data dan maklumat adalah tepat dan lengkap dari masa ke masa;

(c) Menentukan maklumat sedia untuk digunakan;

(d) Menjaga kerahsiaan kata laluan;

(e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;

(f) Memberi perhatian kepada maklumat terperingkat terutama semasa diwujudkan, diproses, disimpan, dihantar, sedang digunakan, diedarkan, disimpan, diselenggara, dihapuskan dan dimusnahkan serta diarkibkan; dan

(g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

7.1.5.4 **Pengasingan Tugas**

(a) Bagi mengekalkan prinsip semak dan imbang *(check and balance)*, PTj/PBU hendaklah melaksanakan perasingan tugas bagi tugas yang kritikal supaya tidak dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

(b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset data dan maklumat daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasikan. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian, keselamatan dan aplikasi mengikut kesesuaian.

7.1.5.5 **Prinsip Kepercayaan Sifar *(Zero Trust)***

Prinsip ini menegaskan bahawa tiada pengguna, peranti, atau rangkaian harus dipercayai secara automatik, sama ada berada dalam atau luar perimeter rangkaian. Setiap permintaan untuk mencapai data dan maklumat hendaklah melalui proses pengesahan yang teliti sebelum hak capaian diberikan. Prinsip ini menyatakan bahawa:

(a) semua trafik rangkaian (dalaman dan luaran) dianggap sebagai tidak dipercayai;

(b) capaian kepada sumber diberikan berdasarkan set kriteria yang komprehensif dan dinamik, termasuk identiti pengguna, keadaan dan kesihatan peranti, lokasi capaian, serta faktor konteks lain yang relevan. Capaian kepada sumber hanya akan diluluskan selepas pengesahan menyeluruh terhadap identiti pengguna dan status peranti, tanpa mengira lokasi fizikal, untuk memastikan keselamatan yang maksimum; dan

(c) menekankan prinsip keistimewaan yang paling sedikit, capaian kepada sumber yang perlu dicapai akan akan diberikan berdasarkan keperluan, apabila diperlukan dan hanya untuk masa yang ditetapkan.

7.1.5.6 **Pengauditan**

Pengauditan ialah tindakan untuk menilai, memeriksa, serta menganalisis aktiviti, rekod dan proses yang telah dilaksanakan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Tujuannya adalah untuk memastikan bahawa aktiviti tersebut mematuhi peraturan, piawaian, dan prosedur yang ditetapkan serta untuk mengidentifikasikan sebarang isu, ketidakpatuhan, atau potensi risiko. Oleh itu, aset data dan maklumat seperti komputer, *server,* penghala rangkaian *(network router)*, tembok keselamatan *(firewall)* dan peralatan rangkaian hendaklah dapat menjana dan menyimpan log tindakan keselamatan atau jejak audit.

7.1.5.7 **Pematuhan**

Dasar ini hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan data dan maklumat.

7.1.5.8 **Pemulihan**

Pemulihan sistem amat perlu untuk memastikan kesediaan 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.

7.1.5.9 **Saling Bergantungan**

Setiap prinsip keselamatan adalah saling melengkapi dan bergantung antara dengan lain untuk membentuk sistem keselamatan yang menyeluruh dan berkesan. Prinsip-prinsip ini tidak boleh dilaksanakan secara terpisah, tetapi mesti diintegrasikan dan diselaraskan untuk mencapai keselamatan yang maksimum.

7.1.6 CIRI KESELAMATAN DATA DAN MAKLUMAT

Ciri-ciri keselamatan data dan maklumat yang perlu yang perlu diberi perhatian oleh semua pihak merangkumi perkara yang berikut:

7.1.6.1 Kerahsiaan

Kerahsiaan merujuk kepada perlindungan data dan maklumat daripada capaian yang tidak dibenarkan. Ciri keselamatan ini bertujuan untuk memastikan bahawa hanya pihak yang sah dan berhak sahaja boleh mencapai data dan maklumat tertentu. Perkara ini penting untuk melindungi maklumat terperingkat seperti data peribadi, maklumat kewangan, dan rahsia perniagaan. Langkah-langkah yang biasa digunakan untuk mengekalkan kerahsiaan termasuk penyulitan maklumat, kawalan capaian yang ketat, dan penggunaan kata laluan yang kukuh.

7.1.6.2 Integriti

Integriti merujuk kepada ketepatan, kelengkapan, dan kesempurnaan data dan maklumat. Ciri ini diperlukan bagi memastikan bahawa data dan maklumat tidak diubah suai atau dirosakkan oleh pihak yang tidak dibenarkan. Sebarang perubahan terhadap data dan maklumat hendaklah dilakukan hanya oleh pihak yang mempunyai kebenaran yang sah dan perubahan tersebut hendaklah direkodkan dengan jelas

untuk tujuan audit. Integriti adalah sangat penting dalam memastikan bahawa keputusan yang dibuat berdasarkan data dan maklumat tersebut adalah tepat dan boleh dipercayai

7.1.6.3 Tidak Boleh Disangkal

Ciri ini memastikan bahawa pihak yang bertanggungjawab terhadap penciptaan, penghantaran, atau penerimaan data dan maklumat tidak boleh menafikan penglibatan mereka. Dalam transaksi digital, ciri ini dapat membuktikan penglibatan pihak tertentu dalam transaksi secara digital yang dilaksanakan. Contoh langkah keselamatan yang digunakan untuk memastikan tiada penafian termasuk penggunaan tandatangan digital dan rekod transaksi yang terperinci dalam jejak audit.

7.1.6.4 Kesahihan

Kesahihan merujuk kepada pengesahan bahawa data dan maklumat adalah sah dan berasal daripada sumber yang dipercayai. Ciri kesahihan memastikan bahawa data dan maklumat yang diterima atau dihantar tidak dimanipulasi oleh pihak ketiga. Langkah-langkah seperti penggunaan sijil digital dan protokol pengesahan membantu memastikan bahawa maklumat yang diterima adalah sahih dan boleh dipercayai.

7.1.6.5 Ketersediaan

Ketersediaan memastikan bahawa data dan maklumat boleh dicapai oleh pihak yang dibenarkan pada bila-bila masa yang diperlukan. Ketersediaan adalah penting untuk memastikan operasi harian dan membuat keputusan yang tepat pada masanya. Untuk mengekalkan ketersediaan, semua pihak yang terlibat hendaklah melaksanakan langkah-langkah seperti menyediaan dan pengaktifan pelan

pemulihan bencana, menyediakan sistem sandaran, dan melaksanakan pengurusan risiko yang menyeluruh untuk mengurangkan gangguan terhadap capaian data dan maklumat.

7.1.7 IMPLIKASI

Ketidakpatuhan terhadap DKS ini boleh mengakibatkan pelbagai implikasi yang serius, termasuk tetapi tidak terhad kepada:

(a) **Risiko Keselamatan**: Ketidakpatuhan boleh menyebabkan pendedahan maklumat terperingkat, pencerobohan sistem, atau gangguan operasi, yang boleh mengakibatkan kehilangan maklumat penting atau kerosakan kepada infrastruktur digital.

(b) **Gangguan Operasi**: Ketidakpatuhan boleh menyebabkan gangguan kepada operasi harian Jabatan, termasuk masa henti *(time out)* sistem, kehilangan data, dan kerosakan peralatan, yang boleh memberi kesan langsung kepada penyampaian perkhidmatan.

(c) **Kesan Undang-Undang**: Kegagalan mematuhi mana-mana bahagian DKS ini boleh menyebabkan tindakan undang-undang diambil terhadap pihak yang terlibat, termasuk denda atau tindakan undang-undang lain yang berkaitan dengan pelanggaran peraturan dan undang-undang keselamatan siber.

(d) **Kerugian Kewangan**: Ketidakpatuhan boleh membawa kepada kerugian kewangan yang besar, sama ada melalui denda, kos pemulihan, atau kehilangan kepercayaan pelanggan dan pihak berkepentingan yang boleh menjejaskan kedudukan kewangan UTeM.

(e) **Kerosakan Reputasi**: Insiden keselamatan siber yang disebabkan oleh ketidakpatuhan boleh merosakkan reputasi UTeM, mengurangkan kepercayaan pihak berkepentingan dan masyarakat umum terhadap keupayaan UTeM dalam menguruskan keselamatan maklumat.

(f) **Tindakan Disiplin**: Pengguna hendaklah mematuhi DKS ini. Sebarang pelanggaran terhadap mana-mana atau keseluruhan DKS ini, boleh dikenakan tindakan di bawah:-

(i) Akta 605 bagi staf;

(ii) KTP bagi pelajar; atau

(iii) undang-undang lain yang berkuatkuasa bagi pihak luar.

7.2 TADBIR URUS

7.2.1 Bagi memastikan keberkesanan dan kejayaan pelaksanaan DKS ini, sebuah struktur tadbir urus yang mantap telah diwujudkan dengan penubuhan JPICT. Rujuk Bab 2 – Dasar Pengurusan ICT

7.3 PENGURUSAN RISIKO

7.3.1 Semua pihak yang terlibat dalam pengurusan data dan maklumat di UTeM hendaklah mengambil kira risiko yang wujud terhadap aset data dan maklumat akibat kelemahan *(vulnerability)* dan ancaman yang semakin berkembang dalam persekitaran digital masa kini. Oleh itu, langkah-langkah proaktif dan bersesuaian perlu diambil untuk menilai tahap risiko terhadap aset maklumat, bagi memastikan pendekatan dan keputusan yang paling berkesan dapat dikenal pasti dalam menyediakan perlindungan dan kawalan yang optimum.

7.3.2 Penilaian risiko ini bertujuan untuk mengenal pasti dan mengambil tindakan susulan serta langkah-langkah mitigasi yang bersesuaian bagi mengurangkan atau mengawal risiko keselamatan maklumat berdasarkan penemuan daripada penilaian risiko tersebut. Penilaian risiko keselamatan maklumat hendaklah dilaksanakan secara berkala **sekurang-kurangnya sekali setahun sekiranya terdapat perubahan aset maklumat**.

7.3.3 Laporan Penilaian Risiko dan Pelan Pengurangan Risiko harus dijadikan agenda tetap dalam mesyuarat bahagian atau mesyuarat yang setara dengannya, dan dimaklumkan kepada Mesyuarat JKICT.

7.3.4 Penilaian risiko keselamatan data dan maklumat hendaklah dilaksanakan ke atas semua aset maklumat UTeM, termasuk aset fizikal, aplikasi, perisian, *server*, rangkaian, serta proses dan prosedur yang berkaitan. Selain itu, penilaian risiko ini juga perlu dijalankan di kampus yang menempatkan aset maklumat seperti pusat data, bilik media storan, kemudahan utiliti, dan sistem-sistem sokongan lain.

7.3.5 Dalam menghadapi potensi risiko, semua pihak yang terlibat perlu mengenal pasti tindakan yang sewajarnya, termasuk:

(a) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
(b) Menerima atau bersedia menghadapi risiko yang mungkin berlaku selagi risiko tersebut tidak menjejaskan penyampaian perkhidmatan UTeM;
(c) Mengelakkan atau mencegah risiko dengan mengambil langkah-langkah yang dapat mengelakkan atau mencegah mencegah terjadinya risiko; dan
(d) Memindahkan risiko kepada pihak ketiga seperti pembekal, pakar runding, atau pihak berkepentingan lain.

7.3.6 Pelan ini hendaklah mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data. Pelan Pengurusan Keselamatan Maklumat hendaklah mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen barikut:

(a) Peranti Pengkomputeran Peribadi
    (i) Peranti Pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan system. Contoh peranti pengkomputeran peribadi ialah komputer riba, telefon pintar, tablet dan peranti storan.

(b) Peranti Rangkaian

(i) Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan system seperti *switch*, penghala rangkaian, tembok keselamatan, peranti *Visual Private Network* (VPN) dan kabel.

(ii) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data dalam pergerakan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

(c) Aplikasi

(i) Perisian aplikasi digunakan oleh manusia untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi ialah pelayan web, pelayan aplikasi dan sistem operasi.

(ii) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi datadalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

(d) *Server*

(i) *Server* ertinya pelayan iaitu komputer yang mempunyai keupayaan tinggi yang memberi perkhidmatan berpusat.

(ii) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data dalam penggunaan, datadalam pergerakan, data dalam simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

(e) Persekitaran Fizikal

(i) Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan aset ICT.

(ii) Cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat hendaklah dirujuk Pejabat Ketua Pegawai Keselamatan Kerajaan untuk mendapatkan nasihat seta hendaklah selaras dengan perundangan dan arahan yang sedang berkuat kuasa.

(iii) Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip kawalan *defend-in-depth.*

7.4 PENGURUSAN KESELAMATAN MAKLUMAT

7.4.1 Setiap projek ICT yang hendak dilaksanakan di UTeM perlu memastikan keselamatan maklumat terjamin. Pemilik projek perlu mengambilkira isu-isu keselamatan data dan maklumat dan membuat penilaian risiko.

7.4.2 Pelan ini hendaklah dibangunkan dengan berpandukan surat pekeliling/arahan yang sedang berkuat kuasa untuk menangani isu keselamatan operasi semasa projek dilaksanakan.

