DOKUMEN INDUK

PENGURUSAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT) UNIVERSITI MALAYA

UNIVERSITI MALAYA

Nama Dokumen	:	Dokumen Induk Pengurusan Teknologi Maklumat dan Komunikasi (ICT) Universiti Malaya (UM)
Diluluskan Oleh	:	Lembaga Pengarah Universiti (LPU)
Tarikh Kuat Kuasa	:	31 Oktober 2025
Pemilik Dokumen	:	Jabatan Teknologi Maklumat
Versi	:	1.0

KAWALAN DOKUMEN

No. Versi	Tarikh	Ringkasan Pindaan
1.0	12 Jun 2025	Dokumen versi pertama selesai disediakan.

KANDUNGAN

SENARAI GAMBARAJAH

SENARAI JADUAL

1.0 PENGENALAN

Perkhidmatan Teknologi Maklumat dan Komunikasi (ICT) memainkan peranan penting dalam menyokong pengajaran, pembelajaran, penyelidikan dan pentadbiran yang merupakan fungsi utama Universiti Malaya (UM). Perkhidmatan ini merangkumi penyediaan infrastruktur digital, pembangunan dan penyelenggaraan sistem aplikasi, perlindungan keselamatan siber, serta penyampaian sokongan ICT kepada seluruh warga Universiti.

Dokumen Induk Pengurusan ICT Universiti Malaya dibangunkan sebagai rujukan utama yang menyelaras dan menyatukan keseluruhan kerangka tadbir urus ICT. Dokumen ini menggantikan pelbagai dasar, polisi, prosedur dan garis panduan terdahulu yang dibangunkan secara berasingan, bagi memastikan pendekatan pengurusan ICT yang lebih konsisten, menyeluruh dan bersepadu.

1.1 TUJUAN

Dokumen Induk Pengurusan ICT UM disediakan kepada warga Universiti bertujuan untuk:

(1) Menjadi dokumen rujukan utama ICT kepada semua pihak berkepentingan dalam mengurus perkhidmatan dan aset ICT Universiti secara sistematik.
(2) Memastikan tadbir urus ICT adalah selaras dengan keperluan perundangan, piawaian dan pekeliling ICT Universiti dan kerajaan yang berkuat kuasa.
(3) Meningkatkan kecekapan serta prestasi pengurusan ICT di semua peringkat Pusat Tanggungjawab (PTj) secara konsisten dan berkualiti selari dengan strategi dan hala tuju pendigitalan Universiti.

Dokumen ini turut memperincikan hala tuju serta komitmen Universiti terhadap pematuhan dasar, perundangan dan piawaian semasa yang berkaitan dengan ICT. Ini termasuk aspek keselamatan maklumat, tadbir urus digital, dan amalan terbaik sejajar dengan aspirasi transformasi digital negara.

1.2 SKOP

Dokumen Induk Pengurusan ICT UM merangkumi keseluruhan aspek pengurusan dan penyampaian perkhidmatan ICT di UM. Skop dokumen ini meliputi lima (5) komponen utama tadbir urus seperti berikut:

(1) Tadbir Urus Organisasi ICT
(2) Tadbir Urus Strategik ICT
(3) Tadbir Urus Projek ICT
(4) Tadbir Urus Polisi Keselamatan Siber
(5) Tadbir Urus Perkhidmatan ICT

1.3 PERANAN DAN TANGGUNGJAWAB

Dokumen Induk ini dikuatkuasakan oleh Naib Canselor dengan sokongan daripada Timbalan Naib Canselor (Pembangunan), Ketua Pegawai Digital (CDO), Pegawai Keselamatan ICT (ICTSO), Pengarah Eksekutif ICT, serta jabatan-jabatan di bawah seliaan.

Semua warga Universiti Malaya, termasuk staf dan pelajar, serta pihak berkepentingan yang terlibat dalam perkhidmatan ICT, bertanggungjawab untuk **MEMBACA, MEMAHAMI** dan **MEMATUHI** ketetapan yang dinyatakan dalam dokumen ini.

1.4 PENGURUSAN DAN PENYELENGGARAAN DOKUMEN INDUK

1.4.1 Pengurusan Dokumen Induk

Pelaksanaan pengurusan Dokumen Induk Pengurusan ICT UM adalah seperti berikut:

(1) Dokumen Induk Pengurusan ICT UM dikawal selia oleh Pengurusan ICT UM dan diuruskan oleh Jabatan Teknologi Maklumat (JTM).

(2) Dokumen ini hendaklah disemak sekurang-kurangnya setiap dua (2) tahun atau berdasarkan keperluan.

(3) Sebarang perubahan atau pindaan terhadap dokumen ini perlu mendapat kelulusan daripada pihak yang mempunyai kuasa melulus, tertakluk kepada had kuasa yang ditetapkan.

1.4.2 Penyebaran Dokumen Induk

Dokumen ini perlu disebarkan kepada semua pengguna dan pihak yang terlibat dengan perkhidmatan serta aset ICT Universiti, termasuk staf, pelajar dan pihak ketiga.

1.4.3 Penyelenggaraan Dokumen Induk

Perubahan dan pindaan melibatkan Dokumen Induk Pengurusan ICT UM, Sistem Pengurusan Kualiti (SPK) dan Sistem Pengurusan Keselamatan Maklumat (ISMS).

(1) Dokumen Induk Pengurusan ICT mengandungi polisi, prosedur dan garis panduan dalam aspek pengurusan dan penyampaian perkhidmatan ICT UM yang seragam dan bersepadu, selain menggariskan kawalan-kawalan keselamatan maklumat berasaskan piawaian dan amalan terbaik antarabangsa secara ringkas.

(2) SPK merangkumi semua proses teras atau aktiviti pengajaran dan pembelajaran pada peringkat ijazah dasar dan ijazah tinggi serta penyelidikan yang secara langsung terletak di bawah kelolaan atau bidang kuasa Naib Canselor UM. Dokumen UM02-PT04: Pengurusan Infrastruktur dan Perkhidmatan Maklumat merupakan salah satu proses teras di bawah SPK, di mana aspek pengurusan ICT merupakan salah satu komponen dalam dokumen tersebut. Dokumen boleh didapati di laman web Jabatan Pengurusan dan Penambahbaikan Kualiti (QMED) (https://qmec.um.edu.my).

(3) ISMS adalah sebuah kerangka kerja yang teratur dan sistematik bagi menilai risiko serta melaksanakan kawalan keselamatan maklumat Universiti, berasaskan prinsip kerahsiaan, integriti dan kebolehsediaan, selaras dengan piawaian ISO/IEC 27001. Dokumen ini mengandungi prosedur dan borang yang menyokong

pelaksanaan kawalan keselamatan siber UM. Dokumen boleh diakses melalui Portal Staf (https://portal.um.edu.my).

Senarai dokumen SPK dan ISMS adalah seperti di **Lampiran A**.

(4) Pelaksanaan penyelenggaraan Dokumen Induk, SPK dan ISMS adalah seperti berikut:

(a) Sebarang pembentukan dasar baharu yang ingin diguna pakai di UM hendaklah mendapat perakuan Jawatankuasa Pengurusan Universiti (JKPU) dan kelulusan Lembaga Pengarah Universiti (LPU).

(b) Perubahan dan pindaan Dokumen Induk Pengurusan ICT UM adalah tertakluk kepada peraturan, arahan dan pekeliling yang berkuat kuasa. Perubahan kandungan dokumen yang tidak mengubah maksud asal dasar adalah di bawah bidang kuasa dan kelulusan CDO.

(c) Setiap perubahan perlu direkodkan dengan pengemaskinian versi dan ringkasan pindaan dokumen.

(d) Pindaan dan pengubahsuaian dokumen kualiti di bawah SPK adalah melalui kelulusan QMED tertakluk kepada arahan kerja yang berkuat kuasa.

(e) Pindaan dan pengubahsuaian dokumen ICT di bawah ISMS adalah melalui kelulusan Pengarah Eksekutif JTM tertakluk kepada arahan yang berkuat kuasa.

Sekiranya berlaku sebarang percanggahan atau ketidakselarasan antara kandungan dalam Dokumen Induk Pengurusan ICT ini dengan mana-mana dokumen di bawah Sistem Pengurusan Kualiti (SPK) atau Sistem Pengurusan Keselamatan Maklumat (ISMS), maka peruntukan di dalam Dokumen Induk ini adalah terpakai dan mengatasi (*shall prevail*) dokumen-dokumen yang lain.

1.4.4 Pengecualian dan Akses Dokumen Induk

Dokumen ini terpakai kepada semua warga UM, pihak ketiga dan mana-mana pihak yang berurusan dengan perkhidmatan ICT UM. Tiada pengecualian diberikan terhadap pematuhan dokumen ini.

Namun begitu, akses kepada komponen tertentu dalam dokumen ini adalah tertakluk kepada peranan dan keperluan pengguna seperti berikut:

(1) Dasar dan garis panduan adalah terbuka untuk rujukan semua warga UM dan pihak ketiga.

(2) Dokumen kualiti di bawah SPK dan prosedur adalah terhad kepada pihak yang diberi kuasa dan/atau pengguna berdaftar sahaja.

1.5 DAFTAR KATA

1.5.1 Definisi

Pengurusan ICT UM	:	Struktur tadbir urus yang bertanggungjawab terhadap hal ehwal perancangan, pelaksanaan dan pemantauan berkaitan ICT di UM. Struktur ini merangkumi Lembaga Pengarah Universiti, Pengurusan Tertinggi Universiti, Ketua Pegawai Digital serta Jabatan Teknologi Maklumat selaku entiti pelaksana utama.
Staf	:	Individu lantikan UM sama ada berstatus tetap, pinjaman dan kontrak yang berkhidmat di dalam premis UM.
Pelajar	:	Individu yang sedang mengikuti program pengajian, kursus atau aktiviti akademik, sama ada sepenuh masa atau separuh masa, dan yang status pengajiannya masih aktif serta belum ditamatkan secara rasmi oleh UM.
Pihak Ketiga	:	Individu, organisasi atau entiti yang bukan sebahagian daripada struktur organisasi UM tetapi mempunyai hubungan rasmi melalui perjanjian, kontrak atau kerjasama untuk menyediakan perkhidmatan atau sokongan ICT kepada Universiti.

Pengguna	:	Pihak yang berinteraksi dengan atau menggunakan sistem, perkhidmatan, aplikasi, perisian atau perkakasan ICT bagi tujuan tertentu seperti mendapatkan maklumat, menjalankan tugasan, atau menggunakan kemudahan digital.
Pihak Berkuasa Melulus	:	Pihak yang mempunyai kuasa untuk meluluskan perkara tertentu berdasarkan had kuasa yang diberikan.
Pusat Tanggungjawab	:	Merujuk kepada tiga (3) entiti termasuk entiti akademik, bukan akademik dan penyelidikan. PTj Akademik merujuk kepada Fakulti/ Sekolah/ Pusat/ Akademi/ Institut. Manakala, PTj Bukan Akademik merujuk kepada Jabatan/ Pusat / Bahagian/ Seksyen. PTj Penyelidikan pula merujuk kepada termasuk tetapi tidak terhad kepada Pusat Kecemerlangan Pendidikan Tinggi (UMCoE/ HICoE), Kluster Penyelidikan dan Pusat Penyelidikan.
Sistem Pengurusan Keselamatan Maklumat	:	Kerangka kerja yang teratur dan sistematik bagi menilai risiko serta melaksanakan kawalan keselamatan maklumat Universiti, berasaskan prinsip kerahsiaan, integriti dan kebolehsediaan, selaras dengan piawaian ISO/IEC 27001.
Aset Maklumat	:	Sebarang data, sistem, peralatan, kemudahan, proses atau sumber yang mempunyai nilai kepada Universiti dan perlu dilindungi bagi menjamin kerahsiaan, integriti dan ketersediaannya.
Kerahsiaan	:	Merujuk kepada maklumat hendaklah dilindungi daripada pendedahan atau capaian tanpa kebenaran, dan hanya boleh diakses oleh pihak yang sah dan diberi kuasa.
Integriti	:	Merujuk kepada jaminan bahawa semua aset Universiti adalah lengkap, tepat, sahih, konsisten dan tidak diubah tanpa kebenaran sepanjang kitar hayatnya.
Ketersediaan	:	Merujuk kepada jaminan bahawa semua aset Universiti sentiasa boleh diakses serta digunakan oleh pihak yang diberi kuasa apabila diperlukan tanpa gangguan yang tidak sepatutnya.