7.5 KAWALAN ORGANISASI

Terdapat 37 kawalan organisasi yang terpakai dalam perlu dipatuhi oleh semua pihak yang terlibat dalam pengurusan data dan maklumat di UTeM. Perincian kawalan organisasi seperti di bawah:

7.5.1 DASAR KESELAMATAN SIBER

ID	KETERANGAN	PERANAN
7.5.1.1	**Pelaksanaan Dasar** Satu set dasar untuk keselamatan siber perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan kepada pengguna yang mempunyai urusan dengan perkhidmatan ICT di UTeM. Pelaksanaan DKS hendaklah dikuatkuasakan oleh Naib Canselor dengan disokong oleh JPICT UTeM.	Naib Canselor
7.5.1.2	**Pengesahan Dasar** DKS perlu diperakui di peringkat pengurusan tertinggi UTeM.	Lembaga Pengarah Universiti
7.5.1.3	**Penguatkuasaan Dasar** DKS hendaklah dipatuhi oleh semua pengguna, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT di UTeM. Sebarang ketidakpatuhan kepada DKS ini boleh mengakibatkan tindakan termasuk sebarang remedi/	Pihak yang mempunyai urusan dengan perkhidmatan ICT UTeM

ID	KETERANGAN	PERANAN
	tindakan undang- undang lain di bawah akta/ peraturan/ undang- undang semasa yang berkuat kuasa	
7.5.1.4	**Penyebaran Dasar** Program kesedaran tentang DKS ini hendaklah diatur dan diselaraskan.	ICTSO
7.5.1.5	**Pengecualian Dasar** Keselamatan ICT UTeM adalah terpakai kepada pengguna, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT di UTeM dan tiada pengecualian diberikan	Pengguna yang mempunyai urusan dengan perkhidmatan ICT UTeM
7.5.1.6	**Penyelenggaraan Dasar** Penyelenggaraan dan kajian semula DKS hendaklah dilaksanakan mengikut keperluan. Semua dokumen atau rekod hendaklah diwujudkan dan diselenggara untuk menyediakan bukti pematuhan kepada keperluan dan operasi berkesan pengurusan keselamatan maklumat. Semua dokumen dan rekod hendaklah dilindungi dan dikawal mengikut undang-undang/arahan/peraturan/garis panduan semasa yang berkuat kuasa.	CDO, ICTSO

ID	KETERANGAN	PERANAN
7.5.1.7	**Kajian Semula/Semakan Dasar** DKS ini perlu disemak dan dipinda apabila terdapat perubahan teknologi, aplikasi, prosedur, perundangan, dan polisi Kerajaan bagi memastikan kesesuaian, kecukupan dan keberkesanannya berterusan	CDO, ICTSO

7.5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
7.5.2.1	**Peranan dan Tanggungjawab Keselamatan Maklumat** Semua peranan dan tanggungjawab keselamatan maklumat hendaklah ditakrifkan dan diperuntukkan mengikut keperluan. Peranan dan tanggungjawab keselamatan maklumat ialah seperti berikut: **(a) Naib Canselor** Tanggungjawab: (i) Memastikan penguatkuasaan DKS ini. (ii) Memastikan pengguna yang mempunyai urusan dengan perkhidmatan ICT di UTeM memahami dan mematuhi peruntukan-peruntukan di bawah DKS ini.	Naib Canselor

ID	KETERANGAN	PERANAN
	(iii) Memastikan semua keperluan seperti sumber kewangan, staf dan perlindungan keselamatan adalah mencukupi. (iv) Memastikan pengurusan risiko dan program keselamatan siber dilaksanakan seperti yang ditetapkan dalam DKS. (v) Melantik CDO. **(b) Ketua Pegawai Digital (CDO)** CDO yang dilantik hendaklah mempunyai pengalaman dalam bidang teknikal serta transformasi digital yang kukuh. Tanggungjawab: (diambil dari statut) (i) menjadi ketua Pejabat Ketua Pegawai Digital. (ii) menjadi ahli jawatankuasa pengurusan dan mana-mana jawatankuasa lain sebagaimana yang ditetapkan oleh Perlembagaan, statut-statut, kaedah-kaedah dan peraturan-peraturan UTeM. (iii) menjadi pengerusi Mesyuarat Pejabat Ketua Pegawai Digital, mesyuarat pengurusan PTj dan Mesyuarat Teknikal ICT peringkat UTeM. (iv) bertanggungjawab terhadap perkara berkaitan pembangunan dan perkhidmatan termasuk kemudahan asas infostruktur dan infrastruktur, polisi dan latihan kemahiran kepada pekerja dalam hal teknologi maklumat dan komunikasi. (v) bertanggungjawab kepada Naib Canselor dalam semua aspek pengurusan maklumat, teknologi maklumat dan teknologi komunikasi antara Pusat Tanggungjawab di UTeM.	

ID	KETERANGAN	PERANAN
	(vi) melaksanakan apa-apa kuasa dan kewajipan lain dan mengambil apa-apa tindakan sebagaimana yang diperlukan dalam menjalankan kuasa dan kewajipan yang ditetapkan oleh Perlembagaan, statut-statut, kaedah-kaedah dan peraturan-peraturan UTeM. (vii) menjalankan apa-apa kuasa dan kewajipan lain yang diarahkan oleh Lembaga, Senat dan Naib Canselor dari semasa ke semasa. **(c) Pegawai Keselamatan ICT (ICTSO)** ICTSO yang dilantik hendaklah mempunyai pengalaman dalam bidang teknikal, keselamatan rangkaian, pengurusan insiden dan perlindungan data yang kukuh. Tanggungjawab: (i) Mengurus keseluruhan program-program keselamatan ICT UTeM. (ii) Menguatkuasakan pelaksanaan DKS. (iii) Memberi penerangan dan pendedahan berkenaan DKS kepada semua pengguna. (iv) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan DKS. (v) Menjalankan pengurusan risiko. (vi) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan UTeM berdasarkan hasil penemuan dan menyediakan laporan mengenainya.	

ID	KETERANGAN	PERANAN
	(vii) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian. (viii) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah- langkah baik pulih dengan segera. (ix) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT. (x) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan. **d) Ketua PTj / PBU** Tanggungjawab: (i) Melaksanakan keperluan DKS dalam operasi semasa pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu, pembelian atau peningkatan perisian dan sistem komputer serta perolehan teknologi dan perkhidmatan komunikasi baharu. (ii) Memastikan pembekal dan pihak ketiga yang berkaitan dengan perkhidmatan ICT di UTeM membuat perakuan pematuhan DKS ini. (iii) Memastikan pematuhan kepada pelaksanaan rangka kerja, dasar, polisi, pekeliling/ garis	

ID	KETERANGAN	PERANAN
	panduan dan pelan pengurusan keselamatan maklumat UTeM yang berkuat kuasa dari semasa ke semasa. **(e) Pentadbir ICT** Tanggungjawab: (i) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai staf yang berhenti, bertukar, atau berlaku perubahan dalam bidang tugas. (ii) Menentukan ketepatan dan kesahihan sesuatu tahap capaian berdasarkan arahan pemilik sistem seperti mana yang telah ditetapkan di dalam DKS ini. (iii) Memantau aktiviti capaian sistem. (iv) Mengenal pasti dan melaporkan aktiviti-aktiviti tidak normal seperti pencerobohan atau pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta- merta. (v) Menganalisis dan menyimpan rekod jejak audit. (vi) Menyediakan laporan mengenai aktiviti capaian secara berkala. **(f) Pemilik Sistem** Tanggungjawab Pemilik Sistem merujuk kepada Perenggan 5.5.3, Bab 5 Dasar Aplikasi	

ID	KETERANGAN	PERANAN
	(g) Pengurus ICT Pengurus ICT bagi UTeM adalah staf yang menguruskan infrastruktur ICT seperti rangkaian, perkakasan ICT, pusat data dll. Peranan dan tanggungjawab Pengurus ICT ialah seperti yang berikut: (i) Mentadbir akaun pengguna. (ii) Merangka, melaksana dan menguatkuasakan DKS seperti perlindungan dan perkongsian data. (iii) Merancang dan melaksana polisi ancaman keselamatan, memantau keadaan rangkaian dan mengawal penggunaan sumber. (iv) Pemantauan aktiviti capaian harian pengguna. (v) Menyediakan laporan mengenai aktiviti capaian secara berkala. (vi) Menyelia dan membuat proses sandaran *server.* (vii) Memberi bantuan dalam menyelesaikan masalah-masalah berkaitan rangkaian yang dilaporkan oleh pengguna. **(h) Jawatankuasa Pemandu ICT (JPICT)** Peranan dan tanggungjawab JPICT seperti yang dinyatakan di Bab 1 Dasar Pengurusan. **(i) UTeM Cyber Security Incident Response Team (UTeM-CSIRT)** Peranan dan tanggungjawab JPICT seperti yang dinyatakan di Bab 2 Dasar Pengurusan.	

ID	KETERANGAN	PERANAN
	j) Pengguna (i) Membaca, memahami dan mematuhi DKS ini. (ii) Mengetahui dan memahami implikasi keselamatan siber kesan daripada tindakannya. (iii) Menjalani tapisan keselamatan sekiranya diperlukan dikehendaki berurusan dengan maklumat terperingkat. (iv) Mematuhi prinsip-prinsip keselamatan yang dinyatakan dalam DKS ini dan menjaga kerahsiaan maklumat UTeM. (v) Melaksanakan langkah-langkah perlindungan seperti yang berikut: (vi) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan. (vii) Memeriksa maklumat dan menentukan maklumat tersebut sentiasa tepat dan lengkap dari semasa ke semasa. (viii) Menentukan maklumat sedia untuk digunakan. (ix) Menjaga kerahsiaan maktumat. (x) Mematuhi dasar, piawaian dan garis panduan keselamatan siber yang ditetapkan. (xi) Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan. (xii) Menjaga kerahsiaan kawalan keselamatan siber dari diketahui umum.	

ID	KETERANGAN	PERANAN
	(xiii) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada UTeM-CSIRT dengan segera; (xiv) Menghadiri program-program kesedaran mengenai keselamatan siber; dan (xv) Bersetuju dengan terma dan syarat yang terkandung dalam DKS ini.	

7.5.3 PENGASINGAN TUGAS

ID	KETERANGAN	PERANAN
7.5.3.1	**Pengasinagan Tugas** Pengasingan tugas dan bidang tanggungjawab dilaksanakan bagi mengurangkan peluang pengubahsuaian data dan maklumat tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT	Pengarah/ Pentadbir ICT/ Pengurus ICT

ID	KETERANGAN	PERANAN
	daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. (b) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai produksi. (c) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian. (d) Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya. (e) Semakan dan pemantauan hak capaian perkakasan, perisian dan sistem hendaklah dilaksanakan secara berkala.	

7.5.4 TANGGUNGJAWAB PENGURUSAN

ID	KETERANGAN	PERANAN
7.5.4.1	**Tanggungjawab Pengurusan** Pelaksanaan DKS ini dijalankan oleh Naib Canselor dengan disokong oleh JPICT UTeM. DKS hendaklah dipatuhi oleh semua pengguna yang mempunyai urusan dengan perkhidmatan ICT di UTeM.	Naib Canselor, CDO, JPICT, JKICT

ID	KETERANGAN	PERANAN
	Ketua PTj/ PBU UTeM hendaklah memastikan semua pengguna yang mempunyai urusan dengan perkhidmatan ICT supaya mengamalkan keselamatan maklumat mematuhi DKS dan prosedur yang ditetapkan.	

7.5.5 HUBUNGAN DENGAN PIHAK BERKUASA

ID	KETERANGAN	PERANAN
7.5.5.1	**Hubungan dengan Pihak Berkuasa** Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara- perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab. (b) Mewujudkan dan mengemas kini prosedur/ senarai pihak berkuasa perundangan/ pihak yang dihubungi semasa kecemasan. Pihak berkuasa perundangan ialah Polis Diraja Malaysia dan Suruhanjaya Komunikasi dan Multimedia. Pihak yang dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik,	ICTSO, UTeM-CSIRT, Pemilik Sistem

ID	KETERANGAN	PERANAN
	keselamatan dan kesihatan serta bomba, penyedia perkhidmatan telekomunikasi dan perkhidmatan bekalan air. (c) Insiden keselamatan maklumat harus dilaporkan tepat pada masanya kepada UTeM-CSIRT, Ketua PTj/PBU dan pihak berkaitan seperti Agensi Keselamatan Siber (NACSA) selaras dengan pekeliling berkaitan yang sedang berkuatkuasa bagi mengurangkan impak insiden.	

7.5.6 HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN YANG KHUSUS

ID	KETERANGAN	PERANAN
7.5.6.1	**Hubungan dengan Kumpulan Berkepentingan yang Khusus** Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menganggotai pertubuhan profesional atau forum yang berkaitan bagi: (a) Meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat.	ICTSO, UTeM-CSIRT, Pemilik Sistem

ID	KETERANGAN	PERANAN
	(b) Memastikan pemahaman tentang persekitaran keselamatan maklumat adalah terkini. (c) Menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini. (d) Mendapat capaian kepada nasihat pakar keselamatan maklumat. (e) Berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan. (f) Berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.	

7.5.7 PERISIKAN ANCAMAN

ID	KETERANGAN	PERANAN
7.5.7.1	**Perisikan Ancaman** Maklumat berkaitan ancaman keselamatan maklumat yang berpotensi atau memberi ancaman kepada fungsi UTeM perlu diperoleh dan dianalisis untuk menghasilkan maklumat perisikan berkaitan ancaman. Maklumat tentang ancaman sedia ada atau baharu akan dikumpul dan dianalisis untuk memudahkan tindakan dan mengelakkan ancaman atau mengurangkan impak kepada aset maklumat yang terlibat.	UTeM-CSIRT, Pemilik Sistem, Pentadbir ICT, Pengurus ICT

ID	KETERANGAN	PERANAN
	Pemilik sistem hendaklah melaksanakan tindakan berikut bagi meningkatkan tahap kawalan keselamatan aset maklumat: (a) Mengenal pasti ancaman dengan melaksanakan penilaian risiko terhadap aset maklumat; (b) Mengenal pasti dan melaksanakan kawalan keselamatan yang berkaitan. Kawalan keselamatan tersebut juga dijadikan sebagai satu daripada keperluan dalam kitar hayat pembangunan sistem dan penyediaan infrastruktur ICT; dan (c) Menjadikan ancaman sebagai satu daripada ancaman yang perlu diambil kira dalam pelaksanaan ujian keselamatan sistem dan infrastruktur ICT	

7.5.8 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK

ID	KETERANGAN	PERANAN
7.5.8.1	**Keselamatan Maklumat dalam Pengurusan Projek** Aspek keselamatan secara keseluruhan iaitu fizikal, infrastruktur ICT, aplikasi dan data perlu diambil kira dalam menentukan pendekatan projek.	Pemilik Projek, Pengurus Projek

7.5.9 INVENTORI MAKLUMAT DAN ASET LAIN YANG BERKAITAN

ID	KETERANGAN	PERANAN
7.5.9.1	**Inventori Aset** Menyokong dan memberi perlindungan yang bersesuaian ke atas semua aset ICT jabatan. Tanggungjawab yang perlu dipatuhi merangkumi perkara yang berikut: (a) Memastikan pegawai penerima aset di setiap PTj dikenalpasti untuk mengurus penerimaan aset-aset ICT. (b) Memastikan semua aset ICT dikenal pasti, diklasifikasi, didokumentasikan, diselenggara dan dilupuskan. Maklumat aset direkod dan dikemas kini sebagaimana arahan dan peraturan yang berkuat kuasa dari semasa ke semasa. (c) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pegawai yang dibenarkan sahaja. (d) Memastikan inventori maklumat dan aset lain yang berkaitan hendaklah tepat, terkini, dan konsisten. (e) Pegawai Aset hendaklah mengesahkan penempatan aset ICT.	Pegawai Aset, Pegawai Penerima Aset
7.5.9.2	**Pemilikan Aset** Aset hak milik UTeM hendaklah diselenggara mengikut jadual penyelenggaraan yang ditetapkan serta mematuhi PKPU yang berkuatkuasa dari semasa ke semasa.	Pegawai Aset, Pemilik Aset

ID	KETERANGAN	PERANAN
	Tanggungjawab yang perlu dipatuhi oleh pemilik aset merangkumi perkara yang berikut: (a) Memastikan aset didaftarkan dalam senarai aset mengikut klasifikasi aset dan diserahkan kepada pemilik aset. (b) Memastikan semua jenis aset dipelihara dan diselenggara dengan baik. (c) Kenal pasti dan kaji semula capaian ke atas asset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan. (d) Memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapuskan atau dilupuskan. (e) Aset bukan hakmilik jabatan hendaklah diurus mengikut prosedur / arahan-arahan atau polisi *Bring Your Own Device* (BYOD) yang sedang berkuat kuasa.	
7.5.9.3	**Pengelasan Maklumat Aset** Memastikan setiap data dan maklumat dalam aset ICT dikelaskan mengikut klasifikasi dan peringkat keselamatan dokumen.	Pegawai Aset, Pegawai Pengelas

7.5.10 PENGGUNAAN MAKLUMAT YANG BOLEH DITERIMA DAN ASET LAIN YANG BERKAITAN

ID	KETERANGAN	PERANAN
7.5.10.1	**Penggunaan Aset yang dibenarkan** Memastikan penggunaan aset untuk tujuan rasmi dan mengikut fungsi sebenar yang telah ditetapkan oleh UTeM.	Pemilik Aset
7.5.10.2	**Pengendalian Aset** Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, membuat salinan, menghantar, menyampai, menukar dan memusnah perlu mengambil kira langkah-langkah keselamatan berikut: (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan. (b) Memeriksa dan menentukan maklumat adalah tepat dan lengkap dari smeasa ke semasa. (c) Menentukan maklumat sedia untuk digunakan. (d) Menjaga kerahsiaan kata laluan. (e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan. (f) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum. (g) Penyelenggaraan rekod pengguna yang dibenarkan bagi maklumat dan aset lain yang berkaitan.	Pegawai Aset, Pemilik Aset

7.5.11 PEMULANGAN ASET

ID	KETERANGAN	PERANAN
7.5.11.1	**Pemulangan Aset** Pengguna hendaklah mengembalikan aset termasuk semua aset lain yang berkaitan mengikut peraturan dan terma perkhidmatan yang ditetapkan. Pemulangan aset yang mengandungi maklumat rasmi kerajaan hendaklah disanitasi mengikut PKPU yang berkuatkuasa dari semasa ke semasa.	Pemilik Aset, Pegawai Aset

7.5.12 PENGELASAN DATA DAN MAKLUMAT

ID	KETERANGAN	PERANAN
7.5.12.1	**Pengelasan Maklumat** Data dan maklumat perlu dikelas oleh Pegawai Pengelas mengikut keperluan keselamatan maklumat yang telah ditetapkan berdasarkan keperluan perlindungan keselamatan maklumat tersebut. Pengelasan maklumat terdiri daripada aktiviti penentuan maklumat terperingkat iaitu rahsia besar, rahsia, sulit dan terhad. Perkara berikut hendaklah dilaksanakan oleh semua	Pegawai Pengelas

ID	KETERANGAN	PERANAN
	pihak yang terlibat dalam pengelasan maklumat: (a) Maklumat hendaklah dikelaskan oleh Pegawai Pengelas. (b) Memastikan tiada pendedahan maklumat kepada pihak yang tidak dibenarkan. (c) Memastikan kesemua fail fizikal dan digital maklumat disimpan mengikut keperluan perlindungan keselamatan yang telah ditetapkan oleh pihak kerajaan.	

7.5.13 PELABELAN MAKLUMAT

ID	KETERANGAN	PERANAN
7.5.13.1	**Pelabelan Maklumat** (a) Maklumat hendaklah dilabel dan dikendali berasaskan peringkat keselamatan yang dikenal pasti selaras dengan Arahan Keselamatan (Semakan dan Pindaan 2017) (b) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat	Pegawai Pengelas

7.5.14 PEMINDAHAN DATA DAN MAKLUMAT

ID	KETERANGAN	PERANAN
7.5.14.1	**Pengurusan Pemindahan Data dan Maklumat** Memastikan keselamatan perpindahan/pertukaran data, maklumat dan perisian antara pihak luar terjamin. Pihak luar ialah pihak yang menggunakan atau pihak yang membekalkan data, maklumat atau perisian	Pemilik Sistem, Pentadbir ICT
7.5.14.2	**Pesanan Elektronik** Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya mengikut arahan, peraturan dan garis panduan yang sedang berkuat kuasa bagi pengurusan pesanan elektronik.	Pengguna

7.5.15 KAWALAN CAPAIAN

ID	KETERANGAN	PERANAN
7.5.15.1	**Prosedur Kawalan Capaian** (a) Dokumen khusus mengenai kawalan capaian hendaklah ditakrifkan dengan mengambil kira keperluan ini dan harus dimaklumkan kepada semua pihak yang berkepentingan yang berkaitan. Pemilik sistem dan pemilik aset hendaklah menentukan tahap perlindungan keselamatan maklumat dan kawalan capaian	Pentadbir Akses, Pentadbir ICT, Pemilik Sistem

ID	KETERANGAN	PERANAN
	yang diperlukan bagi mencapai maklumat tersebut. (b) Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Kawalan capaian ditetapkan berdasar prinsip perlu tahu iatu capaian diberikan atas dasar keperluan untuk melaksanakan tugas dan keperluan untuk digunakan iaitu hanya diberikan capaian kepada infrastruktur teknologi maklumat di mana terdapat keperluan yang jelas. (c) Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Kawalan capaian perlu disemak, dikemas kini dan disahkan sekurang-kurangnya sekali dalam tempoh setahun atau mengikut keperluan sekiranya terdapat perubahan serta menyokong peraturan kawalan capaian pengguna sedia ada. (d) Perkara-perkara yang perlu dipertimbangkan dalam menentukan kawalan capaian ialah seperti berikut: (i) Menentukan entiti mana yang memerlukan jenis capaian kepada maklumat dan aset lain yang berkaitan. (ii) Keperluan keselamatan aplikasi ditentukan dan diselaraskan dengan keperluan capaian entiti.	

ID	KETERANGAN	PERANAN
	(iii) Hak capaian dan dasar klasifikasi maklumat sistem dan rangkaian. (iv) Capaian fizikal yang perlu disokong oleh kawalan kemasukan fizikal yang sesuai. (v) Penyebaran maklumat dan kebenaran capaian perlu mematuhi prinsip-prinsip keselamatan yang ditetapkan dan mengikut pengkelasan maklumat. (vi) Sekatan kepada capaian istimewa hendaklah dihadkan dan diurus (pengurusan capaian). (vii) Pengasingan tugas, fungsi kawalan capaian (contohnya permintaan capaian, kebenaran capaian, pentadbiran capaian). (viii) Patuh undang-undang, peraturan berkaitan yang berkuat kuasa semasa dan sebarang kewajipan kontrak berkaitan pengehadan capaian kepada data atau perkhidmatan. (ix) Kebenaran rasmi untuk permintaan capaian. (x) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran. (xi) Pengasingan peranan kawalan capaian. (xii) Kebenaran rasmi permohonan capaian. (xiii) Keperluan semakan hak capaian berkala. (xiv) Pembatalan hak capaian. (xv) Pengarkiban semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat. (xvi) Hak capaian istimewa. (xvii) Pengelogan aktiviti yang dilaksanakan.	

ID	KETERANGAN	PERANAN
7.5.15.2	**Capaian kepada Rangkaian dan Perkhidmatan Rangkaian** Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari Pejabat CDO. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Menempatkan atau memasang aset maklumat dan perkakasan ICT yang bersesuaian antara rangkaian UTeM, rangkaian jabatan lain dan rangkaian awam. (b) Mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian. (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Pengurus ICT
7.5.15.3	**Kawalan Capaian** Kawalan capaian adalah untuk mengurus, mengawasi, dan meningkatkan capaian maklumat dan aset maklumat dengan selamat. Ini merangkumi pelbagai aspek operasi dan pengurusan untuk memastikan mencapai matlamat, sasaran, dan hasil yang diinginkan dengan kawalan seperti yang berikut:	Pentadbir Akses, Pemilik Sistem, Pentadbir ICT

ID	KETERANGAN	PERANAN
	(a) Mematuhi undang-undang, peraturan, dan dasar yang berkaitan dengan keselamatan data dan maklumat. (b) Memastikan bahawa dasar, tatacara, dan amalan keselamatan maklumat diikuti dan dilaksanakan dengan betul. (c) Mengenal pasti, menilai, dan menguruskan risiko keselamatan maklumat yang berkaitan dengan operasi dan capaian maklumat organisasi. (d) Memastikan keselamatan maklumat dan data dalam organisasi dengan mematuhi amalan keselamatan maklumat yang sesuai. (e) Meningkatkan kesedaran dan kefahaman kakitangan tentang peningkatan capaian dan amalan keselamatan dalam organisasi. (f) Memantau dan menilai prestasi keselamatan capaian berterusan untuk mengenal pasti peningkatan dan kesan tindakan yang diperlukan	
7.5.15.4	**Keperluan Pemindahan Data dan Maklumat** Menghadkan capaian pengguna kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat. Memastikan dokumen perjanjian diwujudkan antara UTeM dengan pihak luar bagi pemindahan maklumat melibatkan pihak luar.	Pentadbir ICT, Pengurus ICT

7.5.16 PENGURUSAN IDENTITI

ID	KETERANGAN	PERANAN
7.5.16.1	**Pendaftaran dan Pembatalan Pengguna** Setiap pengguna bertanggungjawab ke atas aset maklumat yang diamanahkan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: (a) Akaun yang diperuntukkan kepada pengguna sahaja boleh digunakan. (b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna. (c) Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada Pemilik Sistem terlebih dahulu. (d) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan semua pengguna tertakluk kepada peraturan yang ditetapkan. (e) Akaun boleh ditarik balik jika penggunaannya melanggar peraturan. (f) Penggunaan akaun milik individu lain **DILARANG.** (g) Akaun pengguna tidak boleh dikongsi. Capaian kepada proses, data dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Semua capaian ini perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.	Pentadbir Akses, Pemilik Sistem, Pentadbir ICT

ID	KETERANGAN	PERANAN
7.5.16.2	**Pengurusan Identiti** Pengurusan akaun pengguna bagi capaian ke sistem atau aset maklumat bermula daripada penciptaan rekod pengguna baharu sehingga penamatan profil apabila pengguna telah meletakkan jawatan, bersara atau meninggal dunia dalam perkhidmatan. Pendaftaran, pengemaskinian dan penamatan akaun pengguna dilaksanakan mengikut prosedur yang ditetapkan. Proses pengurusan akaun pengguna hendaklah memastikan bahawa: (a) Identiti yang diberikan khusus hanya dikaitkan dengan seorang sahaja untuk membolehkan orang itu bertanggungjawab atas tindakan yang dilakukan dengan identiti khusus ini. (b) Identiti yang diberikan kepada entiti selain manusia seperti mesin atau sistem tertakluk kepada kelulusan yang diasingkan dengan sewajarnya dan pengawasan berterusan. (c) Rekod penggunaan dan pengurusan identiti pengguna dan maklumat pengesahan hendaklah disimpan. (d) Tahap capaian akaun pengguna akan dikemaskini atas sebab-sebab yang berikut: (i) Bertukar bidang tugas kerja. (ii) Bertukar ke PTj lain.	Pentadbir Akses, Pentadbir ICT, Pemilik Sistem

7.5.17 MAKLUMAT PENGESAHAN IDENTITI

ID	KETERANGAN	PERANAN
7.5.17.1	**Pengurusan Maklumat Pengesahan Identiti Pengguna** Peruntukan maklumat pengesahan identiti pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan. Peruntukan dan proses pengurusan hendaklah memastikan bahawa: (a) Kata laluan atau nombor pengenalan diri (*Personal Identification Number, PIN*) yang dijana secara automatik semasa proses pendaftaran sebagai maklumat pengesahan rahsia sementara dan pengguna dikehendaki menukarnya selepas penggunaan pertama. (b) Maklumat pengesahan tetapan asal (*default*) seperti yang ditetapkan atau diberikan oleh sistem diubah dengan segera selepas pemasangan sistem, perkakasan atau perisian.	Pengguna, Pentadbir ICT
7.5.17.2	**Penggunaan Maklumat Pengesahan Rahsia** Peranan dan tanggungjawab pengguna ialah seperti yang berikut: (a) Membaca, memahami dan mematuhi DKS. (b) Mengetahui dan memahami implikasi keselamatan siber kesan dari tindakannya. (c) Melaksanakan prinsip-prinsip dan menjaga kerahsiaan maklumat UTeM.	Pengguna, UTeM-CSIRT, Pentadbir ICT

ID	KETERANGAN	PERANAN
	(d) Melaksanakan langkah-langkah perlindungan seperti yang berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan. ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa. iii. Menentukan maklumat sedia untuk digunakan. iv. Menjaga kerahsiaan kata laluan. v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan. vi. Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan. vii. Menjaga kerahsiaan langkah- langkah keselamatan siber daripada diketahui umum. viii. Maklumat pengesahan terjejas atau telah dikompromi hendaklah diubah apabila pemberitahuan atau petunjuk sebarang kompromi diterima. ix. Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada UTeM-CSIRT dengan segera. x. Menghadiri program-program kesedaran mengenai keselamatan siber. (e) Pengguna perlu mengikut amalan keselamatan yang baik dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi	

ID	KETERANGAN	PERANAN
	maklumat yang digunakan untuk pengesahan identiti pengguna.	