Kawalan	:	Tindakan yang mungkin perlu untuk meminimumkan atau menghapuskan risiko daripada menjadi kenyataan dengan memindahkan atau mengurangkan tahap risiko.
Annex A, ISO/IEC 27001	:	Senarai kawalan keselamatan maklumat yang disusun mengikut kategori tertentu berperanan sebagai panduan kepada universiti tentang kawalan yang boleh dilaksanakan untuk mengurus risiko keselamatan maklumat.
Prinsip Kepercayaan Sifar	:	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 atau maklumat mesti melalui proses pengesahan yang teliti sebelum hak capaian diberikan.
Ancaman	:	Sebarang potensi kejadian, peristiwa atau tindakan yang boleh menyebabkan kemudaratan kepada aset maklumat, sistem, atau organisasi melalui pendedahan, pengubahsuaian, kehilangan, atau pemusnahan.
Risiko	:	Kesan ketidaktentuan terhadap pencapaian objektif, yang boleh memberi kesan negatif (ancaman) atau positif (peluang). Risiko biasanya diukur berdasarkan kebarangkalian (*likelihood*) sesuatu kejadian berlaku dan impak (*impact*) yang terhasil daripadanya.
Insiden Keselamatan Maklumat	:	Merujuk kepada sebarang kejadian yang berlaku atau disyaki berlaku yang boleh mengakibatkan pencerobohan, pendedahan tanpa kebenaran, pengubahsuaian, pemusnahan, atau kehilangan kerahsiaan, integriti dan ketersediaan maklumat atau sistem yang menguruskannya.
Kerentanan	:	Kelemahan dalam aset, sistem, proses atau kawalan keselamatan yang boleh dieksploitasi oleh ancaman, sekaligus menjejaskan kerahsiaan, integriti atau ketersediaan maklumat.
Kata Laluan	:	Kata laluan merupakan sejenis data gabungan sebilangan aksara yang digunakan oleh pengguna untuk tujuan pengenalan dan pengesahan diri ketika mengakses sesebuah

		rangkaian komputer/sumber untuk memperoleh/membaca maklumat yang diingini.
Media Elektronik	:	Sebarang peranti elektronik yang mempunyai keupayaan atau digunakan untuk merekod maklumat, termasuk, tetapi tidak terhad kepada PC, komputer riba, pelayan, storan awan, peralatan rangkaian, cakera keras, pita LTO dan storan boleh tanggal seperti pemacu USB.
Plugin	:	Komponen perisian tambahan yang dipasang pada sistem atau aplikasi utama bagi memperluas, menambah baik atau menyesuaikan fungsi tanpa mengubah struktur teras sistem tersebut.

1.5.2 Singkatan

ICT	:	Teknologi Maklumat dan Komunikasi (*Information and Communication Technology*)
UM	:	Universiti Malaya
PTj	:	Pusat Tanggungjawab
CDO	:	Ketua Pegawai Digital (*Chief Digital Officer*)
ICTSO	:	Pegawai Keselamatan ICT (*ICT Security Officer*)
JTM	:	Jabatan Teknologi Maklumat
SPK	:	Sistem Pengurusan Kualiti
ISMS	:	Sistem Pengurusan Keselamatan Maklumat (*Information Security Management System*)
QMED	:	Jabatan Pengurusan dan Penambahbaikan Kualiti
JKPU	:	Jawatankuasa Pengurusan Universiti
LPU	:	Lembaga Pengarah Universiti
AUKU	:	Akta Universiti dan Kolej Universiti
PKP	:	Pelan Kesinambungan Perkhidmatan
NACSA	:	Agensi Keselamatan Siber Negara (*National Cyber Security Agency*)
PE	:	Pengarah Eksekutif
PDCA	:	Strategi Rancang-Laksana-Periksa-Tindak

		(Plan-Do-Check-Act)
SOA	:	Pernyataan Kebolehgunaan (*Statement of Applicability*)
JK ISMS	:	Jawatankuasa Kerja ISMS
ISMR	:	Wakil Pengurusan Keselamatan ISMS (ISMS *Representative*)
PP	:	Pengarah Pusat
PKS	:	Polisi Keselamatan Siber
NDA	:	Perjanjian Tanpa Pendedahan *(Non-Disclosure Agreement)*
LAN	:	Rangkaian Setempat (*Local Area Network*)
WAN	:	Rangkaian Luas (*Wide Area Network*)
UMCERT	:	Pasukan Tindak Balas Kecemasan Komputer UM (UM *Computer Emergency Response Team*)
NC4	:	Pusat Penyelarasan dan Kawalan Siber Negara (*National Cyber Coordination and Command Centre*)
JKPICT	:	Jawatankuasa Pengurusan ICT
DRT	:	Pasukan Pemulihan Bencana (*Disaster Recovery Team*)
PPB	:	Pelan Pemulihan Bencana
TOR	:	Terma Rujukan (*Terms and Reference*)
JPICT	:	Jawatankuasa Pengguna ICT
JTICT	:	Jawatankuasa Teknikal ICT
JPSA	:	Jawatankuasa Penilaian Sistem Aplikasi
JK Pintar	:	Jawatankuasa Kerja Pelaksana Kampus Lestari Pintar UM
JAPPICT	:	Jawatankuasa Pembangunan Projek ICT
JK ISMS	:	Jawatankuasa Kerja Sistem Pengurusan Keselamatan Maklumat
PSP	:	Pelan Strategik Pendigitalan
CCTV	:	Kamera Litar Tertutup (*Closed-Circuit Television*)

CD	:	Cakera Padat (*Compact Disc*)
USB	:	Bas Bersiri Sejagat (*Universal Serial Bus*)
RBAC	:	Kawalan Akses Berasaskan Peranan *(Role-Based Access Control)*
VPN	:	Rangkaian Persendirian Maya (*Virtual Private Network*)
MFA	:	Pengesahan Pelbagai Faktor (*Multi Factor Authentication*)
PII	:	Maklumat Pengenalan Peribadi (*Personally Identifiable Information*)
CPU	:	Unit Pemprosesan Pusat (*Central Processing Unit*)
SSL	:	Lapisan Soket Selamat (*Secure Socket Layer*)
CMS	:	Sistem Pengurusan Kandungan (*Content Management System*)
BIA	:	Analisis Impak Perniagaan (*Business Impact Analysis*)
RTO	:	Objektif Masa Pemulihan (*Recovery Time Objective*)
RPO	:	Objektif Titik Pemulihan (*Recovery Point Objective*)
JSM	:	Jabatan Sumber Manusia
PIN	:	Nombor Pengenalan Diri (*Personal Identification Number*)
BYOD	:	*Buy Your Own Device*
SLA	:	Perjanjian Tahap Perkhidmatan (*Service Level Agreement*)
UPS	:	Bekalan Kuasa Tanpa Gangguan (*Uninterruptible Power Supply*)
RAM	:	Ingatan Capaian Rawak (*Random Access Memory*)
CDR	:	Cakera Padat-Boleh Rakam

		(*Compact Disc-Recordable*)
CDRW	:	Cakera Padat-Boleh Tulis Semula (*Compact Disc-ReWritable*)
CPU	:	Unit Pemprosesan Pusat (*Central Processing Unit*)
DDOS	:	Serangan Penafian-Perkhidmatan Teragih (*Distributed Denial-of-Services*)
DNS	:	Sistem Nama Domain (*Domain Name System*)
MST	:	Waktu Piawai Malaysia (Malaysia *Standard Time*)
OJT	:	Latihan Sambil Bekerja (*On-Job-Training*)
WiFi	:	Rangkaian Tanpa Wayar (*Wireless Fidelity*)
IP	:	Protokol Internet (*Internet Protocol*)
SHA	:	Algoritma Cincangan Selamat (*Secure Hash Algorithm*)
RADIUS	:	Perkhidmatan Pengesahan Capaian Jauh (*Remote Authentication Dial-In User Service*)
TACACS	:	Sistem Kawalan Akses Pengawal Terminal (*Terminal Access Controller Access-Control System*)
CAS	:	Perkhidmatan Pengesahan Berpusat (*Central Authentication Service*)
TLS	:	Keselamatan Lapisan Pengangkutan (*Transport Layer Security*)
CSR	:	Permintaan Penandatanganan Sijil (*Certificate Singning Request*)
SQL	:	Bahasa Pertanyaan Berstruktur (*Structured Query Language*)
EOS	:	Tamat Tempoh Sokongan (*End of Support*)
IPR	:	Hak Harta Intelek (*Intellectual Property Rights*)

ADPD : Akta Perlindungan Data Peribadi

1.6 SUMBER RUJUKAN

Bil	Nama Dokumen
1.6.1	Akta Universiti dan Kolej Universiti 1971
1.6.2	Akta Rahsia Rasmi 1972
1.6.3	Akta Perlindungan Data Peribadi 2010 [Akta 709]
1.6.4	Arahan Keselamatan
1.6.5	Piawaian ISO/IEC 27001
1.6.6	Pekeliling Am Bilangan 3 Tahun 2000: Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan
1.6.7	Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam
1.6.8	Garis Panduan Pengurusan Aset/Inventori
1.6.9	Polisi Pengurusan Maklumat Rasmi Universiti Malaya 2024
1.6.10	Dokumen Induk Pengurusan Kewangan Universiti Malaya
1.6.11	PK 2.6 Perolehan Perkhidmatan Pengkomputeran Awan (*Cloud*) Sektor Awam
1.6.12	Surat Pekeliling Am Bilangan 2 Tahun 2021 Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (*Cloud Computing*) Dalam Perkhidmatan Awam (versi 2.0)

2.0 TADBIR URUS ORGANISASI ICT

2.1 PENGENALAN

Tadbir urus dan pengurusan ICT merangkumi pendekatan menyeluruh dalam merancang, mengawal selia, dan memantau penggunaan teknologi maklumat bagi menyokong fungsi teras Universiti. Ia melibatkan pengurusan sumber, proses, dan tanggungjawab yang berkaitan bagi memastikan kecekapan, keberkesanan dan keselamatan perkhidmatan ICT di UM sentiasa berada pada tahap yang optimum.

Tadbir urus ini juga memastikan penerangan peranan dan tanggungjawab yang jelas kepada pihak berkepentingan dalam organisasi bagi menjamin kelestarian dan pematuhan terhadap dasar, peraturan serta hala tuju strategik Universiti.

2.2 TUJUAN

Tadbir urus dan pengurusan ICT yang berkesan membantu Universiti untuk menerangkan perkara berikut dengan jelas:

(1) Peranan utama dalam pengurusan ICT UM;

(2) Skop dan fungsi pengurusan ICT; dan

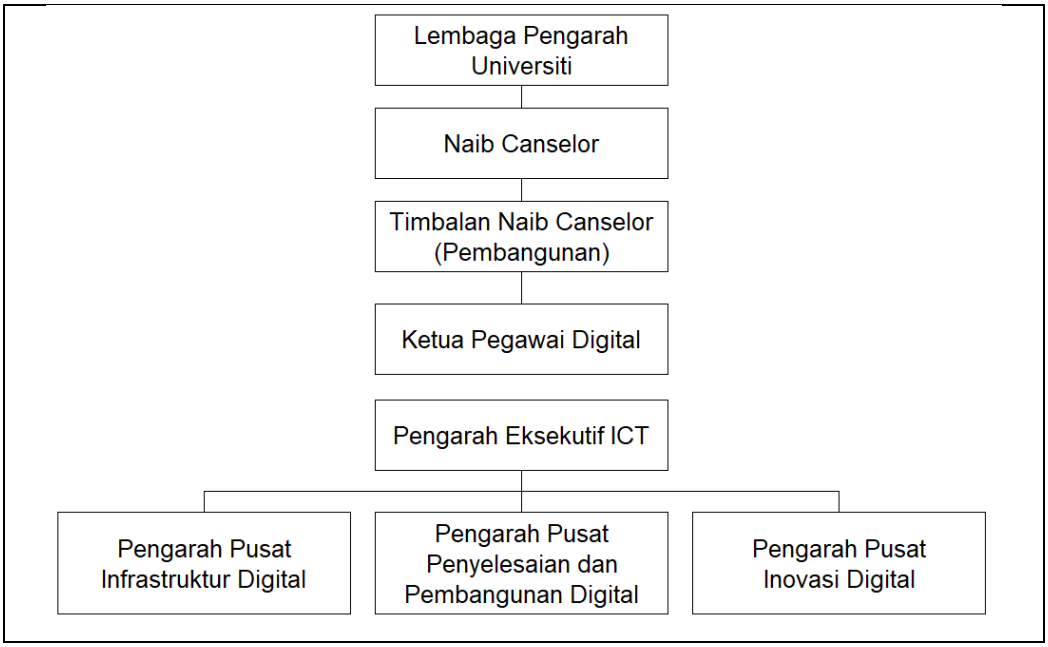
(3) Tadbir urus dalam pengurusan ICT.