7.5.18 HAK CAPAIAN

ID	KETERANGAN	PERANAN
7.5.18.1	**Peruntukan Capaian Pengguna** Hak capaian kepada data, maklumat dan aset maklumat yang berkaitan hendaklah diperuntukkan, disemak, diubah suai dan dikeluarkan mengikut dasar/peraturan atau garis panduan kawalan capaian yang berkuat kuasa. Pentadbir ICT perlu mewujudkan prosedur pendaftaran dan penamatan pengguna sistem masing-masing. Proses peruntukan capaian pengguna dan pembatalan hak capaian fizikal dan logik yang diberikan kepada entiti yang telah disahkan identitinya hendaklah termasuk: (a) Hak capaian yang berkaitan dengan setiap sistem atau produk yang perlu diberikan hendaklah dikenal pasti dan dibenarkan. (b) Hak capaian maklumat dan aset maklumat mesti dihadkan berdasarkan keperluan untuk	Pentadbir ICT, pengguna

ID	KETERANGAN	PERANAN
	mengetahui dan prinsip-prinsip keselamatan yang ditetapkan. (c) Pihak luar TIDAK boleh diberikan ID pengguna atau diberi keistimewaan untuk menggunakan atau mencapai aset (komputer, maklumat atau sistem komunikasi) melainkan setelah mendapat kebenaran Pejabat CDO. (d) Kebenaran rasmi hendaklah ditandatangani oleh wakil yang diberi kuasa sebelum capaian diberikan kepada mana-mana pihak luar. (e) Hak capaian hendaklah ditamatkan apabila entiti/individu tidak lagi perlu mencapai maklumat dan aset maklumat yang berkaitan. (f) Hak capaian sementara untuk tempoh masa terhad boleh dipertimbangkan bila diperlukan dan hendaklah dibatalkan pada tarikh tamat tempoh. (g) Tahap capaian yang diberikan hendaklah mengikut dasar kawalan capaian yang ditetapkan, peranan dan konsisten dengan keperluan keselamatan maklumat lain seperti pengasingan tugas. (h) Hak capaian pengguna hendaklah diubah suai selari dengan peranan atau pekerjaan. (i) Hak capaian diaktifkan hanya selepas kebenaran diperoleh.	
7.5.18.2	**Kajian Semula Hak Capaian Pengguna** Pentadbir Akses hendaklah menyemak hak capaian pengguna secara berkala sekurang- kurangnya sekali	Pentadbir Akses, Pentadbir ICT, Pemilik Sistem

ID	KETERANGAN	PERANAN
	dalam tempoh setahun. Pentadbir ICT perlu mewujudkan rekod pendaftaran dan penamatan pengguna sistem masing-masing sebagai rujukan semakan ke atas hak capaian pengguna secara berkala. Semakan ke atas hak capaian harus mempertimbangkan perkara berikut: (a) Hak capaian pengguna selepas sebarang perubahan dalam organisasi (contohnya pertukaran pekerjaan, kenaikan pangkat, penurunan pangkat). (b) Kebenaran untuk hak capaian istimewa.	
7.5.18.3	**Tanggungjawab Pengguna** Memastikan pengguna sistem atau aset maklumat bertanggungjawab melindungi maklumat pengesahan identiti mereka.	Pengguna

7.5.19 KESELAMATAN MAKLUMAT DALAM HUBUNGAN DENGAN PEMBEKAL

ID	KETERANGAN	PERANAN
7.5.19.1	**Dasar Keselamatan Siber untuk Hubungan dengan pihak luar**	Pemilik Projek, Pengurus Projek, pengguna,

ID	KETERANGAN	PERANAN
	Keperluan keselamatan maklumat hendaklah ditakrifkan, dilaksanakan, dipersetujui dan didokumentasikan dengan pihak luar bagi mengurangkan risiko kepada aset maklumat. Perkara yang perlu dipertimbangkan ialah seperti yang berikut: (a) Mengenal pasti dan mendokumentasi maklumat pihak luar. (b) Menyediakan prosedur pengurusan pihak luar termasuk kaedah penilaian mutu perkhidmatan. (c) Memilih pihak luar mengikut klasifikasi maklumat dan perkhidmatan yang disediakan oleh pihak luar selaras dengan dasar dan peraturan yang berkuat kuasa. (d) Mengawal dan memantau capaian pihak luar. (e) Keperluan minimum keselamatan maklumat bagi setiap pihak luar dinyatakan dalam dokumen perjanjian. (f) Jenis-jenis obligasi kepada pihak luar. (g) Pelan kontigensi (*contingency plan*) bagi memastikan ketersediaan kemudahan pemprosesan maklumat. (h) Melaksanakan program kesedaran terhadap DKS kepada pihak luar. (i) Menandatangani Surat Akuan Pembida Berjaya dan Surat Setuju Terima. (j) Membuat akuan pematuhan DKS UTeM.	ICTSO

ID	KETERANGAN	PERANAN
	(k) Pihak luar perlu mematuhi arahan keselamatan yang sedang berkuat kuasa. (l) Mengenal pasti dan melaksanakan proses dan prosedur bagi mengurus risiko yang berkaitan dengan penggunaan produk dan perkhidmatan pihak luar termasuk penamatan penggunaan produk dan perkhidmatan pihak luar. Pemilik projek hendaklah memastikan proses penamatan pihak luar yang selamat, termasuk: (a) Membatalkan peruntukan hak capaian. (b) Pengendalian maklumat. (c) Menentukan pemilikan harta intelek yang dibangunkan semasa penjanjian dilaksanakan. (d) Mudah alih maklumat sekiranya berlaku pertukaran pembekal atau penyumberan. (e) Pengurusan rekod. (f) Pemulangan aset.	

7.5.20 MENANGANI KESELAMATAN DALAM PERJANJIAN DENGAN PEMBEKAL

ID	KETERANGAN	PERANAN
7.5.20.1	**Menangani Keselamatan Maklumat Dalam Perjanjian Pihak luar** Semua keperluan keselamatan maklumat yang berkaitan hendaklah ditakrifkan, disediakan dan	Pengurus Projek, pihak luar, Pengurus ICT

ID	KETERANGAN	PERANAN
	dipersetujui dengan setiap pembekal yang boleh mencapai, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur ICT untuk maklumat organisasi. Pihak luar hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak UTeM selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa. Sekiranya syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak UTeM mempunyai kuasa untuk menghalang syarikat pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Pihak luar hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mencapai, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan UTeM sebagaimana Perjanjian Kerahsiaan (NDA) dan Borang Akuan Pematuhan. (b) Pihak luar hendaklah mematuhi pengelasan maklumat yang telah ditetapkan oleh UTeM.	

7.5.21 MENGURUS KESELAMATAN MAKLUMAT DALAM RANGKAIAN BEKALAN ICT

ID	KETERANGAN	PERANAN
7.5.21.1	**Rantaian Bekalan Teknologi Maklumat dan Komunikasi** Perjanjian dengan pihak luar hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk. Perkara-perkara yang perlu diambil kira ialah seperti yang berikut: (a) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan. (b) Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan atau pembekalan produk. (c) Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	Pengurus Projek, pihak luar, Pengurus ICT

7.5.22 MEMANTAU, MENYEMAK DAN MENGURUS PERUBAHAN PERKHIDMATAN PEMBEKAL

ID	KETERANGAN	PERANAN
7.5.22.1	**Memantau dan Mengkaji Semula Perkhidmatan Pihak Luar** UTeM hendaklah sentiasa memantau dan mengkaji semula perkhidmatan pihak luar dan mengurus perubahan dalam amalan risiko keselamatan maklumat pembekal dan penyampaian perkhidmatan. Perkara-perkara yang perlu diambil kira ialah seperti yang berikut: (a) Memantau tahap prestasi perkhidmatan untuk mengesahkan pihak luar mematuhi perjanjian perkhidmatan. (b) Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pihak luar dan mengemukakan status kemajuan. (c) Memaklumkan mengenai insiden keselamatan kepada pihak luar /pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.	Pengurus Projek
7.5.22.2	**Menguruskan Perubahan Kepada Perkhidmatan Pihak Luar (*Managing Changes to Supplier Services*)** Perubahan kepada peruntukan perkhidmatan oleh pihak luar, termasuk mempertahan dan menambah	Pengurus Projek, Pemilik Projek

ID	KETERANGAN	PERANAN
	baik dasar keselamatan maklumat sedia ada, prosedur dan kawalan, hendaklah diurus dengan mengambil kira kepentingan maklumat, sistem dan perkhidmatan yang terlibat dan penilaian semula risiko. Perkara yang perlu diambil kira ialah seperti yang berikut: (a) Perubahan dalam perjanjian dengan pihak luar. (b) Perubahan yang dilakukan oleh UTeM bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur. (c) Perubahan dalam perkhidmatan pihak luar selaras dengan perubahan rangkaian, teknologi baru, produk-produk baru, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.	

7.5.23 KESELAMATAN MAKLUMAT BAGI PENGGUNAAN PERKHIDMATAN PENGKOMPUTERAN AWAN

ID	KETERANGAN	PERANAN
7.5.23.1	**Keselamatan maklumat bagi penggunaan perkhidmatan pengkomputeran awan** Pengurusan perkhidmatan awan ini melibatkan pelbagai aspek teknikal dan pentadbiran untuk memastikan perkhidmatan awan digunakan secara	Pentadbir ICT, Pengurus ICT

ID	KETERANGAN	PERANAN
	berkesan, selamat, dan sesuai dengan keperluan organisasi. Perkara berikut perlu dipatuhi oleh semua pihak yang terlibat: (a) Memastikan kepatuhan terhadap keperluan perundangan, peraturan, garis panduan dan perjanjian kontrak yang berkaitan antaranya: (i) PK 2.6: Perolehan Perkhidmatan Pengkomputeran Awan (Cloud) Sektor Awam. (ii) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2021 Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam. (iii) Surat Pekeliling Am Bilangan 2 Tahun 2021 Garis Panduan Pengurusan Keselamatan Maklumat melalui Pengkomputeran Awan dalam Perkhidmatan Awam dan tertakluk kepada arahan-arahan yang dikeluarkan oleh Kerajaan dari semasa ke semasa (b) Pengurusan perkhidmatan yang disediakan oleh pihak luar yang dilantik oleh UTeM. (c) Memastikan keperluan keselamatan maklumat yang berkaitan dengan penggunaan perkhidmatan pengkomputeran awan dilaksanakan. (d) Melaksanakan kawalan terhadap keperluan perlesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.	

7.5.24 PERANCANGAN DAN PENYEDIAAN PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
7.5.24.1	**Tanggungjawab dan Prosedur** Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat dengan mentakrif, mewujudkan dan menyampaikan proses pengurusan insiden keselamatan maklumat, peranan dan tanggungjawab. Pengurusan insiden UTeM ialah berdasarkan prosedur pengurusan pengendalian insiden keselamatan maklumat yang sedang berkuat kuasa. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Melaksanakan program kesedaran mengenai prosedur pengendalian insiden keselamatan dan hebahan kepada pengguna. (b) Memastikan staf yang mengurus insiden mempunyai tahap kompetensi yang diperlukan.	UTeM-CSIRT, ICTSO
7.5.24.2	**Perancangan dan Penyediaan Pengurusan Insiden Keselamatan Maklumat** Memastikan pendekatan yang konsisten dan berkesan dalam pengurusan insiden keselamatan maklumat, termasuk komunikasi tentang kejadian dan kerentanan kelemahan keselamatan.	UTeM-CSIRT, ICTSO

7.5.25 PENILAIAN DAN KEPUTUSAN MENGENAI KEJADIAN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
7.5.25.1	**Penilaian dan Keputusan Mengenai Peristiwa Keselamatan Data dan Maklumat** Insiden keselamatan data dan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat berdasarkan pekeliling dan prosedur pengurusan insiden keselamatan data dan maklumat yang sedang berkuat kuasa.	UTeM-CSIRT, ICTSO

7.5.26 TINDAK BALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
7.5.26.1	**Tindak Balas Terhadap Insiden Keselamatan** Insiden keselamatan data dan maklumat hendaklah dikendalikan menurut prosedur yang didokumenkan. Tindak balas yang dirancang dan yang diambil perlu direkodkan.	UTeM-CSIRT, ICTSO

7.5.27 PENGAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
7.5.27.1	**Pembelajaran Daripada Insiden Keselamatan Maklumat** Setiap insiden keselamatan data dan maklumat direkodkan dan dinilai untuk memastikan kawalan dan tindakan yang diambil adalah mencukupi atau perlu ditambah.	UTeM-CSIRT, ICTSO, JKICT

7.5.28 PENGUMPULAN BAHAN BUKTI

ID	KETERANGAN	PERANAN
7.5.28.1	**Pengumpulan Bahan** UTeM hendaklah mengenal pasti maklumat atau rekod, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti dengan merujuk kepada arahan semasa yang berkaitan.	UTeM-CSIRT, Pemilik Sistem, Pentadbir ICT, Pengurus ICT

7.5.29 KESELAMATAN MAKLUMAT SEMASA GANGGUAN

ID	KETERANGAN	PERANAN
7.5.29.1	**Keselamatan Maklumat Semasa Gangguan**	CDO, ICTSO, UTeM-CSIRT

ID	KETERANGAN	PERANAN
	Keselamatan data dan maklumat semasa gangguan merujuk kepada langkah-langkah dan prosedur yang diambil untuk melindungi dan mengekalkan keselamatan maklumat, data, dan sistem ICT semasa terjadi gangguan, bencana atau insiden yang boleh mengancam integriti dan ketersediaan maklumat. Gangguan ini termasuk pelbagai situasi seperti serangan siber, bencana alam, kebakaran, banjir, kecurian, atau insiden teknikal yang tidak diingini. Aspek penting berkaitan dengan keselamatan maklumat semasa gangguan yang perlu diberi perhatian ialah seperti yang berikut: a) Pembangunan dan pelaksanaan Pelan Pemulihan Bencana ICT (*ICT Disaster Recovery Plan*) untuk memastikan penyampaian perkhidmatan ICT UTeM berfungsi dengan minimum gangguan ketika terjadi insiden. b) Pemulihan Bencana ICT melibatkan pelan dan tindakan untuk memulihkan sistem maklumat dan data setelah bencana atau insiden. c) Perlindungan data melibatkan salinan data secara berkala, pengekalan data yang baik, dan pelaksanaan tindakan keselamatan yang sesuai untuk melindungi data terperingkat. d) Pencegahan Serangan Siber (*Cybersecurity Measures*) melibatkan tindakan untuk mencegah serangan siber dan melindungi data dari pada ancaman siber.	

ID	KETERANGAN	PERANAN
	e) Kawalan fizikal ke pusat data dan peralatan komputer terhad kepada individu yang sah untuk mencegah capaian yang tidak dibenarkan. f) Pemulihan data memastikan keupayaan untuk memulihkan data yang hilang atau terjejas dalam insiden. g) Kesedaran keselamatan (*Security Awareness*) untuk mengurangkan ancaman dalaman dan mencegah insiden yang disebabkan oleh kesalahan manusia. Keselamatan data dan maklumat semasa gangguan ialah aspek penting dalam perancangan keselamatan dan keselamatan data, yang memastikan organisasi mampu menjaga integriti, kerahsiaan, dan ketersediaan data dan maklumat penting dalam pelbagai situasi yang mengancam.	

7.5.30 KESEDIAAN ICT BAGI KESINAMBUNGAN PERKHIDMATAN

ID	KETERANGAN	PERANAN
7.5.30.1	**Kesinambungan Keselamatan Maklumat** Kesinambungan keselamatan maklumat hendaklah diterapkan dalam pengurusan kesinambungan perkhidmatan.	ICTSO

ID	KETERANGAN	PERANAN
7.5.30.2	**Perancangan, Pelaksanaan dan Penilaian Kesinambungan Keselamatan Maklumat** Pelan Pemulihan Bencana ICT hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JKICT UTeM dan perkara-perkara berikut perlu diberi perhatian: (a) Mengenalpasti semua tanggungjawab dan prosedur kecemasan atau pemulihan. (b) Mengenalpasti peristiwa yang boleh mengakibatkan gangguan terhadap operasi UTeM bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT. (c) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan. (d) Mendokumentasikan proses dan prosedur yang telah dipersetujui. (e) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan. (f) Membuat penduaan.	Jawatankuasa Pemulihan Bencana

ID	KETERANGAN	PERANAN
	(g) Menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali. Pelan Pemulihan Bencana ini perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: (a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan. (b) Senarai staf UTeM dan pihak luar berserta nombor yang boleh dihubungi (telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan staf yang tidak dapat hadir untuk menangani insiden; (c) Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan. (d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh. (e) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh. Salinan Pelan Pemulihan Bencana ICT perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan ini hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi operasi UTeM untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah	

ID	KETERANGAN	PERANAN
	dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian Pelan Pemulihan Bencana ICT hendaklah dijadualkan untuk memastikan semua ahli dalam jawatankuasa pemulihan dan staf yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. UTeM hendaklah memastikan salinan Pelan Pemulihan Bencana ICT sentiasa dikemaskini dan dilindungi seperti di lokasi utama.	

7.5.31 KEPERLUAN PERUNDANGAN DAN KONTRAK

ID	KETERANGAN	PERANAN
7.5.31.1	**Pematuhan Terhadap Keperluan Perundangan dan Kontrak** Meningkat dan memantapkan tahap keselamatan siber bagi mengelakkan pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.	Pengguna

ID	KETERANGAN	PERANAN
7.5.31.2	**Pengenalpastian Keperluan Undang- Undang dan Kontrak Yang Terpakai** Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh pengguna yang terlibat dalam pembekalan perkhidmatan ICT di UTeM. Keperluan perundangan yang perlu dipatuhi mengikut undang-undang yang sedang berkuatkuasa dari semasa ke semasa.	Pemilik Projek, Pengurus Projek, pengguna
7.5.31.3	**Peraturan Kawalan Kriptografi** Penggunaan kriptografi hendaklah mematuhi keperluan perundangan, dasar dan pekeliling yang sedang berkuatkuasa dari semasa ke semasa.	Pengurus ICT, Pentadbir ICT

7.5.32 HAK HARTA INTELEK

ID	KETERANGAN	PERANAN
7.5.32.1	**Hak Harta Intelek** Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual. Semua pihak yang terlibat hendaklah melaksanakan kawalan terhadap keperluan perlesenan supaya	Pengguna, Pemilik Sistem, Pengurus ICT, Pentadbir ICT

ID	KETERANGAN	PERANAN
	menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.	

7.5.33 PERLINDUNGAN REKOD

ID	KETERANGAN	PERANAN
7.5.33.1	**Perlindungan Rekod** Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, capaian tanpa izin dan capaian ke atas orang yang tidak berkenaan.	pengguna, Pemilik Sistem, Pengurus ICT, Pentadbir ICT

7.5.34 PRIVASI DAN PERLINDUNGAN MAKLUMAT PERIBADI

ID	KETERANGAN	PERANAN
7.5.34.1	**Privasi dan Perlindungan Maklumat Peribadi** Maklumat peribadi merujuk kepada sebarang data yang boleh digunakan untuk mengenal pasti individu seperti nombor kad pengenalan, rekod perubatan dan lain-lain. Jika terdapat sebarang keperluan terhadap pengenalan tersebut hendaklah terlebih dahulu mendapat persetujuan daripada individu berkenaan.	pengguna

7.5.35 KAJIAN SEMULA KESELAMATAN MAKLUMAT SECARA BERKECUALI

ID	KETERANGAN	PERANAN
7.5.35.1	**Kajian Semula Keselamatan Maklumat Secara Berkecuali** Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.	Pemilik Sistem

7.5.36 PEMATUHAN DASAR, PERATURAN DAN PIAWAIAN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
7.5.36.1	**Pematuhan Dasar dan Standard Keselamatan** Kajian semula secara berkala terhadap pematuhan dasar dan standard keselamatan pemprosesan maklumat dan prosedur di kawasan yang dipertanggungjawabkan dengan polisi, piawaian dan keperluan teknikal yang bersesuaian.	CDO, ICTSO
7.5.36.2	**Kajian Semula Pematuhan Teknikal** Kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung dalam polisi, piawaian dan keperluan komputer.	CDO, ICTSO

7.5.37 DOKUMENTASI PROSEDUR OPERASI STANDARD

ID	KETERANGAN	PERANAN
7.5.37.1	**Dokumentasi Prosedur Operasi Standard** Semua prosedur operasi hendaklah didokumenkan dan disediakan kepada pihak yang melaksanakan operasi serta mematuhi perkara yang berikut: (a) Semua prosedur keselamatan siber yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal. (b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti. (c) Semua prosedur hendaklah disemak dan dikemas kini dari semasa ke semasa atau mengikut keperluan.	Pentadbir ICT, Pengurus ICT

7.6 KAWALAN SUMBER MANUSIA

Terdapat 8 kawalan sumber manusia yang terpakai dalam perlu dipatuhi oleh semua pihak yang terlibat dalam pengurusan data dan maklumat di UTeM. Perincian kawalan sumber manusia seperti di bawah.

7.6.1 TAPISAN KESELAMATAN

ID	KETERANGAN	PERANAN
7.6.1.1	Tapisan keselamatan hendaklah dijalankan terhadap pengguna yang mempunyai urusan dengan perkhidmatan ICT UTeM yang terlibat selaras dengan keperluan perkhidmatan. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pengguna yang terlibat dalam menjamin keselamatan aset maklumat sebelum, semasa dan selepas perkhidmatan. (b) Menjalankan tapisan keselamatan untuk pengguna yang mempunyai urusan dengan perkhidmatan ICT PTj yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	pengguna

7.6.2 TERMA DAN SYARAT PERKHIDMATAN

ID	KETERANGAN	PERANAN
7.6.2.1	**Terma dan Syarat Perkhidmatan** Persetujuan berkontrak dengan pengguna yang mempunyai urusan dengan perkhidmatan ICT di UTeM hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi ialah seperti yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan serta tanggung jawab pengguna yang mempunyai urusan dengan perkhidmatan ICT PTj yang terlibat dalam menjamin keselamatan aset ICT. (b) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	pengguna, dan Pengurus Projek

7.6.3 KESEDARAN, PENDIDIKAN DAN LATIHAN TENTANG KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
7.6.3.1	**Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat** Pengguna hendaklah diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai DKS, sistem pengurusan keselamatan maklumat dan latihan teknikal yang berkaitan dengan keselamatan. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Memastikan kesedaran, pendidikan dan latihan diberikan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. (b) Memastikan kesedaran berkaitan DKS perlu diberi dari masa ke semasa. (c) Memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat.	Pengguna dan ICTSO

7.6.4 PROSES TATATERTIB

ID	KETERANGAN	PERANAN
7.6.4.1	**Proses Tatatertib** Proses tatatertib yang formal perlu ditentukan dan disampaikan kepada pengguna atau pihak berkepentingan terlibat yang lain bagi membolehkan tindakan diambil ke atas pelanggaran keselamatan maklumat yang dilakukan. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Memastikan adanya proses tindakan disiplin dan/ atau undang-undang sekiranya berlaku pelanggaran terhadap polisi, perundangan dan peraturan yang ditetapkan oleh UTeM atau Kerajaan. (b) Tindakan tatatertib atau tindakan yang sewajarnya akan dikenakan bagi sebarang pelanggaran kepada dasar ini.	Unit Integriti

7.6.5 TANGGUNGJAWAB SELEPAS PENAMATAN PERANAN ATAU JAWATAN

ID	KETERANGAN	PERANAN
7.6.5.1	**Pertukaran atau Penamatan Peranan atau Jawatan** Semua pengguna perlu mematuhi perkara-perkara berikut: (a) Memastikan semua aset maklumat milik UTeM dikembalikan kepada UTeM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan. (b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan. (c) Maklumat rasmi dalam aset maklumat tidak dibenarkan dibawa keluar dari UTeM.	pengguna

7.6.6 PERJANJIAN KERAHSIAAN ATAU KETAKDEDAHAN

ID	KETERANGAN	PERANAN
7.6.6.1	**Perjanjian Kerahsian** Syarat-syarat perjanjian kerahsiaan (non-disclosure agreement) perlu mengambil kira keperluan organisasi dan hendaklah dikenal pasti dan didokumentasi dan ditandatangani oleh pengguna. Pihak luar yang terlibat dengan perkhidmatan ICT UTeM hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan.	pengguna

7.6.7 BEKERJA SECARA JARAK JAUH

ID	KETERANGAN	PERANAN
7.6.7.1	**Bekerja Secara Jarak Jauh** Dasar dan langkah-langkah keselamatan hendaklah dilaksanakan bagi melindungi maklumat yang dicapai, diproses atau disimpan secara jarak jauh. Pengguna yang bekerja jarak jauh hendaklah:	pengguna

ID	KETERANGAN	PERANAN
	(a) Memastikan keselamatan maklumat UTeM dipatuhi dan tidak disebarkan kepada pihak luar. (b) Memastikan arahan bekerja dari luar dipatuhi mengikut garis panduan yang ditetapkan.	

7.6.8 PELAPORAN INSIDEN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
7.6.8.1	**Pelaporan Insiden Keselamatan Maklumat** Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat berdasarkan pekeliling atau prosedur pengendalian insiden yang berkuat kuasa, Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Menentukan mekanisme untuk melaporkan sebarang insiden melalui saluran dan dalam tempoh masa yang ditentukan. (b) Memberi kesedaran berkaitan prosedur pengendalian insiden dan hebahan	Pemilik Sistem dan UTeM-CSIRT

ID	KETERANGAN	PERANAN
	kepada pengguna sekiranya terdapat perubahan. (c) Memastikan pengguna yang mengurus insiden mempunyai kompetensi yang diperlukan. (d) Insiden keselamatan ICT atau ancaman yang berlaku hendaklah dilaporkan kepada UTeM-CSIRT berdasarkan prosedur pengendalian insiden yang berkuat kuasa	

7.7 KAWALAN FIZIKAL

Terdapat 14 kawalan fizikal yang terpakai dalam perlu dipatuhi oleh semua pihak yang terlibat dalam pengurusan data dan maklumat di UTeM. Perincian kawalan fizikal seperti di bawah.

7.7.1 PERIMETER KESELAMATAN FIZIKAL

ID	KETERANGAN	PERANAN
7.7.1.1	**Perimeter Keselamatan Fizikal** Kawalan bertujuan untuk menghalang capaian tanpa kebenaran, gangguan secara fizikal dan kerosakan terhadap kampus dan aset maklumat UTeM. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: Perimeter keselamatan fizikal digunakan untuk melindungi aset, individu, dan persekitaran fizikal daripada ancaman, bahaya, atau kemungkinan kerosakan. Pelaksanaan kawalan ini melibatkan pelbagai strategi dan tindakan untuk memastikan keselamatan dalam ruang fizikal seperti bangunan, infrastruktur, atau kawasan penting yang berkaitan dengan perimeter keselamatan fizikal: a) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan	Pentadbir ICT, Pengurus ICT, Pejabat Keselamatan UTeM dan PPF

ID	KETERANGAN	PERANAN
	maklumat. b) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan staf yang diberi kebenaran sahaja boleh malalui pintu masuk ini. c) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan. d) Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana alam atau perbuatan manusia. e) Melaksanakan perlindungan fizikal untuk staf yang bekerja di dalam kawasan terhad. f) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya. g) Memasang alat penggera atau kamera keselamatan.	

7.7.2 KEMASUKAN FIZIKAL

ID	KETERANGAN	PERANAN
7.7.2.1	**Kawalan Kemasukan Fizikal** Kawalan kemasukan fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke kampus UTeM. Perkara yang perlu dipatuhi ialah seperti yang berikut: a) Setiap staf dan pelajar hendaklah mempamerkan kad staf atau kad matrik pelajar sekiranya diperlukan. b) Pihak luar hendaklah mendaftar dan mendapatkan pas keselamatan pelawat di kaunter keselamatan dan hendaklah dikembalikan selepas tamat lawatan. c) Kehilangan kad staf/kad matrik pelajar/pas pelawat hendaklah dilaporkan segera kepada Pejabat Keselamatan UTeM. d) Hanya pengguna yang diberi kebenaran sahaja boleh menggunakan aset maklumat UTeM.	Pengguna
7.7.2.2	**Kawasan Larangan** UTeM hendaklah memastikan kawasan larangan dan juga tempat-tempat lain dikawal daripada dimasuki oleh pihak yang tidak diberi kebenaran.	Pejabat Keselamatan UTeM dan Pengguna

7.7.3 KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN

ID	KETERANGAN	PERANAN
7.7.3.1	**Keselamatan Pejabat, Bilik dan Kemudahan** Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Kawasan tempat bekerja, bilik fail, bilik cetakan, bilik kawalan kamera litar tertutup (CCTV) dan pusat data perlu dihadkan daripada dicapai tanpa kebenaran. (b) Kawasan tempat bekerja, bilik dan tempat operasi ICT perlu dihadkan daripada dicapai oleh pihak luar. (c) Petunjuk lokasi bilik operasi dan tempat larangan hendaklah mematuhi arahan keselamatan.	Pengurus ICT, Pejabat Keselamatan UTeM dan Pengguna

7.7.4 PEMANTAUAN KESELAMATAN FIZIKAL

ID	KETERANGAN	PERANAN
7.7.4.1	**Pemantauan keselamatan fizikal** Kampus fizikal hendaklah dipantau oleh sistem pengawasan termasuk pengawal, dan sistem pemantauan video seperti CCTV. Sistem pemantauan hendaklah dilindungi daripada capaian yang tidak dibenarkan untuk mengelakkan maklumat pengawasan, seperti suapan video, daripada dicapai oleh orang yang tidak dibenarkan atau sistem diceroboh secara jarak jauh. Melaksanakan pemantauan secara berterusan di kampus bagi mengelakkan capaian secara fizikal yang tidak dibenarkan. Capaian kepada bangunan yang menempatkan sistem kritikal hendaklah dipantau secara berterusan untuk mengesan capaian yang tidak dibenarkan atau tingkah laku yang mencurigakan dengan memasang sistem pemantauan video seperti CCTV untuk melihat dan merakam capaian di kampus UTeM.	Pengurus ICT, Pejabat Keselamatan UTeM dan Pengguna.