2.3 PENGURUSAN ORGANISASI ICT

Pengurusan organisasi ICT di UM merangkumi struktur tadbir urus yang bertanggungjawab untuk merancang, melaksanakan, dan memantau semua aktiviti berkaitan teknologi maklumat Universiti. Setiap peringkat mempunyai tanggungjawab yang jelas dalam memastikan operasi ICT berjalan dengan efisien, selamat, dan selaras dengan pelan strategik Universiti.

Struktur ini terdiri daripada Lembaga Pengarah Universiti (LPU), Pengurusan Tertinggi Universiti, Ketua Pegawai Digital (CDO) serta

Pengarah Eksekutif ICT dan Pengarah Pusat ICT yang memainkan peranan sebagai entiti utama seperti diterangkan dalam **Rajah 2-1**.



Rajah 2-1 Struktur Pengurusan ICT UM

2.3.1 Lembaga Pengarah Universiti

Menurut Akta Universiti dan Kolej Universiti (AUKU) 1971, pihak berkuasa Universiti ialah Lembaga, Senat, Jawatankuasa Pengurusan Universiti atau dengan apa-apa jua nama ia disebut, Fakulti, Sekolah, Pusat, Akademi, Institut, Jawatankuasa Pengajian, Jawatankuasa Pemilih, Jawatankuasa Kebajikan Pekerja, Jawatankuasa Kebajikan Pelajar, dan badan lain sebagaimana yang ditetapkan oleh statut sebagai Pihak Berkuasa Universiti.

Dalam konteks ini, pihak berkuasa tertinggi Universiti ialah Lembaga Pengarah Universiti (LPU). LPU hendaklah menjadi badan yang mengelola, membuat dasar dan mengawasi Universiti, dan boleh menjalankan segala kuasa yang diberikan kepada Universiti kecuali setakat yang kuasa itu diberikan oleh Perlembagaan ini atau statut, kaedah-kaedah dan peraturan-peraturan kepada pihak berkuasa, badan atau kepada pegawai lain Universiti.

2.3.2 Naib Canselor

Naib Canselor yang dilantik berperanan sebagai Ketua Pegawai Eksekutif Universiti dan bertanggungjawab terhadap keseluruhan aspek pentadbiran, akademik, pengurusan dan hal ehwal harian Universiti, tertakluk kepada kuasa yang diperuntukkan melalui statut.

Dalam konteks ICT di UM, Naib Canselor bertanggungjawab untuk:

(1) Menentukan hala tuju strategik dan menyeluruh pembangunan ICT Universiti selaras dengan visi, misi, nilai teras serta Pelan Strategik UM yang berkuat kuasa.

(2) Menguatkuasakan pematuhan terhadap Dokumen Induk Pengurusan ICT UM oleh seluruh warga dan pihak berkepentingan.

(3) Menyokong pembangunan ICT melalui penyediaan sumber manusia, kewangan dan keselamatan yang mencukupi.

(4) Melantik Ketua Pegawai Digital (CDO), Pengarah Eksekutif ICT, Pegawai Keselamatan ICT (ICTSO) dan Pengarah Pusat ICT bagi memastikan pelaksanaan strategi dan keselamatan ICT Universiti dilaksanakan dengan berkesan.

2.3.3 Timbalan Naib Canselor (Pembangunan)

Timbalan Naib Canselor (Pembangunan) bertanggungjawab membantu Naib Canselor dalam menentukan objektif dan hala tuju pembangunan, kegiatan keusahawanan dan penjanaan pendapatan Universiti, serta memberi kepimpinan untuk merealisasikan visi, misi dan nilai teras UM.

Dalam konteks pembangunan ICT, Timbalan Naib Canselor (Pembangunan) berperanan untuk:

(1) Menyelaraskan pembangunan ICT dengan strategi pembangunan fizikal Universiti bagi menyokong fungsi pengajaran, pembelajaran, penyelidikan dan inovasi.

(2) Menyokong pengurusan pembangunan ICT selaras dengan dasar, prosedur dan garis panduan Universiti.

(3) Memastikan pembangunan ICT menyumbang kepada kecekapan operasi akademik dan pentadbiran Universiti.

(4) Menyokong pelaksanaan infrastruktur ICT yang selamat dan bersepadu dalam pembangunan Universiti.

2.3.4 Ketua Pegawai Digital

Ketua Pegawai Digital (CDO) bertanggungjawab untuk membantu Timbalan Naib Canselor (Pembangunan) dalam memacu transformasi digital Universiti dan memastikan tadbir urus serta keselamatan ICT Universiti dilaksanakan secara menyeluruh dan berkesan. Peranan dan tanggungjawab CDO merangkumi:

(1) Merancang dan memimpin pelaksanaan strategi transformasi digital Universiti selaras dengan objektif dan pelan strategik ICT Universiti yang berkuat kuasa.

(2) Memastikan dasar, prosedur dan garis panduan ICT dilaksanakan secara cekap dan mematuhi peraturan yang ditetapkan.

(3) Menyelia dan menyelaras projek ICT yang strategik dan berskala besar.

(4) Menyelaras pelaksanaan inisiatif keselamatan siber selaras dengan peraturan dan pekeliling yang berkuat kuasa.

(5) Berperanan sebagai Pengerusi Pasukan Krisis ICT UM dan bertanggungjawab terhadap pelaksanaan Pelan Kesinambungan Perkhidmatan (PKP).

(6) Memastikan keberkesanan pelaksanaan program latihan dan kesedaran keselamatan siber.

(7) Bertindak sebagai penghubung rasmi dengan agensi keselamatan siber kerajaan seperti Agensi Keselamatan Siber Negara (NACSA).

(8) Memberi nasihat strategik kepada pengurusan Universiti berkenaan ICT dan keselamatan digital.

2.3.5 Pengarah Eksekutif ICT

Pengarah Eksekutif ICT (PE ICT) merujuk kepada Pengarah Eksekutif JTM yang berperanan untuk membantu CDO dalam aspek pengurusan dan tadbir urus ICT Universiti. Peranan dan tanggungjawab Pengarah Eksekutif ICT secara keseluruhan seperti berikut:

(1) Menterjemah hala tuju strategik kepada pelaksanaan inisiatif ICT bagi menyokong pelan strategik Universiti.

(2) Menyelaraskan pelaksanaan dasar, piawaian dan prosedur ICT selaras dengan tadbir urus dan keperluan pematuhan.

(3) Menyokong pelaksanaan pembangunan digital Universiti selari dengan strategi Universiti.

(4) Memastikan pelaksanaan dasar, prosedur dan garis panduan ICT Universiti memenuhi keperluan perkhidmatan yang cekap serta pematuhan.

(5) Merancang, melaksanakan dan memantau projek ICT mengikut perancangan strategik Universiti.

(6) Mematuhi dan melaksanakan langkah-langkah keselamatan ICT serta menyokong penguatkuasaan kawalan keselamatan oleh ICTSO.

Dalam konteks pengurusan keselamatan maklumat, Pengarah Eksekutif ICT berperanan sebagai peneraju bagi keseluruhan inisiatif ISMS. Peranan dan tanggungjawab Pengarah Eksekutif ICT adalah seperti berikut:

(1) Bertanggungjawab ke atas polisi keselamatan.

(2) Mengatur strategi Rancang-Laksana-Periksa-Tindak (PDCA) berdasarkan penilaian risiko.

(3) Menyediakan sumber yang mencukupi untuk menangani ancaman bisnes.

(4) Meluluskan pelaksanaan kawalan yang diperlukan seperti yang dinyatakan dalam Pernyataan Kebolehgunaan (SOA) berdasarkan *Annex A, ISO:IEC 27001*.

(5) Menghebahkan strategi keselamatan dan mengarahkan Jawatankuasa Kerja ISMS (JK ISMS) untuk mewujudkan budaya kesedaran keselamatan dalam JTM.

(6) Dari semasa ke semasa, mengarahkan Wakil Pengurusan Keselamatan ISMS (ISMR) untuk membuat keputusan berkaitan dengan isu keselamatan semasa ketiadaannya.

(7) Melantik pegawai yang bertindak sebagai Pengawal Dokumen untuk mengekalkan dokumen berkaitan ISMS dan bertindak sebagai Urus Setia JK ISMS.

2.3.6 Pengarah Pusat ICT

Pengarah Pusat ICT (PP ICT) bertanggungjawab untuk membantu Pengarah Eksekutif ICT dalam melaksanakan tugas-tugas pengurusan dan tadbir urus ICT mengikut bidang. Peranan dan tanggungjawab Pengarah Pusat ICT adalah seperti berikut:

(1) Memberi input teknikal dan pengurusan berdasarkan bidang kepakaran bagi menyokong pelaksanaan strategi ICT Universiti.

(2) Memastikan pelaksanaan dan pematuhan terhadap keperluan teknikal dan garis panduan pelaksanaan ICT.

(3) Merancang, melaksana dan memantau projek ICT mengikut fungsi serta peranan pusat.

(4) Menyelia dan memastikan keberkesanan operasi ICT menyokong pelan strategik ICT Universiti.

(5) Mematuhi dan melaksanakan keperluan keselamatan ICT serta menyokong kawalan keselamatan oleh ICTSO.

Dalam konteks pengurusan keselamatan maklumat, peranan dan tanggungjawab Pengarah Pusat ICT adalah seperti berikut:

(1) Memperuntukkan dan menyediakan sumber untuk menjalankan fungsi mereka demi kelestarian ISMS.

(2) Menetapkan kaedah dan sumber sedia ada untuk menambah baik dan jika perlu, meminta pihak pengurusan memperuntukkan sumber tambahan untuk mematuhi keperluan ISMS.

(3) Mencadangkan pelantikan ahli JK ISMS dari kalangan staf di Pusat masing-masing.

(4) Mengetuai sesi perbincangan berkaitan penemuan audit dalaman bahagian dan mengarahkan tindakan yang perlu diambil.

(5) Melaporkan kepada JK ISMS apabila terdapat penemuan audit seperti pelanggaran polisi, keperluan undang-undang, perbuatan jenayah atau penemuan/kejadian yang setara.

2.3.7 Pegawai Keselamatan ICT

Pegawai Keselamatan ICT (ICTSO) dilantik selaras dengan Pekeliling Am Bilangan 3 Tahun 2000, dan bertanggungjawab memastikan pengurusan keselamatan ICT Universiti dilaksanakan secara menyeluruh, berkesan dan mematuhi dasar serta piawaian yang berkuat kuasa. Peranan dan tanggungjawab ICTSO adalah seperti berikut:

(1) Memberi panduan dan nasihat dalam perancangan strategik ICT untuk memastikan aspek keselamatan sentiasa diambil kira.

(2) Memastikan piawaian, polisi, arahan kerja, prosedur dan garis panduan keselamatan ICT dibangunkan, dikemas kini dan dikuatkuasakan mengikut keperluan Universiti dan peraturan semasa.

(3) Memastikan infrastruktur keselamatan ICT mematuhi prinsip dan peraturan keselamatan yang berkuat kuasa.

(4) Menyokong keperluan keselamatan dalam projek pembangunan ICT dan pelaksanaan sistem serta aplikasi.

(5) Menyelaras kawalan keselamatan, pelaporan dan siasatan insiden keselamatan serta tindakan pemulihan.