7.7.5 PERLINDUNGAN DARIPADA ANCAMAN FIZIKAL DAN PERSEKITARAN

ID	KETERANGAN	PERANAN
7.7.5.1	**Perlindungan Daripada Ancaman Fizikal dan Persekitaran** Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirangka dan dilaksanakan. Pelan Pemulihan Bencana ICT perlu disediakan bagi melindungi aset ICT di UTeM.	Pejabat CDO

7.7.6 BEKERJA DI KAWASAN SELAMAT

ID	KETERANGAN	PERANAN
7.7.6.1	**Bekerja di Kawasan Selamat** Langkah-langkah kawalan keselamatan bekerja di kawasan selamat hendaklah dirangka dan dilaksanakan. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pihak yang dibenarkan sahaja. Kawalan ini dilakukan untuk melindungi aset maklumat yang terdapat dalam kampus UTeM termasuklah pusat data. Kawasan ini hendaklah dilindungi daripada sebarang ancaman, kelemahan dan risiko	ICTSO, Pengurus ICT, Pejabat Keselamatan UTeM.

ID	KETERANGAN	PERANAN
	seperti pencerobohan, kebakaran dan bencana alam. Langkah-langkah kawalan keselamatan ke atas kawasan tersebut ialah seperti yang berikut: (a) Sumber data atau server, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik server atau bilik khas yang mempunyai ciri-ciri keselamatan seperti sistem pencegahan kebakaran. (b) Capaian adalah terhad kepada pihak yang telah diberi kuasa sahaja dan dipantau pada setiap masa. (c) Pemantauan dibuat menggunakan CCTV atau lain-lain peralatan yang sesuai. (d) Peralatan keselamatan (CCTV, log capaian) perlu diperiksa secara berjadual. (e) Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan. (f) Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan. (g) Memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan. (h) Memperkukuh dinding dan siling. (i) Menghadkan jalan keluar masuk.	

7.7.7 KAWALAN MEJA KOSONG DAN SKRIN KOSONG

ID	KETERANGAN	PERANAN
7.7.7.1	**Kawalan meja kosong dan skrin kosong** Kawalan meja kosong dan skrin kosong bermaksud tidak meninggalkan dan mendedahkan maklumat terperingkat sama ada atas meja pengguna, pada paparan skrin komputer, mesin pencetak, mesin faksimili atau mesin pengimbas apabila pengguna tidak berada di tempatnya. Objektif utama kawalan ini adalah untuk memastikan data dan maklumat terjamin keselamatannya dan tidak didedahkan kepada pihak yang tidak mempunyai hak capaian ke atas data atau maklumat tersebut. Kawalan ini merangkumi aspek-aspek berikut: (a) Penggunaan fungsi kata laluan penyelamat skrin (screen saver password) atau log keluar apabila meninggalkan komputer. (b) Penyimpanan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci. (c) Semua dokumen hendaklah diambil segera daripada pencetak, pengimbas, mesin faksimili dan mesin fotostat. (d) Pengawalan e-mel masuk dan keluar. (e) Memadamkan maklumat sensitif atau	Pengguna

ID	KETERANGAN	PERANAN
	kritikal pada papan putih dan jenis paparan lain apabila tidak diperlukan lagi.	
7.7.7.2	**Peralatan Pengguna Tanpa Kawalan** Pengguna hendaklah memastikan kelengkapan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya. Pengguna hendaklah memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara yang berikut: (a) Tamatkan sesi aktif apabila selesai tugas. (b) Log keluar komputer meja, komputer riba dan server apabila sesi bertugas selesai. (c) Komputer, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan.	Pengguna

7.7.8 PENEMPATAN DAN PERLINDUNGAN PERALATAN ICT

ID	KETERANGAN	PERANAN
7.7.8.1	**Penempatan dan Perlindungan Peralatan ICT** Peralatan ICT hendaklah ditentukan tempatnya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran dan	Pengguna, Pengurus ICT dan Pegawai Aset

ID	KETERANGAN	PERANAN
	peluang kemasukan yang tidak dibenarkan. Langkah-langkah keselamatan yang perlu diambil ialah seperti yang berikut: (a) Capaian ke sistem komputer menggunakan kata laluan. (b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan. (c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan. (d) Pengguna dilarang membuat instalasi sebarang perisian tambahan yang tidak sah dan boleh mengancam keselamatan. (e) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (activated) dan dikemaskini disamping melakukan imbasan ke atas media storan yang digunakan. (f) Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubah suai tanpa kebenaran dan salah guna. (g) Setiap pengguna adalah bertanggungjawab atas kerosakan dan	

ID	KETERANGAN	PERANAN
	kehilangan perkakasan ICT di bawah kawalannya. (h) Peralatan-peralatan kritikal perlu disokong oleh Uninterruptable Power Supply (UPS) dan Generator Set (Gen-Set). (i) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. (j) Peralatan rangkaian seperti suis, penghala dan peralatan-peralatan lain perlu diletakkan di dalam rak khas dan berkunci. (k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (air ventilation) yang sesuai. (l) Pengendalian Peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa. (m) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal komputer tersebut ditempatkan tanpa kebenaran Pegawai Aset. (n) Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal tanpa kebenaran Pengurus ICT.	

ID	KETERANGAN	PERANAN
	(o) Pengguna dilarang sama sekali mengubah kata laluan pentadbir yang telah ditetapkan oleh Pengurus ICT. (p) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat dibawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi kerajaan dan UTeM sahaja.	

7.7.9 KESELAMATAN ASET DI LUAR PREMIS

ID	KETERANGAN	PERANAN
7.7.9.1	**Keselamatan Aset di Luar Premis** Keselamatan aset di luar kampus hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar kampus UTeM. Peralatan yang dibawa keluar dari kampus UTeM adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Peralatan perlu dilindungi dan dikawal sepanjang masa. (b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian. (c) Keselamatan peralatan yang dibawa keluar adalah bertanggungjawab pegawai yang berkenaan.	Pengguna

7.7.10 MEDIA STORAN

ID	KETERANGAN	PERANAN
7.7.10.1	**Pengurusan Media Boleh Alih** Untuk mengelakkan kerosakan pada aset maklumat dan gangguan kepada aktiviti perkhidmatan, media boleh alih harus dikawal dan dilindungi secara fizikal. (a) Melabelkan semua media mengikut tahap sensitiviti sesuatu data dan maklumat. (b) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja. (c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja. (d) Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan. (e) Menyimpan semua jenis media di tempat yang selamat.	Pengguna
7.7.10.2	**Pelupusan Media** Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan di dalam PKPU yang berkuatkuasa dari semasa ke semasa.	Pegawai Aset

ID	KETERANGAN	PERANAN
	Media yang mengandungi maklumat terperingkat hendaklah dikelaskan semula oleh Pegawai Pengelas terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.	
7.7.10.3	**Pengalihan Aset** Kelengkapan, maklumat atau perisian tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran UTeM terlebih dahulu. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut: (a) Peralatan ICT yang hendak dibawa keluar dari kampus UTeM untuk tujuan rasmi, perlulah mengikut peraturan yang sedang berkuatkuasa. (b) Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan.	Pegawai Aset
7.7.10.4	**Pengendalian Media** Melindungi aset maklumat daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	Pengguna, Pegawai Aset

7.7.11 UTILITI SOKONGAN

ID	KETERANGAN	PERANAN
7.7.11.1	**Utiliti Sokongan** Aset maklumat hendaklah dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. Semua alat sokongan bagi aset maklumat perlu diselenggara mengikut keperluan.	PPF dan Pengurus ICT

7.7.12 KESELAMATAN KABEL

ID	KETERANGAN	PERANAN
7.7.12.1	**Keselamatan Kabel** Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan. Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah-langkah keselamatan yang perlu diambil ialah seperti yang berikut:	PPF dan Pengurus ICT

ID	KETERANGAN	PERANAN
	(a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan. (b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan. (c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan pemintasan maklumat pada kabel. (d) Semua kabel hendaklah dilabelkan dengan jelas dan mestilah melalui sesalur kabel bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.	

7.7.13 PENYELENGGARAAN PERALATAN

ID	KETERANGAN	PERANAN
7.7.13.1	Peralatan ICT hendaklah diselenggara dengan betul bagi memastikan ketersediaan dan keutuhannya berterusan. Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut: (a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan.	Pengurus ICT

ID	KETERANGAN	PERANAN
	(b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan. (c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan pemintasan maklumat pada kabel. (d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui sesalur kabel bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.	

7.7.14 PELUPUSAN YANG SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN

ID	KETERANGAN	PERANAN
7.7.14.1	**Pelupusan yang Selamat atau Penggunaan Semula Peralatan** Semua peralatan yang mengandungi media penyimpanan hendaklah dipastikan bahawa data yang sensitif dan perisian berlesen telah dikeluarkan atau berjaya ditulis ganti (overwrite) sebelum dilupuskan atau diguna semula. Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh UTeM dan	Pengurus ICT, Pentadbir ICT, Pegawai Aset

ID	KETERANGAN	PERANAN
	ditempatkan di UTeM. Peralatan aset maklumat yang hendak dilupuskan perlu mematuhi prosedur pelupusan yang berkuat kuasa. Langkah-langkah seperti yang berikut hendaklah diambil: (a) Bagi peralatan ICT yang akan dilupuskan sebelum dipindah milik, data-data dalam storan hendaklah dipastikan telah dihapuskan dengan cara yang selamat. (b) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya. (c) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang bersesuaian bagi menjamin keselamatan peralatan tersebut. (d) Pelupusan aset maklumat hendaklah dilakukan mengikut tatacara pelupusan semasa yang berkuat kuasa. (e) Pengguna **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti yang berikut tanpa kebenaran UTeM: (i) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. (ii) Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, hardisk, motherboard dan sebagainya.	

ID	KETERANGAN	PERANAN
	(iii) Menyimpan dan memindahkan perkakasan luaran komputer seperti pembesar suara dan mana-mana peralatan yang berkaitan. (iv) Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan. (v) Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan dibawah tanggungjawab jabatan. (f) Pengguna bertanggungjawab memastikan segala maklumat terperingkat disalin pada media storan pendua sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan bagi tujuan sandaran maklumat. (g) Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal. Sekiranya maklumat perlu disimpan, maka pengguna boleh membuat salinan. (h) Pegawai Aset bertanggungjawab merekod butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem pengurusan aset.	

7.8 KAWALAN TEKNOLOGI

Terdapat 34 kawalan teknologi yang utama dan perlu dipatuhi oleh semua pihak yang terlibat dalam pengurusan data dan maklumat di UTeM. Perincian kawalan teknologi seperti di bawah.

7.8.1 PERIMETER KESELAMATAN FIZIKAL (PHYSICAL SECURITY PARAMETER)

ID	KETERANGAN	PERANAN
7.8.1.1	**Peranti Mudah Alih** Langkah-langkah keselamatan sokongan hendaklah digunakan bagi mengurus risiko yang timbul melalui penggunaan peranti mudah alih. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk melindungi daripada risiko penggunaan peralatan mudah alih dan kemudahan komunikasi. (b) Komputer mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	ICTSO, Pengguna

7.8.2 HAK CAPAIAN ISTIMEWA

ID	KETERANGAN	PERANAN
7.8.2.1	**Pengurusan Hak Capaian Istimewa** Peruntukan dan penggunaan hak capaian istimewa hendaklah dihadkan dan dikawal. Penetapan dan penggunaan ke atas hak capaian perlu diberikan kawalan dan penyeliaan yang ketat mengikut keperluan skop tugas yang telah dikenal pasti.	Pentadbir ICT, Pengurus ICT

7.8.3 SEKATAN CAPAIAN MAKLUMAT

ID	KETERANGAN	PERANAN
7.8.3.1	**Sekatan Capaian Maklumat** Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: (a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan.	Pentadbir ICT, Pemilik Sistem

ID	KETERANGAN	PERANAN
	(b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkod (log) bagi mengesan aktiviti-aktiviti yang tidak diingini. (c) Setiap aktiviti capaian kepada sistem dan aplikasi yang berisiko tinggi hendaklah dihadkan kepada pengguna yang sah sahaja. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat. (d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah. (e) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah dibenarkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	

7.8.4 KAWALAN CAPAIAN KEPADA KOD SUMBER

ID	KETERANGAN	PERANAN
7.8.4.1	**Kawalan Capaian Kepada Kod Sumber** Kawalan kod sumber (source code) dan dokumentasi sistem aplikasi hendaklah dilaksanakan ke atas sistem yang baharu dibangunkan secara outsource dan in-house.	Pentadbir ICT, Pengurus Projek, Pengguna

ID	KETERANGAN	PERANAN
	Ini bagi memastikan kesinambungan sistem aplikasi itu dapat berjalan dengan lancar sama ada selepas pertukaran pegawai atau penyerahan sistem kepada pemilik sistem aplikasi. Kod sumber sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	

7.8.5 PENGESAHAN IDENTITI YANG SELAMAT

ID	KETERANGAN	PERANAN
7.8.5.1	**Prosedur Log Masuk yang Selamat** Kawalan terhadap capaian aplikasi sistem perlu mempunyai kaedah pengesahan log masuk yang selamat dan bersesuaian bagi mengelakkan sebarang capaian yang tidak dibenarkan. Langkah dan kaedah kawalan yang digunakan ialah seperti yang berikut: (a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan Jabatan. (b) Menjana amaran (alert) sekiranya berlaku perlanggaran semasa proses log masuk terhadap aplikasi sistem. (c) Mengawal capaian ke atas aplikasi	Pentadbir ICT, Pemilik Sistem

ID	KETERANGAN	PERANAN
	sistem mengikut prosedur yang ditetapkan. (d) Mewujudkan teknik pengesahan pelbagai faktor (multi factor authentication, MFA) berdasarkan pengkelasan maklumat yang bersesuaian bagi mengesahkan pengenalan diri pengguna. (e) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan yang kukuh dan berkualiti. (f) Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.	
7.8.5.2	**Sistem Pengurusan Kata Laluan** Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh UTeM seperti berikut: (a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun. (b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi. (c) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan	Pengguna

ID	KETERANGAN	PERANAN
	gabungan antara huruf besar, huruf kecil, simbol dan nombor. (d) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun. (e) Kata laluan windows hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang gunasama. (f) Kata laluan hendaklah TIDAK dipaparkan semasa input, dalam laporan atau media lain. (g) Kuatkuasakan pertukaran kata laluan semasa log in kali pertama atau selepas log in kali pertama atau selepas kata laluan diset semula. (h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; (i) Had kemasukan katalaluan bagi capaian kepada sistem aplikasi adalah maksimum tiga (3) kali sahaja. (j) Setelah mencapai tahap maksimum, capaian kepada sistem akan dibekukan. Kemasukan kata laluan seterusnya hanya boleh dibuat selepas bagi tempoh masa selama 3 minit atau setelah diset semula oleh Helpdesk.	

7.8.6 PENGURUSAN KAPASITI

ID	KETERANGAN	PERANAN
7.8.6.1	**Pengurusan Kapasiti** Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi sistem yang dikehendaki dicapai. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa kana datang. (b) Kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang. (c) Mempertimbangkan penggunaan pengkomputeran awan bagi pengurusan kapasiti yang berkesan, anjal (*elasticity*) dan boleh skala (*scalability*).	Pemilik Sistem, Pentadbir ICT, Pengurus ICT

7.8.7 PERLINDUNGAN DARIPADA PERISIAN HASAD

ID	KETERANGAN	PERANAN
7.8.7.1	**Perlindungan daripada Perisian Hasad** Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan daripada serangan perisian hasad hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut. Perkara yang perlu dilaksanakan bagi memastikan perlindungan aset maklumat daripada perisian hasad ialah seperti yang berikut: (a) Memasang sistem keselamatan untuk mengesan perisian atau program perisian hasad seperti antivirus, Intrusion Detection System (IDS), Intrusion Prevention System (IPS) dan Web Application Firewall (WAF). (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang yang sedang berkuat kuasa. (c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya. (d) Mengemas kini antivirus dengan signature/pattern antivirus yang terkini.	Pemilik Sistem, Pentadbir ICT, Pengurus ICT

ID	KETERANGAN	PERANAN
	(e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat. (f) Menghadiri program kesedaran mengenai ancaman perisian hasad dan cara mengendalikannya. (g) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya. (h) Menyediakan pelan kesinambungan perkhidmatan yang sesuai untuk pulih daripada serangan perisian hasad. (i) Menentukan prosedur dan tanggungjawab untuk menangani perlindungan terhadap perisian hasad pada sistem. (j) Mengesahkan ketepatan sumber maklumat yang berkaitan dengan perisian hasad.	

7.8.8 PENGURUSAN KERENTANAN TEKNIKAL

ID	KETERANGAN	PERANAN
7.8.8.1	**Pengurusan Kerentanan Teknikal** Maklumat berkaitan kerentanan teknikal sistem maklumat yang digunakan hendaklah diperoleh, pendedahan organisasi terhadap kerentanan tersebut hendaklah dinilai dan langkah-langkah yang sesuai hendaklah diambil untuk menangani risiko yang berkaitan. Kawalan teknikal kerentanan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memperoleh maklumat teknikal kerentanan (vulnerability) yang terkini ke atas sistem maklumat yang digunakan. (b) Menilai tahap teknikal kerentanan (vulnerability) bagi mengenal pasti tahap risiko yang bakal dihadapi. (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pemilik Sistem, Pentadbir ICT, Pengurus ICT

7.8.9 PENGURUSAN KONFIGURASI

ID	KETERANGAN	PERANAN
7.8.9.1	**Pengurusan konfigurasi** Pengurusan konfigurasi perlu dilaksanakan untuk memastikan perkakasan, perisian, perkhidmatan dan rangkaian berfungsi dengan betul berserta dengan keperluan keselamatan. Konfigurasi tidak diubah tanpa kebenaran. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Melindungi capaian terhadap fail konfigurasi mengikut kawalan yang ditetapkan. (b) Merekod dan menyimpan sebarang perubahan konfigurasi dengan selamat. (c) Memantau konfigurasi untuk mengesahkan tetapan konfigurasi dan menilai kawalan keselamatan.	Pentadbir ICT, Pengurus ICT

7.8.10 PENGHAPUSAN MAKLUMAT

ID	KETERANGAN	PERANAN
7.8.10	**Penghapusan Maklumat** Maklumat yang disimpan di dalam sistem, peralatan dan mana-mana storan media perlu dihapuskan apabila tidak diperlukan mengikut tatacara yang berkuatkuasa dari semasa ke semasa.	Pemilik Sistem, Pegawai Aset, Pemilik Aset

7.8.11 PENYEMBUNYIAN DATA (*DATA MASKING*)

ID	KETERANGAN	PERANAN
7.8.11.1	**Penyembunyian data** Penyembunyian data dilaksanakan bagi melindungi data sensitif seperti *data* Personal Identifiable Information (PII), dan data terperingkat dengan mengambil kira keperluan perkhidmatan dan kawalan capaian serta peraturan lain yang berkuatkuasa. Penyembunyian data diperlukan bagi melindungi data PII dan data sensitif daripada terdedah atau bocor kepada pihak yang tidak bertanggungjawab yang akan menyebabkan imej UTeM terjejas. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Mengenal pasti klasifikasi data yang perlu dikongsi dengan pihak luar. (b) Mengenal pasti teknik yang sesuai selaras dengan sensitiviti data. Memastikan pengguna hanya dapat mencapai data yang minimum yang dibenarkan sahaja	Pemilik Sistem, Pentadbir ICT

7.8.12 PENCEGAHAN KETIRISAN DATA

ID	KETERANGAN	PERANAN
7.8.12.1	**Pencegahan ketirisan Data** Data dalam sistem, rangkaian dan peralatan lain perlu dilindungi daripada pendedahan dan pengekstrakan data yang tidak sah oleh individu atau sistem. Perkara yang perlu dipatuhi ialah seperti berikut: (a) Mengenal pasti dan mengelaskan maklumat untuk dilindungi daripada ketirisan. (b) Memantau saluran transaksi dan perkongsian data (contohnya e-mel, pemindahan fail, perkhidmatan peranti atau media mudah alih). (c) Melaksanakan tindakan pengukuhan untuk mengelakkan ketirisan maklumat.	Pemilik Sistem, Pentadbir ICT

7.8.13 SANDARAN MAKLUMAT (*INFORMATION BACKUP*)

ID	KETERANGAN	PERANAN
7.8.13.1	**Sandaran Maklumat** Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara berkala mengikut prosedur sandaran yang	Pentadbir ICT

ID	KETERANGAN	PERANAN
	dipersetujui. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, sandaran hendaklah dilakukan setiap kali konfigurasi berubah. Sandaran hendaklah direkodkan dan disimpan. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Membuat sandaran keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru. (b) Membuat sandaran ke atas semua data dan maklumat mengikut keperluan operasi. (c) Menguji sistem sandaran sedia ada secara berkala sekurang-kurangnya setahun sekali bagi memastikannya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana. (d) Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara harian, mingguan, bulanan atau tahunan. Kekerapan sandaran bergantung pada tahap kritikal maklumat, dan hendaklah disimpan dengan selamat.	

7.8.14 LEWAHAN BAGI KEMUDAHAN PEMPROSESAN MAKLUMAT

ID	KETERANGAN	PERANAN
7.8.14.1	**Lewahan bagi Kemudahan Pemprosesan Maklumat** Mempunyai sistem atau sumber sandaran untuk memastikan kesinambungan operasi. Ia melibatkan penduaan komponen kritikal atau keseluruhan sistem untuk mengurangkan risiko kegagalan akibat kerosakan perkakasan, ralat perisian atau isu lain yang tidak dijangka. Ia perlu diuji keberkesanannya dari semasa ke semasa.	Pentadbir ICT, Pengurus ICT, Pemilik Sistem

7.8.15 PENGELOGAN MAKLUMAT

ID	KETERANGAN	PERANAN
7.8.15.1	**Menyediakan Log** Sistem yang dibangunkan perlu merekod aktiviti dan menjana bahan bukti untuk memastikan maklumat log adalah berintegriti dan boleh digunakan sebagai bahan bukti jika berlaku insiden keselamatan maklumat. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna. (b) Menyemak log secara berkala bagi	Pentadbir ICT, Pengurus ICT

ID	KETERANGAN	PERANAN
	mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan baik pulih dengan segera. (c) Melaporkan kepada ICTSO sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan	
7.8.15.2	Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: (a) Rekod setiap aktiviti transaksi. (b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan. (c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya. (d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. (e) Pentadbir ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini	Pentadbir ICT

ID	KETERANGAN	PERANAN
	akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. (f) Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan	
7.8.15.3	**Perlindungan Maklumat Log** Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada perubahan dan capaian tanpa izin merangkumi perkara berikut: (a) Pengguna, termasuk yang mempunyai hak capaian istimewa, tidak diberi kebenaran untuk memadam atau menyahaktifkan log aktiviti mereka sendiri. (b) Kemudahan pengelogan beroperasi dengan baik.	Pentadbir ICT
7.8.15.4	**Analisis Log** Analisis log perlu merangkumi analisis dan interpretasi aktiviti keselamatan maklumat untuk mengenal pasti aktiviti yang luar biasa atau tingkah laku yang janggal yang menunjukkan indikator sistem terjejas. Perkara yang perlu dipatuhi ialah seperti yang berikut:	Pentadbir ICT, UTeM-CSIRT

ID	KETERANGAN	PERANAN
	(a) Memantau penggunaan kemudahan memproses maklumat secara berkala. (b) Log Audit yang merekodkan semua aktiviti perlu diwujudkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian. (c) Aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir ICT hendaklah melaporkan aktiviti tersebut kepada UTeM – CSIRT.	

7.8.16 AKTIVITI PEMANTAUAN

ID	KETERANGAN	PERANAN
7.8.16.1	**Aktiviti Pemantauan** Rangkaian, sistem dan aplikasi harus dipantau dan tindakan sewajarnya diambil untuk menilai kemungkinan insiden keselamatan maklumat. Pentadbir ICT perlu memantau untuk mengesan tingkah laku tidak normal (anomali) dan kemungkinan berlaku insiden keselamatan maklumat. Aktiviti pemantauan perlu merangkumi perkara seperti yang berikut:	Pentadbir ICT, Pengurus ICT

ID	KETERANGAN	PERANAN
	(a) Trafik keluar (outbound) dan masuk (inbound) bagi rangkaian, sistem dan aplikasi. (b) Capaian kepada sistem, pelayan, peralatan rangkaian, sistem pemantauan, aplikasi kritikal. (c) Log daripada peralatan keselamatan (contohnya antivirus, IDS, sistem pencegahan pencerobohan (IPS), penapis web, firewall, pencegahan kebocoran data). (d) Log peristiwa yang berkaitan dengan sistem dan aktiviti rangkaian; (e) Memastikan supaya kod sumber yang dilaksanakan telah diberi kebenaran untuk dilaksanakan dan tidak diubah tanpa kebenaran. (f) Penggunaan dan prestasi sumber.	

7.8.17 PENYEGERAKAN JAM (*CLOCK SYNCHRONIZATION*)

ID	KETERANGAN	PERANAN
7.8.17.1	**Penyegerakan Jam** Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut waktu	Pengurus ICT

ID	KETERANGAN	PERANAN
	piawai Malaysia. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam jabatan atau domain keselamatan perlu diseragamkan dengan waktu piawai Malaysia yang ditetapkan.	

7.8.18 PENGGUNAAN PROGRAM UTILITI YANG MEMPUNYAI HAK ISTIMEWA (*USE OF PRIVILEGED UTILITY PROGRAMS*)

ID	KETERANGAN	PERANAN
7.8.18.1	**Penggunaan Program Utiliti yang Mempunyai Hak Istimewa** Penggunaan program utiliti yang berkemungkinan mengakibatkan keperluan *overriding* pada kawalan sistem dan aplikasi perlu dihadkan dan dikawal.	Pengurus ICT

7.18.9 PEMASANGAN PERISIAN PADA SISTEM OPERASI

ID	KETERANGAN	PERANAN
7.8.19.1	**Pemasangan Perisian pada Sistem yang Beroperasi**	Pentadbir ICT, Pengurus ICT

ID	KETERANGAN	PERANAN
	Kawalan pemasangan perisian pada sistem operasi hendaklah dilaksanakan. Langh-langkah yang perlu dipatuhi setelah mendapat kelulusan ICTSO adalah seperti berikut: (a) Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian dilaksanakan dan diperaku berjaya. (b) Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur. (c) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan UTeM. (d) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT. (e) Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada CD-rom, disk atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak.	
7.8.19.2	**Sekatan ke atas Pemasangan Perisian** Kawalan pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan. Perkara yang perlu dipatuhi ialah seperti yang berikut:	Pengguna, Pentadbir ICT, Pegawai Aset

ID	KETERANGAN	PERANAN
	(a) Hanya perisian yang diperaku sahaja dibenarkan bagi kegunaan pengguna yang mempunyai urusan dengan perkhidmatan ICT UTeM. (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuatkuasa. (c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya. (d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pejabat CDO.	

7.8.20 KESELAMATAN RANGKAIAN

ID	KETERANGAN	PERANAN
7.8.20.1	**Kawalan Rangkaian** Infrastruktur rangkaian hendaklah dikawal dan diuruskan sebaik mungkin daripada sebarang ancaman untuk melindungi ancaman kepada sistem dan aplikasi dalam rangkaian. Perkara yang perlu dipatuhi ialah seperti yang berikut:	Pengurus ICT

ID	KETERANGAN	PERANAN
	(a) Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan. (b) Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas daripada risiko. (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja. (d) Tembok keselamatan (firewall) hendaklah dipasang, dikonfigurasi dan diselia oleh Pengurus ICT. (e) Semua trafik keluar dan masuk rangkaian hendaklah melalui tembok keselamatan (firewall) di bawah kawalan Pejabat CDO. (f) Semua perisian untuk menganalisis atau menawan paket rangkaian dilarang dipasang pada komputer pengguna KECUALI mendapat kebenaran UTeM. (g) Memasang perisian IPS bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam data dan maklumat universiti. (h) Sebarang penyambungan rangkaian yang bukan di bawah kawalan UTeM tidak dibenarkan. (i) Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di	

ID	KETERANGAN	PERANAN
	UTeM sahaja dan penggunaan peralatan lain seperti modem adalah dilarang sama sekali kecuali setelah mendapat kebenaran Pejabat CDO. (j) Kemudahan bagi rangkaian tanpa wayar UTeM hendaklah dipantau dan dikawal penggunaannya. (k) Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi Service Level Assurance (SLA) yang telah ditetapkan. (l) Menempatkan atau memasang antara muka (interfaces) yang bersesuaian. (m) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya. (n) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja. (o) Mengawal capaian fizikal dan logikal ke atas kemudahan port diagnostik dan konfigurasi jarak jauh. (p) Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan. (q) Mewujud dan melaksana kawalan pengalihan laluan (routing control) bagi memastikan pematuhan terhadap	

ID	KETERANGAN	PERANAN
	peraturan UTeM. Semua peralatan yang hendak disambung kepada rangkaian perlu bebas daripada virus dan mempunyai antivirus yang sah. (r) Capaian kepada rangkaian perlu dilaksanakan mengikut kategori yang telah ditetapkan iaitu Intranet, Internet dan Demilitarized Zone (DMZ). (s) Pihak luar tidak dibenarkan untuk mencapai rangkaian Intranet kecuali untuk kerja-kerja pembangunan atau penyelenggaraan sistem dengan kebenaran UTeM. (t) Capaian kepada rangkaian tanpa wayar hendaklah dikawal mengikut kategori pengguna.	