(6) Mencadangkan langkah pengukuhan keselamatan berdasarkan perubahan teknologi dan ancaman siber.

(7) Merancang dan melaksanakan program keselamatan serta kesedaran ICT bagi meningkatkan kefahaman dan pembudayaan amalan keselamatan dalam kalangan pengguna UM.

(8) Berperanan sebagai ahli Pasukan Pengurusan Krisis Universiti dalam menangani insiden keselamatan ICT yang kritikal.

(9) Melaporkan insiden keselamatan kepada CDO dan pihak berkaitan mengikut keperluan PKP.

(10) Bekerjasama dalam siasatan insiden serta mencadangkan tindakan pemulihan yang bersesuaian.

2.3.8 Pegawai Teknologi Maklumat

Pegawai yang bertanggungjawab untuk membangun, mengurus, mengawal, memantau dan menyelenggara kemudahan dan perkhidmatan ICT. Antara peranan dan tanggungjawab pegawai seperti berikut:

(1) Melaksanakan projek pembangunan, penyediaan dan penaiktarafan ICT berdasarkan pelan strategik ICT UM yang berkuat kuasa.

(2) Memastikan pelaksanaan projek ICT mematuhi garis panduan teknikal serta dokumentasi rasmi.

(3) Melaksanakan pembangunan dan penaiktarafan sistem serta infrastruktur ICT berdasarkan perancangan yang telah ditetapkan.

(4) Melaksanakan konfigurasi dan sokongan keselamatan asas serta menyokong pelaksanaan PKP dan laporan insiden keselamatan di peringkat teknikal.

2.3.9 Penolong Pegawai Teknologi Maklumat

Pegawai pelaksana yang menyokong tugas teknikal dan operasi ICT di bawah seliaan Pegawai Teknologi Maklumat termasuk penyelenggaraan, pelaksanaan dan pemantauan perkhidmatan dan sistem ICT bagi memastikan kelancaran operasi ICT di Universiti. Antara tugas dan tanggungjawab pegawai pelaksana adalah seperti berikut:

(1) Membantu dalam pelaksanaan projek ICT termasuk penyediaan peralatan, konfigurasi awal, dan ujian sistem mengikut spesifikasi teknikal yang ditetapkan.

(2) Menyelenggara sistem dan peralatan ICT, termasuk tugas rutin seperti kemas kini perisian, pemeriksaan keselamatan, dan sokongan teknikal harian kepada pengguna.

(3) Melaksanakan sokongan pengguna (*helpdesk* dan *onsite*), termasuk menyelesaikan aduan, memberikan bimbingan penggunaan sistem/aplikasi, serta mendokumentasikan tindakan sokongan.

(4) Membantu dalam pembangunan sistem dalaman atau penyelenggaraan pangkalan data dengan melakukan input data, ujian fungsi, dan semakan awal.

(5) Melaksanakan kawalan keselamatan asas, seperti konfigurasi antivirus, semakan log sistem, dan pelaksanaan arahan kerja berkaitan insiden keselamatan ICT.

(6) Mengurus inventori peralatan ICT, termasuk merekod, mengagih, dan memantau status penggunaan atau kerosakan peralatan ICT.

(7) Menyediakan laporan teknikal asas berkaitan status operasi sistem, penyelenggaraan, dan aktiviti sokongan ICT untuk dikemukakan kepada Pegawai Teknologi Maklumat.

2.4 ORGANISASI KESELAMATAN SIBER

Sebagai sebahagian daripada rangka tadbir organisasi ICT yang komprehensif di UM, organisasi keselamatan siber memainkan peranan kritikal dalam memastikan keselamatan sistem ICT dan aset maklumat Universiti sentiasa terjamin. Struktur ini menyokong pelaksanaan dasar keselamatan, pengurusan risiko dan pematuhan kepada peraturan, sekaligus menjamin keberkesanan dan kelestarian ekosistem ICT yang selamat di Universiti.

Peranan pelbagai pihak dalam organisasi ini digariskan bagi memastikan tanggungjawab keselamatan siber dilaksanakan secara menyeluruh dan kolaboratif. Dokumen ini menerangkan peranan bagi entiti yang mentadbir urus keselamatan siber selain Pengurusan ICT UM.

2.4.1 Wakil Pengurusan Keselamatan Maklumat (ISMR)

Selain ICTSO, ISMR adalah pegawai yang bertanggungjawab untuk menjaga keseluruhan ISMS. Peranan dan tanggungjawab utama ISMR adalah seperti berikut:

(1) Menganalisis keperluan dan menentukan proses kerja dan garis panduan untuk memastikan strategi PDCA ISMS yang diterima pakai adalah konsisten.

(2) Membuat keputusan berkaitan dengan isu keselamatan semasa ketiadaan Pengarah Eksekutif ICT apabila diarahkan.

(3) Bertindak sebagai penghubung antara Pengarah Eksekutif ICT dan JK ISMS.

(4) Berkomunikasi dengan badan pensijilan yang menjalankan audit ISMS.

(5) Memberikan khidmat nasihat berhubung cadangan tindakan penutupan penemuan audit dan membuat pengesahan.

2.4.2 Pengguna

Pengguna ditakrifkan sebagai individu atau kumpulan yang diberikan kebenaran untuk menggunakan sistem, perisian, perkakasan atau maklumat bagi menyokong fungsi utama Universiti. Ini merangkumi warga Universiti, pihak ketiga seperti pembekal, kontraktor, penyedia perkhidmatan, serta pihak berkepentingan lain yang diberi akses kepada kemudahan ICT Universiti.

Setiap pengguna bertanggungjawab untuk mematuhi prinsip-prinsip keselamatan ICT dan mengamalkan tatakelakuan yang selamat dan beretika. Antara kewajipan yang perlu dipatuhi oleh pengguna ICT Universiti adalah seperti berikut:

(1) Membaca, memahami dan mematuhi Dokumen Induk Pengurusan ICT UM.

(2) Mengetahui dan memahami implikasi keselamatan ICT kesan daripada tindakannya.

(3) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat.

(4) Melaksanakan langkah-langkah perlindungan seperti berikut:

   (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan.

   (b) Menjaga kerahsiaan kata laluan.

   (c) Mematuhi piawaian, garis panduan, prosedur dan arahan kerja keselamatan yang ditetapkan.

   (d) Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan.

(5) Mematuhi prinsip-prinsip Polisi Keselamatan Siber (PKS) yang dinyatakan dalam Dokumen Induk Pengurusan ICT UM dan menjaga kerahsiaan maklumat Universiti.

(6) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera.

(7) Menghadiri program-program kesedaran mengenai keselamatan ICT.

2.4.3 Pihak Ketiga

Pihak ketiga merujuk kepada individu, organisasi atau entiti yang bukan sebahagian daripada struktur organisasi UM tetapi mempunyai hubungan rasmi melalui perjanjian, kontrak atau kerjasama untuk menyediakan perkhidmatan atau sokongan ICT kepada Universiti. Ini adalah termasuk pembekal, penyedia perkhidmatan, kontraktor, konsultan dan pihak luar yang dilantik.

Peranan dan tanggungjawab pihak ketiga adalah seperti berikut:

(1) Menandatangani Perjanjian Tanpa Pendedahan (*Non-Disclosure Agreement,* NDA) sebelum diberikan akses kepada sistem atau maklumat Universiti.

(2) Membaca, memahami dan mematuhi Dokumen Induk Pengurusan ICT UM.

(3) Memahami implikasi keselamatan ICT kesan dari tindakannya.

(4) Melaporkan dengan segera sebarang aktiviti atau keadaan yang meragukan yang mungkin memberikan ancaman kepada aset ICT.

(5) Memastikan kerahsiaan maklumat UM terpelihara.

(6) Mengambil langkah-langkah keselamatan yang bersesuaian bagi memastikan semua aset dan maklumat Universiti yang berada dalam pengurusan atau kawalan mereka dilindungi sepenuhnya daripada sebarang risiko atau pencerobohan.

(7) Mengembalikan semua maklumat dan aset Universiti serta menamatkan akses apabila kontrak atau urusan tamat.

2.4.4 Pemilik Aset

Pemilik Aset dalam konteks ICT ditakrifkan sebagai pegawai yang bertanggungjawab terhadap pengurusan dan perlindungan aset maklumat dan ICT Universiti sepanjang kitar hayatnya. Pemilik Aset memainkan peranan utama dalam memastikan aset maklumat digunakan, disimpan dan dilindungi mengikut keperluan keselamatan Universiti berdasarkan piawaian ISMS. Tanggungjawab utama Pemilik Aset adalah seperti berikut:

(1) Mengenal pasti dan mendaftarkan aset maklumat di bawah kawalan masing-masing dengan tepat.

(2) Menentukan klasifikasi keselamatan aset berdasarkan tahap sensitiviti, nilai dan kepentingan kepada Universiti.

(3) Menetapkan kawalan akses terhadap aset bagi memastikan hanya pihak yang dibenarkan mempunyai capaian yang bersesuaian.

(4) Menilai dan mengurus risiko keselamatan yang berkaitan dengan aset maklumat.

(5) Memastikan kawalan keselamatan ke atas aset dilaksanakan, disemak dan dikemas kini secara berkala.

(6) Menguruskan sebarang penggunaan, pengubahsuaian atau pelupusan aset maklumat mengikut prosedur yang ditetapkan.

(7) Bekerjasama dengan pihak berkaitan bagi menjamin keselamatan maklumat yang menyeluruh.

2.4.5 Pemilik Proses

Pemilik Proses merujuk kepada individu atau entiti yang bertanggungjawab sepenuhnya terhadap pelaksanaan dan pemantauan sesuatu proses selaras dengan kawalan keselamatan maklumat yang berkuat kuasa. Sebagai contoh, Timbalan Naib Canselor (Akademik & Antarabangsa) bertindak sebagai Pemilik Proses bagi sistem maklumat pelajar, manakala Pendaftar merupakan Pemilik Proses bagi sistem sumber manusia.

Peranan dan tanggungjawab Pemilik Proses dan wakilnya adalah seperti berikut:

(1) Mengenal pasti maklumat dan aset yang terlibat dalam proses yang terlibat dalam proses yang dikendalikan serta melaksanakan tahap perlindungan yang sewajarnya.

(2) Bekerjasama dengan pihak berkaitan bagi memastikan keberkesanan pengurusan keselamatan maklumat dalam proses tersebut.

(3) Melaporkan kepada pihak bertanggungjawab sebarang kelemahan atau insiden keselamatan maklumat yang berlaku dalam proses di bawah kawalannya.

2.4.6 Pentadbir Sistem ICT

Pentadbir Sistem ICT ialah individu yang dilantik dan diberi tanggungjawab untuk memastikan pengurusan sistem ICT yang merangkumi perkakasan, perisian, rangkaian dan data dilaksanakan secara selamat dan mematuhi keperluan ISMS, termasuk pelaksanaan kawalan teknikal, pengurusan akses, serta pelaporan insiden keselamatan.

Peranan dan tanggungjawab Pentadbir Sistem ICT dikategorikan seperti dalam **Jadual 2-1**.

Jadual 2-1 Pengasingan Tugas Pentadbir Sistem ICT

Bil	Peranan	Tugas & Tanggungjawab
(1)	Pentadbir Rangkaian	(a) Memastikan ketersediaan rangkaian setempat (LAN) dan rangkaian luas (WAN) di UM; (b) Memastikan semua peralatan dan perisian rangkaian diselenggara; (c) Merancang peningkatan infrastruktur, ciri keselamatan dan prestasi rangkaian sedia ada;

Bil	Peranan	Tugas & Tanggungjawab
		(d) Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil; (e) Memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian; (f) Memastikan laluan trafik keluar masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian UM secara tidak sah; dan (g) Menyediakan zon khas rangkaian untuk tujuan tertentu.
(2)	Pentadbir Pusat Data	(a) Melaksanakan polisi penggunaan pangkalan data; (b) Melaksanakan pemantauan dan penyelenggaraan pangkalan data secara berterusan; (c) Memastikan aktiviti pentadbiran pangkalan data seperti kawalan capaian dan proses pengemaskinian data dilaksanakan dengan teratur; (d) Memastikan persekitaran fizikal dan keselamatan Pusat Data dalam keadaan baik dan selamat; (e) Memastikan keselamatan data dan sistem aplikasi di dalam Pusat Data; dan

Bil	Peranan	Tugas & Tanggungjawab
		(f) Melaporkan sebarang pelanggaran keselamatan pangkalan data dan Pusat Data kepada ICTSO.
(3)	Pentadbir Sistem Aplikasi	(a) Mengkaji cadangan pembangunan atau penyelenggaraan sistem; (b) Membuat kajian semula serta menambah baik sistem sedia ada; (c) Membuat pemantauan dan penyelenggaraan terhadap sistem; (d) Menyediakan dokumentasi sistem yang berkaitan; (e) Memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas; (f) Memastikan kod program sistem aplikasi adalah selamat dari penggodam sebelum sistem tersebut diaktifkan penggunaannya; (g) Melaksanakan pewujudan dan penutupan akaun pengguna ke atas setiap aplikasi mengikut polisi; dan (h) Melaporkan kepada ICTSO jika berlakunya insiden keselamatan ke atas sistem aplikasi di bawah seliaan.
(4)	Pentadbir Keselamatan ICT	(a) Melakukan pemantauan keselamatan ICT; (b) Melakukan ujian penembusan (*penetration*) secara berkala; (c) Menyelaras semakan peraturan (*rules*) perkakasan keselamatan;

Bil	Peranan	Tugas & Tanggungjawab
		(d) Menyelaraskan aktiviti ujian penembusan dan kajian semula infrastruktur ICT oleh pihak luaran; dan (e) Melaporkan sebarang pelanggaran keselamatan ICT kepada ICTSO.

2.4.7 Pasukan Tindak Balas Kecemasan Komputer UM (UMCERT)

Pasukan Tindak Balas Kecemasan Komputer UM (UMCERT) adalah pasukan yang ditubuhkan khas untuk mengendalikan pengurusan insiden keselamatan komputer di UM. Peranan dan tanggungjawab pasukan ini adalah seperti berikut:

(1) Menerima dan mengesan aduan dan menilai tahap keselamatan ICT dan jenis insiden.

(2) Merekod dan menjalankan siasatan awal insiden yang diterima.

(3) Mengambil tindakan ke atas insiden keselamatan ICT yang dilaporkan.

(4) Mengendalikan respons terhadap insiden keselamatan ICT dan melaksanakan pembaikan.

(5) Menasihati PTj untuk mengambil tindakan pemulihan dan pengukuhan sekiranya insiden yang berlaku melibatkan aset ICT yang berada di bawah tanggungjawab PTj.

(6) Hubungi dan laporkan kejadian itu kepada Pusat Penyelarasan dan Kawalan Siber Negara (NC4) di bawah NACSA.

(7) Menyediakan laporan pengendalian insiden untuk Jawatankuasa Pengurusan ICT UM (JKPICT).

(8) Memberi khidmat nasihat kepada pengguna dalam mengesan, mengenal pasti dan mengendalikan sebarang insiden keselamatan ICT.

(9) Menyebarkan maklumat untuk membantu pemantapan keselamatan ICT di UM dari masa ke semasa.

(10) Menjalankan penilaian untuk memastikan keselamatan ICT mencukupi dan mengambil tindakan pembaikan atau pengukuhan untuk meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baharu dapat dielakkan; dan

(11) Meningkatkan pengetahuan dan kesedaran tentang keselamatan maklumat melalui program kesedaran keselamatan ICT.

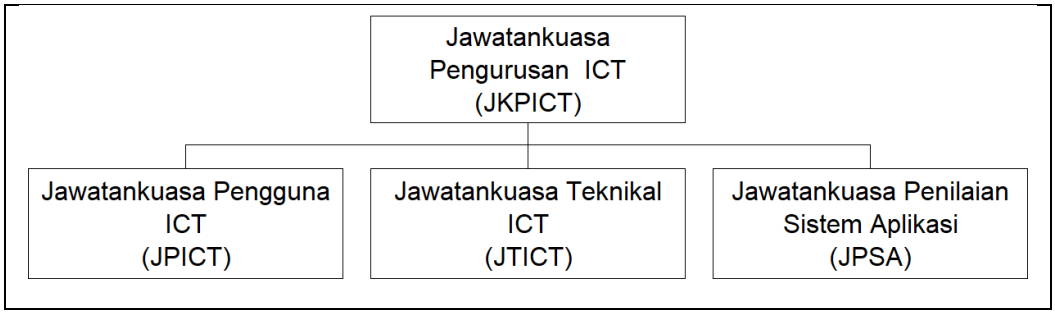
2.4.8 Pasukan Pemulihan Bencana bagi Perkhidmatan ICT

Pasukan Pemulihan Bencana (DRT) bagi Perkhidmatan ICT adalah pasukan yang ditubuhkan di bawah Pelan Kesinambungan Perkhidmatan (PKP). Pasukan ini bertanggungjawab dalam memastikan pelaksanaan memulihkan semula proses yang terganggu dan meneruskan semula perkhidmatan ICT berdasarkan Pelan Pemulihan Bencana (PPB) bagi Perkhidmatan ICT, di mana pelan ini adalah sebahagian daripada PKP.

Pasukan ini melibatkan pelbagai pihak termasuk Pentadbir Sistem ICT dan Pemilik Proses dalam memastikan PPB berjalan dengan teratur dan lancar. Terma rujukan pasukan ini adalah seperti didokumenkan dalam PKP.

2.5 JAWATANKUASA TADBIR URUS ICT UM

Jawatankuasa Tadbir Urus ICT UM berperanan sebagai entiti kawal selia utama dalam pengurusan ICT Universiti, selaras dengan pelan strategik UM yang berkuat kuasa. Skop peranannya meliputi aspek perancangan, pemantauan dan kawalan terhadap sumber ICT seperti perisian, perkakasan, rangkaian dan tenaga kerja, bagi menyokong pembangunan ICT yang mampan, cekap dan berdaya tahan. **Rajah 2-2** menerangkan secara ringkas struktur Jawatankuasa Tadbir Urus ICT UM.



Rajah 2-2 Struktur Jawatankuasa ICT UM

2.5.1 Jawatankuasa Pengurusan ICT

Jawatankuasa Pengurusan ICT (JKPICT) adalah jawatankuasa tertinggi yang menentukan hala tuju perkhidmatan ICT di UM untuk menyokong visi dan misi UM. Jawatankuasa ini menjalankan fungsi yang sama dengan Jawatankuasa Pengurusan UM (JKPU) dengan fokus khusus kepada agenda ICT Universiti. Terma rujukan Jawatankuasa adalah seperti dalam **Lampiran B1**.

2.5.2 Jawatankuasa Pengguna ICT

Jawatankuasa Pengguna ICT (JPICT) berperanan sebagai platform untuk membincangkan hal-hal berkaitan kepenggunaan ICT di UM dan menyuarakan keperluan ICT kepada JKPICT. Terma rujukan Jawatankuasa adalah seperti dalam **Lampiran B2**.

2.5.3 Jawatankuasa Teknikal ICT

Jawatankuasa Teknikal ICT (JTICT) UM bertanggungjawab menilai permohonan projek-projek ICT dari segi teknikal dan kewangan untuk menyokong visi dan misi UM. Terma rujukan Jawatankuasa adalah seperti dalam **Lampiran B3.**

2.5.4 Jawatankuasa Penilaian Sistem Aplikasi

Jawatankuasa Penilaian Sistem Aplikasi (JPSA) adalah jawatankuasa yang bertanggungjawab dalam membuat penilaian bagi semua permohonan pembangunan/ perolehan baharu, penaiktarafan dan perubahan (*change request*) sistem aplikasi sedia ada. Hanya projek yang mendapat sokongan JPSA layak dikemukakan untuk kelulusan

teknikal dari JTICT UM. Terma rujukan Jawatankuasa adalah seperti dalam **Lampiran B4**.

2.5.5 Jawatankuasa Pembangunan Projek ICT

Jawatankuasa Pembangunan Projek ICT (JAPPICT) adalah salah satu jawatankuasa di bawah seliaan CDO yang bertanggungjawab memperakukan kebolehlaksanaan dan memantau pelaksanaan projek ICT di bawah JTM. Ini bagi memastikan setiap projek dilaksanakan secara menyeluruh, selaras dengan prosedur yang ditetapkan, menggunakan sumber secara optimum, serta disiapkan mengikut jangka masa yang ditetapkan. Terma rujukan Jawatankuasa adalah seperti dalam **Lampiran B5**.

2.5.6 Jawatankuasa Kerja Sistem Pengurusan Keselamatan Maklumat

Jawankuasa Kerja Sistem Pengurusan Keselamatan Maklumat (JK ISMS) ialah entiti tunggal yang bertanggungjawab untuk merancang, melaksana, memantau dan bertindak ke atas semua bidang pengurusan keselamatan maklumat di JTM di bawah seliaan Pengarah Eksekutif ICT. Jawatankuasa ini terdiri di kalangan warga JTM yang dilantik tertakluk kepada terma rujukan dan berperanan untuk menggerak, membangun, melaksana dan menyelenggara ISMS. Terma rujukan Jawatankuasa adalah seperti di **Lampiran B6.**

3.0 TADBIR URUS STRATEGIK ICT

3.1 PENGENALAN

Tadbir urus strategik ICT merujuk kepada proses perancangan dan pelaksanaan strategi ICT yang sejajar dengan visi dan misi Universiti. Ia merangkumi penyelarasan objektif, pengagihan sumber secara optimum, serta penerapan teknologi untuk meningkatkan kecekapan operasi, menggalakkan inovasi, dan memperkukuh daya saing Universiti dalam bidang pengajaran, pembelajaran serta penyelidikan.

3.2 TUJUAN

Pelaksanaan tadbir urus strategik ICT yang berstruktur dan terancang membolehkan Universiti bertindak proaktif dalam menyesuaikan diri dengan perubahan teknologi yang pesat, selain memanfaatkan sumber secara optimum dan melaksanakan pelaburan ICT dengan lebih berhemah serta memberi impak yang signifikan. Pendekatan ini juga mendorong pembentukan ekosistem digital Universiti yang holistik dan lestari, sekali gus memperkukuh pencapaian aspirasi Universiti dalam bidang pengajaran, pembelajaran dan penyelidikan.

3.3 PERANCANGAN STRATEGIK ICT

Perancangan strategik ICT memerlukan pendekatan yang sistematik dalam merangka, melaksana dan menilai strategi ICT bagi menyokong misi dan visi Universiti. Pelaksanaannya perlu mengambil kira perkara berikut:

(1) Perancangan strategik ICT hendaklah memenuhi keperluan fungsi teras Universiti, iaitu pengajaran, pembelajaran, penyelidikan dan pentadbiran.

(2) Perancangan strategik ICT hendaklah selaras dengan dasar, polisi, peraturan dan garis panduan kerajaan yang berkuat kuasa,

termasuk Pelan Strategik Pendigitalan (PSP) Sektor Awam dan pelan strategik Universiti.

(3) Keperluan ICT hendaklah dirancang dan dilaksanakan secara kolaboratif antara JTM dan PTj yang berkaitan, dan setiap perancangan tersebut hendaklah dibentang serta mendapat kelulusan daripada pengurusan Universiti.

(4) JTM bertanggungjawab dalam merancang, melaksana dan memantau keperluan ICT Universiti.

4.0 TADBIR URUS PROJEK ICT

4.1 PENGENALAN

Pengurusan projek adalah satu pendekatan yang sistematik dan teratur yang merangkumi proses perancangan, pelaksanaan, pemantauan dan penamatan projek bagi menghasilkan produk atau perkhidmatan yang unik. Panduan ini disediakan khusus kepada staf JTM untuk membantu dalam mentadbir urus dan melaksanakan projek ICT dengan teratur dan berkesan.

Projek ICT merangkumi pelbagai inisiatif pengkomputeran melibatkan salah satu atau gabungan jenis projek berikut:

(1) Pembangunan Sistem Aplikasi;

(2) Peningkatan Sistem;

(3) Perluasan Sistem;

(4) Perolehan Infrastruktur ICT; dan

(5) Perancangan Strategik ICT.