7.8.21 KESELAMATAN PERKHIDMATAN RANGKAIAN

ID	KETERANGAN	PERANAN
7.8.21.1	**Keselamatan Perkhidmatan Rangkaian** Pengurusan bagi semua perkhidmatan rangkaian dalaman dan sumber luar yang merangkumi mekanisme keselamatan dan tahap serta keperluan perkhidmatan rangkaian hendaklah dikenal pasti dan dimasukkan dalam perjanjian perkhidmatan	Pengurus ICT

7.8.22 PENGASINGAN RANGKAIAN

ID	KETERANGAN	PERANAN
7.8.22.1	**Pengasingan dalam Rangkaian** Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian di UTeM.	Pengurus ICT

7.8.23 PENAPISAN WEB

ID	KETERANGAN	PERANAN
7.8.23.1	**Penapisan Web** Kawalan penapisan web dalam bentuk perisian atau sebagainya perlu dilaksanakan bagi mengesan dan menyekat ke laman web yang dianggap tidak selamat dan tidak sesuai. Ini bagi melindungi sistem maklumat daripada sebarang ancaman keselamatan laman web luaran. UTeM hendaklah mengurangkan risiko mencapai laman web yang mengandungi maklumat yang dilarang atau diketahui mengandungi virus atau data pancingan (*phishing*) data oleh pengguna.	Pengurus ICT, Pentadbir ICT

ID	KETERANGAN	PERANAN
	UTeM hendaklah mengenal pasti jenis laman web yang patut atau tidak boleh dicapai oleh pengguna. UTeM hendaklah mempertimbangkan untuk menyekat capaian kepada jenis laman web yang berikut: (a) Laman web yang mempunyai fungsi muat naik maklumat melainkan dibenarkan atas sebab perkhidmatan yang sah. (b) Tapak web yang diketahui atau disyaki berniat jahat. (c) Pelayan arahan dan kawalan (command and control). (d) Laman web berniat jahat yang diperoleh daripada risiko ancaman. (e) Laman web yang berkongsi kandungan haram.	

7.8.24 PENGGUNAAN KRIPTOGRAFI

ID	KETERANGAN	PERANAN
7.8.24.1	**Polisi Penggunaan Kawalan Kriptografi** Kriptografi merangkumi kaedah-kaedah seperti yang berikut: (a) Penyulitan Data (Enkripsi): Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat penyulitan	Pengurus ICT

ID	KETERANGAN	PERANAN
	semasa dalam simpanan atau semasa sedang dipindahkan. (b) Tandatangan Digital: Tandatangan digital boleh digunakan bagi memastikan maklumat digital tulen dan mempunyai integriti serta tidak boleh disangkal.	
7.8.24.2	**Pengurusan Infrastruktur Kunci Awam** Pengurusan ke atas Pengurusan Infrastruktur Kunci Awam (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah sijil digital tersebut.	Pengurus ICT

7.8.25 KITAR HAYAT PEMBANGUNAN SISTEM YANG SELAMAT

ID	KETERANGAN	PERANAN
7.8.25.1	**Pembangunan Sistem yang Selamat** "Garis Panduan Membangun dan Menyelenggara Sistem Maklumat di Universiti Teknikal Malaysia Melaka" digunakan untuk pembangunan dan penyelenggaraan sistem. Perkara yang perlu dipertimbangkan ialah seperti yang	Pembangun Sistem, Pentadbir ICT

ID	KETERANGAN	PERANAN
	berikut: (a) Keselamatan persekitaran pembangunan. (b) Keselamatan pangkalan data. (c) Keperluan keselamatan dalam fasa reka bentuk. (d) Keperluan pengujian dalam carta perbatuan projek. (e) Keperluan pengetahuan ke atas keselamatan aplikasi. (f) Keselamatan dalam kawalan versi. (g) Bagi pembangunan menggunakan sumber luar (outsource), pembekal yang dilantik berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem.	
7.8.25.2	**Kitar Hayat Pembangunan Sistem yang Selamat** Pembangun Sistem hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem. Pembangun Sistem perlu melaksanakan penilaian risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira: (a) Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem.	Pembangun Sistem, Pentadbir ICT

ID	KETERANGAN	PERANAN
	(b) Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran. (c) Keperluan dan pengasingan di antara pelbagai persekitaran pembangunan sistem. (d) Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem. (e) Pegawai yang bekerja di dalam persekitaran pembangunan sistem ialah yang boleh dipercayai. (f) Kawalan ke atas capaian kepada persekitaran pembangunan sistem.	

7.8.26 KEPERLUAN KESELAMATAN APLIKASI

ID	KETERANGAN	PERANAN
7.8.26.1	**Melindungi Perkhidmatan Aplikasi dalam Rangkaian Awam** Perkara yang perlu dipertimbangkan ialah seperti yang berikut: (a) Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala.Perkhidmatan sumber luaran adalah perkhidmatan yang disediakan	Pentadbir ICT

ID	KETERANGAN	PERANAN
	oleh organisasi luar untuk menyokong operasi jabatan, Contoh perkhidmatan sumber luaran ialah: (i) Perisian Sebagai Satu Perkhidmatan. (ii) Platform Sebagai Satu Perkhidmatan. (iii) Infrastruktur Sebagai Satu Perkhidmatan. (iv) Storan Pengkomputeran Awan. (v) Pemantauan Keselamatan (b) Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan identiti. (c) Memastikan pihak luar dimaklumkan mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT. (d) Memastikan pihak luar memahami keperluan kerahsiaan dan integriti.	
7.8.26.2	**Melindungi Transaksi Perkhidmatan Aplikasi** Maklumat yang terlibat dalam urusan perkhidmatan aplikasi hendaklah dilindungi bagi mengelakkan penghantaran tidak sempurna, salah destinasi, pindaan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan, penduaan atau ulang tayang mesej yang tidak dibenarkan. Perkara	Pentadbir ICT, Pemilik Sistem

ID	KETERANGAN	PERANAN
	yang perlu dipertimbangkan adalah seperti yang berikut: (a) Penggunaan tandatangan digital oleh setiap pihak yang terlibat dalam transaksi; (b) Memastikan semua aspek transaksi dipatuhi: (i) Maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan. (ii) Mengekalkan kerahsiaan maklumat. (iii) Mengekalkan privasi pihak yang terlibat. (iv) Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi. (v) Pihak yang mengeluarkan tandatangan digital ialah yang dilantik oleh Kerajaan.	
7.8.26.3	**Keselamatan Aplikasi** Spesifikasi reka bentuk perlu mengandungi keperluan keselamatan sistem maklumat. Sekiranya sesuatu produk perisian aplikasi tersedia (*off-the-shelf*) diperoleh, pembekal perlu dimaklumkan berkenaan keperluan keselamatan.	Pentadbir ICT, Pemilik Sistem

7.8.27 PRINSIP REKA BENTUK DAN KEJURUTERAAN SISTEM YANG SELAMAT

ID	KETERANGAN	PERANAN
7.8.27.1	**Prinsip Kejuruteraan Sistem Yang Selamat** Kawalan perubahan kepada perisian perlu dilaksanakan bagi mengurangkan risiko kerosakan pada perisian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Proses pengemaskinian perisian atau sistem hanya boleh dilakukan oleh Pentadbir ICT atau pegawai yang diberi tanggungjawab dan mengikut prosedur yang telah ditetapkan. (b) Kod atau atur cara sistem yang telah dikemas kini hanya boleh digunakan selepas diuji. (c) Mengawal capaian ke atas kod atau cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian. (d) Data ujian perlu dipilih dangan berhati-hati, dilindungi dan dikawal. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pentadbir ICT, Pembangun Sistem

7.8.28 PENGATURCARAAN PROGRAM SELAMAT

ID	KETERANGAN	PERANAN
7.8.28.1	**Kawalan capaian kepada kod sumber** Kawalan capaian kepada kod sumber atau atur cara program perlu dilaksanakan bagi mengelakkan kecurian, pengubahsuaian dan penghapusan tanpa kebenaran. Kod sumber bagi semua aplikasi dan perisian ialah hak milik UTeM.	Pentadbir ICT, Pembangun Sistem

7.8.29 PENGUJIAN DAN PENERIMAAN KESELAMATAN SISTEM

ID	KETERANGAN	PERANAN
7.8.29.1	**Pengujian Keselamatan Sistem** Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat. (b) Membuat semakan pengesahan dalam aplikasi untuk mengenal pasti kesilapan maklumat.	Pentadbir ICT, Penguji Sistem

ID	KETERANGAN	PERANAN
	(c) Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan. (d) Melakukan pengimbasan kelemahan untuk mengenal pasti konfigurasi yang tidak selamat dan kelemahan sistem. (e) Menjalankan ujian penembusan untuk mengenal pasti kod dan reka bentuk yang tidak selamat.	
7.8.29.2	**Pengujian Penerimaan Sistem** Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Pengujian penerimaan sistem hendaklah merangkumi keperluan keselamatan sistem maklumat dan kepatuhan kepada pembangunan sistem yang selamat. (b) Penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem diguna pakai	Pentadbir ICT, Penguji Sistem

7.8.30 PEMBANGUNAN SISTEM OLEH SUMBER LUAR

ID	KETERANGAN	PERANAN
7.8.30.1	**Pembangunan oleh Sumber Luar** UTeM hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan menggunakan sumber luar. Kod sumber yang dibangunkan ialah HAK MILIK UTeM. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Perjanjian lesen kod sumber ialah HAK MILIK UTeM. (b) Bagi semua perkhidmatan yang disediakan oleh sumber luar, *Software* as a Service (SaaS) yang mengendalikan maklumat terperingkat, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori Pembekal hendaklah membenar UTeM hak mencapai kod sumber dan melaksanakan pengolahan risiko. (c) Keperluan kontrak untuk reka bentuk selamat, pengekodan dan pengujian pembangunan sistem yang dijalankan oleh pihak luar mengikut amalan terbaik. (d) Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem. (e) Mematuhi keberkesanan kawalan dalam melaksanakan pengesahan pengujian;	Pentadbir ICT

ID	KETERANGAN	PERANAN
	(f) Penyediaan model ancaman (*threat modelling*) untuk dipertimbangkan oleh pembangun sistem serta memastikan tahap keselamatan minimum yang boleh diterima. (g) Keperluan keselamatan untuk persekitaran pembangunan.	

7.8.31 PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN PRODUKSI

ID	KETERANGAN	PERANAN
7.8.31.1	**Pengasingan Persekitaran** Persekitaran pembangunan, pengujian dan produksi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada persekitaran operasi. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Perkakasan dan perisian yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji sistem perlu diasingkan daripada perkakasan yang digunakan sebagai produksi.	Pentadbir ICT

ID	KETERANGAN	PERANAN
	(b) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian. (c) Kawalan keselamatan pada data yang mengandungi maklumat rahsia rasmi sekiranya digunakan di dalam persekitaran pembangunan. (d) Menguji perubahan yang dilaksanakan dalam persekitaran ujian. (e) Tidak menguji dalam persekitaran produksi kecuali dalam keadaan yang telah ditentukan dan diluluskan.	

7.8.32 PENGURUSAN PERUBAHAN

ID	KETERANGAN	PERANAN
7.8.32.1	**Pengurusan Perubahan** Perubahan dalam UTeM, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Penyedia dokumen perlu memastikan pengurusan perubahan yang didokumenkan mematuhi perkara-perkara seperti yang berikut: (a) Pengubahsuaian yang melibatkan perkakasan, sistem maklumat, perisian dan prosedur mestilah mendapat	Pentadbir ICT, Pengurus ICT,Pemilik Sistem, Pemilik Aset

ID	KETERANGAN	PERANAN
	kebenaran daripada Pejabat CDO terlebih dahulu. (b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan. (c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan. (d) Semua aktiviti perubahan atau pengubahsuaian hendaklah dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak sengaja.	
7.8.32.2	**Prosedur Kawalan Perubahan Sistem** Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan prosedur kawalan perubahan yang telah ditetapkan. Perubahan ke atas sistem hendaklah dikawal. Perkara yang perlu dipatuhi ialah seperti yang berikut:	Pentadbir ICT, Pengurus ICT

ID	KETERANGAN	PERANAN
	(a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai. (b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan UTeM. (c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan yang dibenarkan sahaja. (d) Capaian kepada kod sumber aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja.	
7.8.32.3	**Kajian Semula Keperluan Teknikal bagi Aplikasi Selepas Perubahan Platform Pengoperasian** Apabila platform pengoperasian berubah, aplikasi penting hendaklah dikaji semula dan diuji bagi memastikan tiada kesan buruk ke atas operasi atau keselamatan UTeM. Perkara yang perlu dipatuhi adalah seperti yang berikut:	Pentadbir ICT, Pemilik Sistem

ID	KETERANGAN	PERANAN
	(a) Pengujian ke atas sistem hendaklah dilaksanakan untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform. (b) Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan. (c) Memastikan maklumat perubahan tersebut dikemas kini dalam dokumen yang berkaitan.	
7.8.24	**Sekatan Ke atas Perubahan Dalam Pakej Perisian** Pengubahsuaian ke atas pakej perisian tidak digalakkan dan terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal.	Pentadbir ICT, Pengguna

7.8.33 DATA PENGUJIAN

ID	KETERANGAN	PERANAN
7.8.33.1	**Perlindungan Data Ujian** Untuk memastikan perlindungan ke atas maklumat yang digunakan untuk pengujian, data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Sebarang kawalan persekitaran sebenar hendaklah dilaksanakan dalam persekitaran pengujian. (b) Staf yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian.	Pentadbir ICT

7.8.34 PERLINDUNGAN SISTEM MAKLUMAT SEMASA PELAKSANAAN AUDIT

ID	KETERANGAN	PERANAN
7.8.34.1	**Kawalan Audit Sistem Maklumat** Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Pentadbir ICT