Penyelenggaraan dan sebarang pembaharuan tahunan yang bersifat berulang dan tidak melibatkan pembangunan baharu tidak dikategorikan sebagai projek dan dikecualikan daripada penubuhan struktur tadbir urus projek.

4.2 TUJUAN

Pengurusan projek ICT membantu dalam menyatakan peranan dan tanggungjawab pihak yang bertanggungjawab dalam mengurus, mentadbir, melaksana dan memantau pelaksanaan projek ICT di bawah kendalian JTM. Ia bertujuan memastikan pelaksanaan projek ICT dapat dijalankan secara sistematik, telus dan mengikut tatacara yang telah ditetapkan.

4.3 PENGURUSAN PROJEK ICT

Tadbir urus projek ICT menetapkan setiap projek mesti melalui proses perancangan, pelaksanaan, pemantauan, dan penilaian yang menyeluruh, dengan penekanan kepada penggunaan sumber secara optimum, pengurusan risiko yang efisien, serta pematuhan kepada prosedur dan piawaian yang ditetapkan. Projek ICT mestilah memenuhi syarat-syarat asas berikut:

(1) Mempunyai punca kuasa yang jelas daripada pengurusan Universiti secara rasmi/bertulis atau telah didaftarkan dalam pelan-pelan strategik Universiti yang berkuat kuasa.

(2) Mempunyai struktur tadbir urus yang jelas bagi memastikan projek dilaksanakan dengan teratur dan berkesan. Setiap struktur tadbir urus projek perlu dilantik secara rasmi dan disertakan dengan maklumat ringkas projek, terma rujukan jawatankuasa, dan tanggungjawab ahli dan pasukan. Ahli pasukan perlu terdiri daripada JTM dan PTj yang berkenaan.

(3) Penyelenggaraan dan sebarang pembaharuan tahunan dikategorikan sebagai bukan projek dan dikecualikan dari syarat-syarat asas pengurusan projek.

Tatacara tadbir urus dan pengurusan projek ICT adalah merujuk kepada prosedur yang berkuat kuasa dan boleh diakses di Portal Staf (https://portal.um.edu.my).

5.0 TABDIR URUS POLISI KESELAMATAN SIBER

5.1 PENGENALAN

Tadbir urus keselamatan siber merupakan kerangka menyeluruh yang merangkumi polisi dan kawalan keselamatan bagi melindungi maklumat dan aset ICT Universiti daripada ancaman, penyalahgunaan, manipulasi dan kehilangan secara sistematik.

Kerangka ini dibangunkan berdasarkan piawaian antarabangsa ISO/IEC 27001 selaras dengan Pekeliling Am Bilangan 3 Tahun 2000: Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan. Pelaksanaan kawalan keselamatan siber dibahagikan kepada jenis dokumen seperti berikut:

(1) **Dokumen Mandatori:** Dokumen yang diwajibkan mengikut piawaian ISO/IEC 27001 dan perlu disediakan bagi tujuan pematuhan dan pensijilan.

(2) **Dokumen Operasi:** Dokumen yang menerangkan pengurusan peroperasian ICT bagi menyokong keselamatan siber dan pematuhan piawaian.

Senarai dokumen boleh dirujuk dalam **Lampiran A** dan boleh didapati di Portal Staf (https://portal.um.edu.my).

5.2 TUJUAN

Kerangka ini dibangunkan bagi menyediakan pendekatan menyeluruh dan sistematik untuk melindungi maklumat dan aset ICT Universiti daripada ancaman, kerentanan (*vulnerability*) dan risiko keselamatan. Ia juga bertujuan untuk memperkukuh pematuhan terhadap keperluan perundangan dan peraturan yang berkuat kuasa, serta memastikan penglibatan pengguna dalam menjamin keselamatan siber di semua peringkat.

Dokumen ini dibangunkan untuk memelihara kerahsiaan, integriti dan ketersediaan semua aset maklumat universiti serta melindunginya

daripada sebarang ancaman, sama ada dalaman atau luaran, disengajakan atau tidak disengajakan, melalui langkah berikut:

(a) Memastikan kelancaran operasi universiti yang berlandaskan ICT dengan meminimumkan impak insiden keselamatan maklumat fizikal dan logikal;

(b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, tidak boleh disangkal, ketersediaan dan kesahihan;

(c) Mematuhi keperluan perundangan, peraturan, garis panduan, prosedur dan arahan kerja yang berkuat kuasa;

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

(e) Memudahkan perkongsian maklumat yang selamat dan terjamin;

(f) Mencegah sebarang penyalahgunaan atau kecurian maklumat Universiti;

(g) Meningkatkan tahap kesedaran keselamatan ICT kepada pihak berkepentingan Universiti merangkumi tetapi tidak terhad kepada pengurusan Universiti, staf, pelajar dan mana-mana pihak yang berurusan dengan perkhidmatan ICT UM; dan

(h) Menyediakan asas bagi penambahbaikan yang berterusan dalam pengurusan keselamatan dan pentadbiran ICT.

5.3 POLISI KESELAMATAN SIBER (PKS)

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

Keselamatan ICT merujuk kepada usaha memastikan semua perkhidmatan yang disediakan dan disampaikan melalui sistem ICT Universiti berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan sistem dan maklumat. Ia amat berkait rapat dengan perlindungan ke atas aset ICT Universiti.

Terdapat empat (4) komponen asas dalam pengurusan keselamatan ICT yang perlu diberi perhatian, iaitu:

(1) Melindungi maklumat rahsia rasmi dan maklumat rasmi Universiti dari capaian tanpa kuasa yang sah;

(2) Menjamin ketepatan dan kesempurnaan maklumat;

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

(4) Memastikan hanya pengguna yang dibenarkan mempunyai akses, serta maklumat diterima daripada sumber yang sah dan boleh dipercayai.

Polisi Keselamatan Siber (PKS) merangkumi perlindungan ke atas semua bentuk maklumat bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

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

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

(3) **Tidak Boleh Disangkal:** Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;

(4) **Kesahihan:** Data dan maklumat hendaklah dijamin kesahihannya; dan

(5) **Ketersediaan:** Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Kesemua langkah keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semulajadi aset ICT, ancaman yang wujud akibat daripada kelemahan tersebut, risiko yang mungkin timbul, dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

5.4 SKOP PKS

Dokumen Induk Pengurusan ICT UM merupakan rujukan utama kepada semua warga UM, dan pihak berkepentingan dalam pengurusan data atau maklumat Universiti. Dokumen ini memperincikan peranan, tanggungjawab, arahan, peraturan, garis panduan, dan amalan yang **WAJIB DIBACA, DIFAHAMI, dan DIPATUHI** oleh semua warga UM dan pihak berkepentingan, termasuk pembekal, pakar runding, serta pihak-pihak yang terlibat dengan perkhidmatan ICT UM.

Penetapan kawalan keselamatan yang digariskan adalah terpakai kepada semua aset maklumat dan perkhidmatan ICT di bawah seliaan JTM, meliputi data dan maklumat dalam bentuk salinan digital (*softcopy*) atau bercetak (*hardcopy*), perkakasan, perisian, sistem dan manusia. Aset-aset ini adalah sangat kritikal dan menjadi asas kepada kelangsungan operasi pengajaran dan pembelajaran, penyelidikan dan operasi pentadbiran yang cekap dan berkesan.

Keperluan asas yang perlu dipenuhi melalui pelaksanaan kawalan keselamatan adalah seperti berikut:

(1) **Kebolehcapaian Data dan Maklumat:** Data dan maklumat hendaklah boleh diakses secara berterusan dengan pantas, tepat, mudah dan boleh dipercayai. Ini adalah penting bagi memastikan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti.

(2) **Kerahsiaan dan Kesempurnaan Maklumat:** Semua data dan maklumat hendaklah dilindungi kerahsiaannya dan dikendalikan

dengan baik pada setiap masa untuk memastikan ketepatan serta melindungi kepentingan UM, perkhidmatan, dan masyarakat.

Skop PKS meliputi perlindungan menyeluruh terhadap semua bentuk maklumat Universiti yang diwujud, diproses, disimpan, dihantar, diguna, diedar, diselenggara, dihapus, dimusnah dan diarkibkan dalam persekitaran ICT UM. Perlindungan ini dilaksanakan melalui kawalan dan prosedur pengendalian yang sistematik ke atas komponen berikut:

(1) **Data dan Maklumat:** Koleksi fakta dalam bentuk kertas atau mesej elektronik yang digunakan untuk mencapai misi dan visi Universiti seperti dokumentasi, prosedur, rekod, pangkalan data, dan arkib maklumat, sama ada dalam bentuk bercetak atau digital.

(2) **Salinan Digital (*Softcopy*):** Fakta dalam bentuk elektronik yang digunakan untuk mencapai visi dan misi Universiti, termasuk rekod digital, e-mel, pangkalan data, dan maklumat arkib.

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

(4) **Perkakasan (*Hardware*):** Semua aset fizikal yang menyokong pemprosesan dan penyimpanan maklumat, termasuk komputer, pelayan, peralatan rangkaian, sistem storan, dan lain-lain peralatan sokongan. Ini termasuk juga kemudahan seperti komputer, pencetak, *firewall*, perkakasan keselamatan rangkaian, kamera litar tertutup (CCTV), sensor, pangkalan data, pelayan, peralatan komunikasi, penyaman udara dan sistem pencegah kebakaran.

(5) **Perisian (*Software*):** Program utiliti dan program perisian percuma/ sumber terbuka/ alatan termasuk perisian aplikasi dan sistem operasi yang digunakan untuk pemprosesan maklumat.

(6) **Sistem:** Semua sistem aplikasi yang digunakan untuk mengendali, memproses, menyimpan dan menghantar data atau maklumat untuk mencapai fungsi tertentu.

(7) **Manusia:** Individu mempunyai pengetahuan dan kebolehan melaksanakan skop tugas harian UM bagi mencapai visi dan misi

UM. Individu ini adalah aset berdasarkan tugas dan fungsi yang dilaksanakan.

Setiap aset ICT yang dinyatakan perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

5.5 PRINSIP PKS

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

(1) Akses Atas Dasar Perlu Mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "**perlu mengetahui**" sahaja. Ini bermakna akses hanya diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut.

(2) Hak Akses Minimum

Hak akses pengguna tahap paling minimum adalah untuk membaca dan/atau melihat sahaja. Kelulusan perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak akses perlu disemak dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna atau bidang tugas.

(3) Akauntabiliti

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT.

(4) Pengasingan

Tugas mewujud, menyimpan, mengemas kini, mengubah, membatal dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat

terperingkat atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan pentadbir dan operasi.

(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 atau maklumat mesti 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 diberikan berdasarkan keperluan apabila diperlukan, dan hanya untuk tempoh masa yang ditetapkan.

(6) Pengauditan

Pengauditan adalah proses mengenal pasti insiden keselamatan serta keadaan yang berpotensi mengancam keselamatan. Oleh itu, aset ICT termasuk tetapi tidak terhad kepada komputer, pelayan, penghala (*router*), tembok api (*firewall*) dan rangkaian hendaklah mampu menjana serta menyimpan log tindakan keselamatan atau jejak audit (*audit trail*).

(7) Pematuhan

Dokumen Induk Pengurusan ICT UM hendaklah **dibaca, difahami** dan **dipatuhi** bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT.

(8) Pemulihan

Pemulihan sistem amat penting bagi memastikan kebolehsediaan dan kebolehcapaian. Objektif utamanya adalah untuk meminimumkan gangguan atau kerugian akibat ketidaksediaan. Pemulihan boleh dicapai melalui aktiviti sandaran (*backup*) dan pelaksanaan pelan pemulihan dan kesinambungan perkhidmatan.

(9) Saling Bergantungan

Setiap prinsip di atas adalah saling melengkapi dan bergantung antara satu sama lain. Oleh itu, kepelbagaian pendekatan dalam merancang dan membangunkan pelbagai mekanisme keselamatan adalah penting bagi memastikan tahap keselamatan yang optimum.

5.6 PENILAIAN RISIKO KESELAMATAN ICT

Universiti hendaklah mengambil kira kewujudan risiko terhadap aset ICT akibat daripada ancaman dan kerentanan (*vulnerability*) yang semakin kompleks dan meningkat dari semasa ke semasa. Justeru itu, langkah-langkah proaktif dan bersesuaian perlu dilaksanakan bagi menilai tahap risiko aset ICT supaya pendekatan kawalan keselamatan yang paling berkesan dapat dikenal pasti dan diterapkan.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan secara berkala dan berterusan bergantung kepada perubahan teknologi, persekitaran kerja dan keperluan keselamatan. Hasil daripada penilaian ini akan digunakan untuk menentukan tindakan susulan atau kawalan mitigasi yang sesuai bagi mengurangkan atau mengawal risiko yang dikenal pasti.

Penilaian risiko ini hendaklah meliputi semua aset maklumat Universiti termasuk data dan maklumat, perkakasan, perisian, sistem dan manusia. Ia juga perlu dilaksanakan di lokasi yang menempatkan sumber-sumber teknologi maklumat termasuk pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain. Bagi menangani risiko, tindakan sewajarnya perlu dikenal pasti, termasuk:

(1) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

(2) Menerima atau bersedia menghadapi risiko yang mungkin berlaku selagi risiko tersebut tidak menjejaskan penyampaian perkhidmatan Universiti;

(3) Mengelak atau mencegah risiko dengan mengambil langkah-langkah yang dapat mengelak atau mencegah berlakunya risiko; dan

(4) Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

5.7 KAWALAN ORGANISASI

Berdasarkan piawaian ISMS, terdapat 37 kawalan yang perlu dipatuhi dalam pengurusan data dan maklumat Universiti.

5.7.1 Polisi Keselamatan Maklumat

Kawalan ini disediakan bagi memastikan polisi adalah bersesuaian, berterusan dan selaras dengan hala tuju Universiti dalam menyokong keselamatan maklumat, undang-undang dan keperluan kontrak perjanjian.

(1) Pelaksanaan Polisi	Tanggungjawab
Polisi ini dikuatkuasakan selari dengan penguatkuasaan Dokumen Induk Pengurusan ICT UM seperti yang telah dinyatakan dalam Perkara 1.3.	Naib Canselor UM dibantu oleh Timbalan Naib Canselor (Pembangunan), CDO, PE ICT, PP ICT, ICTSO

(2) Penyebaran Polisi	Tanggungjawab
Polisi ini terkandung di dalam Dokumen Induk Pengurusan ICT UM dan perlu disebarkan kepada pihak berkaitan seperti yang dinyatakan dalam Perkara 1.4.2.	CDO, PE ICT, PP ICT, ICTSO, Pentadbir Sistem ICT
(3) Penyelenggaraan Polisi	**Tanggungjawab**
Polisi ini adalah tertakluk kepada semakan dan pindaan Dokumen Induk Pengurusan ICT UM dan kaedah pelaksanaan seperti yang diterangkan secara ringkas dalam Perkara 1.4.3. Semua dokumen ICT yang dinyatakan dalam dokumen ini perlu mematuhi prosedur yang berkuat kuasa.	PE ICT, PP ICT, ICTSO, Pentadbir Sistem ICT
(4) Pematuhan Polisi	**Tanggungjawab**
Polisi ini mestilah dipatuhi dan difahami oleh semua pengguna.	Warga UM, Pengguna

5.7.2 Peranan dan Tanggungjawab Keselamatan Maklumat

Kawalan ini bertujuan untuk memastikan wujudnya struktur, peranan dan tanggungjawab dalam pengurusan keselamatan maklumat secara jelas di UM.

(1) Naib Canselor UM	Tanggungjawab
Peranan dan tanggungjawab Naib Canselor UM adalah seperti yang dinyatakan dalam Perkara 2.3.2.	Naib Canselor UM
(2) Ketua Pegawai Digital (CDO)	**Tanggungjawab**
Ketua Pegawai Digital (CDO) adalah jawatan yang dilantik bagi melaksanakan tugas dan tanggungjawab seperti yang dinyatakan dalam Perkara 2.3.4.	CDO

(3) Pengarah Eksekutif ICT	Tanggungjawab
Jawatan Pengarah Eksekutif ICT (PE ICT) merujuk kepada Pengarah Eksekutif JTM dengan peranan dan tanggungjawabnya seperti dinyatakan dalam Perkara 2.3.5.	PE ICT
(4) Pengarah Pusat ICT	**Tanggungjawab**
Peranan dan tanggungjawab Pengarah Pusat ICT (PP ICT) adalah seperti yang dinyatakan dalam Perkara 2.3.6.	PP ICT
(5) Pegawai Keselamatan ICT (ICTSO)	**Tanggungjawab**
Peranan dan tanggungjawab Pegawai Keselamatan ICT (ICTSO) adalah seperti yang dinyatakan dalam Perkara 2.3.7.	ICTSO
(6) Pentadbir Sistem ICT	**Tanggungjawab**
Pentadbir Sistem ICT diperincikan mengikut fungsian kerja yang dilaksanakan termasuk: (a) Pentadbir Rangkaian; (b) Pentadbir Pusat Data; (c) Pentadbir Sistem Aplikasi; dan (d) Pentadbir Keselamatan ICT. Peranan dan tanggungjawab bagi setiap pentadbir yang disenaraikan adalah seperti yang dinyatakan dalam Perkara 2.4.6.	Pentadbir Sistem ICT

5.7.3 Pengasingan Tugas

Kawalan pengasingan tugas ini disediakan bagi menerangkan perbezaan tugas setiap individu dengan jelas dan teratur untuk mengurangkan risiko penipuan, kesilapan dan pemintasan kawalan keselamatan maklumat.

(1) Pengasingan Tugas	Tanggungjawab
Pengasingan tugas dan bidang tanggungjawab dilaksanakan bagi mengurangkan peluang	PE ICT, PP ICT, ICTSO, Pentadbir Sistem ICT

pengubahsuaian tanpa kebenaran, tindakan yang tidak disengajakan, atau penyalahgunaan aset ICT. Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT.

(b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi.

(c) Persekitaran perkakasan yang digunakan bagi tujuan pembangunan (*development*) atau pementasan (*staging*) sistem aplikasi dan produksi (*production*) hendaklah diasingkan.

(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.

5.7.4 Tanggungjawab Pengurusan

Kawalan keselamatan ini diwujudkan bagi memastikan pengurusan dan warga UM memahami peranan serta memenuhi tanggungjawab dalam keselamatan maklumat.

(1) Tanggungjawab Pengurusan	Tanggungjawab
Pelaksanaan PKS dilaksanakan oleh PE ICT dan disokong oleh PP ICT, ICTSO. Dokumen ini mestilah dipatuhi oleh semua warga UM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Universiti. PP ICT hendaklah memastikan semua warga UM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Universiti supaya mematuhi dan mengamalkan keselamatan maklumat yang ditetapkan.	PE ICT, PP ICT, ICTSO

5.7.5 Hubungan dengan Pihak Berkuasa

UM perlu mewujud dan mengekalkan hubungan baik dengan pihak berkuasa yang berkaitan bagi memastikan pertukaran maklumat yang sesuai dapat dilaksanakan secara berterusan. Ini adalah penting untuk menyokong pematuhan terhadap keperluan keselamatan maklumat selaras dengan kehendak pihak berkuasa penguatkuasaan undang-undang, kawal selia dan penyeliaan yang berkenaan.

(1) Hubungan dengan Pihak Berkuasa	Tanggungjawab
Hubungan baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab UM. (b) Mewujud dan mengemas kini senarai pihak berkuasa perundangan atau pihak yang dihubungi semasa kecemasan	Pentadbir Sistem ICT

seperti pihak luaran perkhidmatan, utiliti, kecemasan, keselamatan dan kesihatan.

(c) Melaporkan sebarang insiden keselamatan maklumat dengan segera mengikut prosedur yang ditetapkan.

5.7.6 Hubungan dengan Kumpulan Berkepentingan Khas

UM hendaklah mewujud dan mengekalkan hubungan dengan kumpulan berkepentingan khas, forum keselamatan khusus serta persatuan profesional yang berkaitan, bagi memastikan pertukaran maklumat yang relevan berkaitan keselamatan maklumat dapat dilaksanakan secara berkesan dan berterusan.

(1) Hubungan dengan Kumpulan Berkepentingan Khas	Tanggungjawab
Hubungan baik dengan kumpulan berkepentingan khas, forum keselamatan khusus serta persatuan profesional yang berkaitan diwujudkan dan dikekalkan bagi mencapai perkara berikut: (a) Meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikut perkembangan terkini mengenai keselamatan maklumat; (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;	Pentadbir Sistem ICT

(e) Berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan

(f) Berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.

5.7.7 Risikan Ancaman

Risikan ancaman merupakan satu proses mengumpul, menganalisis dan mentafsir maklumat berkaitan potensi ancaman siber. Ia bagi memastikan kawalan ancaman keselamatan terhadap UM difahami, dianalisis dan kaedah tindakan yang bersesuaian diambil.

(1) Pengurusan Perisikan Ancaman	Tanggungjawab
Universiti perlu menghasilkan maklumat perisikan ancaman dengan mengumpul dan menganalisis maklumat ancaman keselamatan yang berpotensi atau yang memberikan ancaman untuk: (a) Memudahkan tindakan berinformasi untuk mencegah ancaman daripada mendatangkan bahaya kepada Universiti; dan (b) Mengurangkan impak kepada aset maklumat yang terlibat. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memahami ancaman siber dengan mengumpul, menganalisa dan menghasilkan risikan ancaman berkenaan ancaman keselamatan maklumat. (b) Mengenal pasti dan melaksanakan kawalan keselamatan yang bersesuaian.	UMCERT

(c) Mengumpul dan menganalisa maklumat berkenaan dengan tiga (3) bidang ancaman keselamatan maklumat iaitu, perisikan ancaman strategik, perisikan ancaman taktikal dan perisikan ancaman operasi.	

5.7.8 Keselamatan Maklumat dalam Pengurusan Projek

Kawalan ini diwujudkan bagi memastikan risiko keselamatan maklumat yang berkaitan dengan projek ditangani dengan berkesan dalam pengurusan projek sepanjang kitaran hayat projek.

(1) Keselamatan Maklumat dalam Pengurusan Projek	**Tanggungjawab**
Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek tanpa mengira kompleksiti, saiz, tempoh, disiplin atau bidang. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Keselamatan maklumat perlu diintegrasikan dalam setiap pengurusan projek. (b) Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan. (c) Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan yang diperlukan. (d) Penyediaan spesifikasi projek hendaklah memasukkan ciri-ciri keselamatan yang telah ditetapkan. (e) Kesesuaian pertimbangan dan aktiviti keselamatan maklumat hendaklah disusuli	Pengurus Projek, Pentadbir Rangkaian, Pentadbir Pusat Data, Pentadbir Sistem Aplikasi, Pentadbir Keselamatan ICT

pada peringkat yang telah ditetapkan seperti jawatankuasa teknikal projek atau jawatankuasa pemandu projek.

(f) Peranan dan tanggungjawab keselamatan maklumat projek hendaklah ditakrif dan ditentukan dengan jelas.

5.7.9 Inventori Maklumat Inventori dan Aset yang Lain Berkaitan

Kawalan ini adalah untuk memastikan pengurusan maklumat dan aset dikenal pasti, dikelaskan, direkodkan, diselenggarakan dan penempatan ditetapkan untuk perlindungan keselamatan.

(1) Pengurusan Maklumat Inventori dan Aset	**Tanggungjawab**
Semua maklumat dan aset ICT di UM hendaklah diuruskan mengikut pekeliling atau tatacara yang berkuat kuasa. Perkara berikut perlu dipatuhi dalam menguruskan maklumat inventori dan aset: (a) Memastikan semua aset ICT dikenal pasti, diklasifikasi, didokumen, diselenggara dan dilupuskan mengikut arahan dan peraturan yang berkuat kuasa. (b) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja. Pertukaran pemilik hendaklah dilaksanakan sekiranya terdapat perubahan. (c) Memastikan inventori maklumat dan aset lain yang berkaitan aset adalah tepat, terkini dan konsisten.	Pegawai Aset, Pemilik Aset

(2) Pemilikan Aset	Tanggungjawab
Setiap aset milik UM hendaklah diselenggara mengikut arahan dan peraturan yang berkuat kuasa. Pemilik Aset ICT bertanggungjawab mematuhi perkara berikut: (a) Memastikan semua aset ICT didaftarkan dan dikemas kini dalam senarai inventori, serta diklasifikasikan mengikut klasifikasi yang ditetapkan. (b) Mengesahkan lokasi aset ICT yang ditempatkan. (c) Memastikan semua aset dipelihara dan diselenggara dengan baik. (d) Mengenal pasti dan mengkaji semula capaian ke atas aset penting secara berkala berdasarkan kawalan yang ditetapkan. (e) Memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapus atau dilupuskan. (f) Sebarang aset ICT yang perlu dibawa keluar atas urusan rasmi perlu mendapatkan kelulusan.	Pemilik Aset

5.7.10 Penggunaan Maklumat yang Boleh Diterima dan Aset yang Berkaitan

Kawalan ini adalah untuk memastikan setiap maklumat dan aset ICT yang berkaitan dilindungi, diguna dan dikendalikan dengan sewajarnya.

(1) Penggunaan Aset yang Dibenarkan	Tanggungjawab
Memastikan penggunaan aset untuk tujuan rasmi dan mengikut fungsi sebenar yang telah ditetapkan oleh Universiti.	Pemilik Aset

(2) Pengendalian Aset	Tanggungjawab
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, membuat salinan, menghantar, menyampai, mengubah dan menghapus perlu mengambil kira perkara berikut: (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan. (b) Memeriksa dan menentukan maklumat adalah tepat dan lengkap dari semasa ke semasa. (c) Menentukan maklumat sedia untuk digunakan. (d) Mematuhi piawaian, prosedur dan garis panduan keselamatan yang berkuat kuasa.	Pegawai Aset, Pemilik Aset

5.7.11 Pemulangan Aset

Kawalan ini adalah untuk memastikan proses pemulangan aset ICT dilaksanakan apabila berlaku perubahan dan penamatan perkhidmatan, kontrak atau perjanjian.

(1) Pemulangan Aset ICT	Tanggungjawab
Semua Aset ICT, termasuk aset maklumat seperti data dalam CD, pemacu pena (*pendrives*) dan peranti media mudah alih lain hendaklah dipulangkan atau dipadamkan secara selamat mengikut kesesuaian berdasarkan senario berikut: (a) Pertukaran penempatan atau tugasan kerja; (b) Bersara;	Pegawai Aset, Pemilik Aset

(c) Meninggal dunia;

(d) Ditamatkan perkhidmatan;

(e) Tamat kontrak atau perjanjian; dan

(f) Mendapat arahan Ketua.

Setiap perubahan atau penamatan hendaklah didokumentasikan bagi memastikan semua aset ICT dikembalikan kepada UM. Perkara berikut perlu dipatuhi:

(a) Mengenal pasti dan mendokumentasikan semua maklumat dan aset ICT yang perlu dipulangkan atau dipadamkan.

(b) Menghalang sebarang penyalinan maklumat yang tidak dibenarkan oleh pemilik aset yang berada dalam tempoh penamatan sepanjang tempoh notis dan selepasnya.

(c) Memastikan prosedur pemulangan dan perpindahan Aset ICT kepada UM dilaksanakan mengikut tatacara yang berkuat kuasa.

5.7.12 Klasifikasi Maklumat

Kawalan klasifikasi maklumat adalah untuk memastikan pengenalpastian dan pemahaman tentang keperluan perlindungan maklumat selaras dengan kepentingannya kepada UM.

(1) Pengelasan Maklumat	Tanggungjawab
Data dan maklumat perlu diklasifikasikan mengikut keperluan keselamatan maklumat UM yang telah ditetapkan dalam Arahan Keselamatan dan Polisi Pengurusan Maklumat Rasmi Universiti Malaya.	Pegawai Aset

Pengkelasan maklumat terdiri daripada aktiviti penentuan klasifikasi maklumat serta penentuan peringkat keselamatan maklumat. Klasifikasi maklumat terdiri daripada maklumat rahsia dan maklumat rasmi, manakala peringkat keselamatan maklumat terdiri daripada rahsia besar, rahsia, sulit, terhad, dan terbuka.	

5.7.13 Pelabelan Maklumat

Kawalan keselamatan ini bagi memudahkan komunikasi klasifikasi maklumat dan menyokong automasi pemprosesan dan pengurusan maklumat.

(1) Pelabelan Maklumat	Tanggungjawab
Peringkat keselamatan maklumat hendaklah ditandakan mengikut klasifikasi dokumen, lokasi dan format yang ditetapkan oleh arahan, peraturan atau prosedur yang berkuat kuasa.	Pemilik Aset

5.7.14 Pemindahan Maklumat

Kawalan pemindahan maklumat bertujuan untuk memastikan keselamatan perpindahan/pertukaran data, maklumat dan sistem ICT dengan pihak luar terjamin.

(1) Pengurusan Pemindahan Maklumat	Tanggungjawab
Prosedur pemindahan data dan maklumat disediakan bagi memastikan keselamatan perpindahan/pertukaran data, maklumat dan sistem ICT dengan pihak ketiga terjamin. Pemindahan maklumat boleh dilaksanakan melalui medium elektronik atau media storan fizikal.	Pentadbir Sistem ICT, Staf, Pelajar

Perkara berikut perlu dipatuhi dalam pelaksanaan pemindahan maklumat:

(a) Dasar, prosedur dan kawalan pemindahan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan maklumat melalui sebarang jenis kemudahan komunikasi.

(b) Terma pemindahan data, maklumat dan aset dengan pihak luar hendaklah dimasukkan dalam perjanjian.

(c) Media yang mengandungi data, maklumat dan perisian perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan maklumat.

(d) Memastikan maklumat yang terdapat dalam e-mel elektronik dilindungi sebaik-baiknya.

(e) Penghantaran dokumen terperingkat mesti menggunakan medium penghantaran rasmi Universiti.

(f) Sebarang pemindahan maklumat hendaklah direkodkan bagi tujuan pengesanan.

(g) Menggunakan kaedah pengesahan yang selamat bagi pemindahan maklumat menggunakan rangkaian awam.

(h) Memastikan pemindahan maklumat melalui media storan seperti storan awan (*cloud storage*), pemacu keras (*hard disk*), pemacu kilat USB (USB *flash drive*) dan media storan lain berada dalam keadaan

baik, selamat, terjamin kerahsiaan, integriti dan ketersediaan untuk digunakan.

Perkongsian data secara dalaman atau pihak luar juga melibatkan pengendalian e-mel UM. Perkara yang perlu dipatuhi dalam pengendalian e-mel adalah seperti garis panduan yang berkuat kuasa.

5.7.15 Kawalan Capaian

Kawalan capaian bertujuan untuk memastikan akses yang dibenarkan dan menghalang capaian yang tidak dibenarkan kepada maklumat dan aset lain yang berkaitan.

(1) Keperluan Kawalan Capaian	Tanggungjawab
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna. Peraturan kawalan capaian hendaklah diwujud, didokumen dan disemak secara berkala berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Perkara yang perlu dipatuhi bagi kawalan capaian adalah seperti berikut: (a) Menghadkan akses kepada maklumat dan kemudahan pemprosesan maklumat kepada pihak yang dibenarkan mengikut keperluan tugasan dan berdasarkan prinsip perlu mengetahui (*need-to-know-basis*). (b) Hak capaian hendaklah sentiasa dikawal, dipantau dan dikemas kini secara berkala atau mengikut keperluan perkhidmatan dan keselamatan.	Pentadbir Rangkaian, Pentadbir Pusat Data, Pentadbir Sistem Aplikasi, Pentadbir Keselamatan ICT

(2) Capaian Pengguna	Tanggungjawab
Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna yang memerlukan akses pentadbir secara fungsian atau teknikal kepada sistem aplikasi, peranti rangkaian, pelayan dan perkhidmatan ICT mesti mendapatkan kelulusan serta mematuhi prosedur dan panduan yang berkuat kuasa. (b) Hanya akaun yang diperuntukkan boleh digunakan bagi tujuan capaian. Pemilikan akaun pengguna bukanlah hak mutlak individu dan ia tertakluk kepada arahan atau peraturan yang berkuat kuasa. Akaun boleh ditarik balik jika disalah guna. (c) Penggunaan akaun milik orang lain atau perkongsian akaun adalah dilarang. (d) Hak capaian akaun pentadbir hendaklah disemak dan dikemas kini secara berkala atau mengikut keperluan. (e) Akses kepada sistem aplikasi, pangkalan data, pelayan dan peranti rangkaian hanya dibenarkan kepada individu yang disenaraikan dalam Senarai Kawalan Akses Berasaskan Peranan (RBAC).	Pentadbir Rangkaian, Pentadbir Pusat Data, Pentadbir Sistem Aplikasi, Pentadbir Keselamatan ICT, Staf, Pembekal
(3) Capaian Rangkaian	**Tanggungjawab**
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat melalui perkara berikut:	Pentadbir Rangkaian

(a) Mewujudkan segmen rangkaian yang bersesuaian bagi membezakan antara rangkaian UM dan rangkaian awam.

(b) Mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna dengan menggunakan peralatan yang sesuai.

(c) Memantau dan menguatkuasakan kawalan capaian terhadap perkhidmatan rangkaian ICT.

(d) Mengasingkan capaian mengikut kumpulan perkhidmatan maklumat, pengguna dan sistem maklumat dalam rangkaian.

(e) Menetapkan peraturan (*policy*) bagi rangkaian yang dikongsi (*shared networks*), terutama yang keluar daripada rangkaian UM.

(4) Capaian Jarak Jauh	**Tanggungjawab**
Perkara yang perlu dipatuhi bagi capaian jarak jauh adalah seperti berikut: (a) Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada Ketua. Pengguna yang diberi hak adalah bertanggungjawab sepenuhnya ke atas penggunaannya. (b) Capaian jarak jauh hendaklah menggunakan kemudahan yang disediakan oleh Universiti dan mematuhi peraturan yang berkuat kuasa. (c) Kaedah pengesahan yang sesuai seperti VPN atau kaedah-kaedah lain perlu	Pentadbir Rangkaian, Pentadbir Pusat Data, Pentadbir Sistem Aplikasi, Pentadbir Keselamatan ICT, Staf, Pembekal

dilaksanakan untuk capaian jarak jauh (*remote*). (d) Capaian fizikal dan logikal ke atas kemudahan port diagnostik atau konfigurasi jarak jauh hendaklah dikawal.	
(5) Capaian Sistem Aplikasi	**Tanggungjawab**
Kawalan capaian terhadap sistem aplikasi adalah penting untuk melindungi kerahsiaan, integriti dan ketersediaan maklumat. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Capaian ke sistem aplikasi (*Root/Super-User/Super Admin*) hendaklah diberikan berdasarkan prinsip RBAC dan keperluan tugasan yang diluluskan. (b) Pemberian, pengemaskinian dan penamatan hak capaian hendaklah melalui proses yang didokumen dan dikawal, termasuk rekod permohonan dan kelulusan. (c) Capaian kepada aplikasi yang mengandungi maklumat sensitif atau sulit hendaklah dihadkan kepada pengguna yang diberi kuasa sahaja. (d) Penggunaan kaedah pengesahan yang selamat seperti kata laluan kompleks, pengesahan dua faktor atau sebarang kaedah lain yang ditetapkan adalah diwajibkan mengikut tahap risiko aplikasi. (e) Akaun pengguna hendaklah disemak dan dikemas kini secara berkala atau berdasarkan keperluan.	Pentadbir Pusat Data, Pentadbir Sistem Aplikasi, Staf, Pembekal

(f) Akaun yang tidak aktif melebihi tempoh yang ditetapkan hendaklah dinyahaktif secara automatik.

(g) Perkongsian akaun bagi tujuan capaian aplikasi adalah dilarang.

(h) Rekod log capaian dan aktiviti pengguna hendaklah diaktifkan bagi aplikasi kritikal dan disemak secara berkala untuk tujuan pengesanan aktiviti tidak sah.

(6) Capaian Internet	**Tanggungjawab**
Kawalan capaian internet adalah untuk memastikan hanya pengguna yang dibenarkan menggunakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan Internet di UM hendaklah dipantau secara berterusan bagi memastikan ia digunakan untuk capaian yang dibenarkan sahaja. Kawalan ini akan dapat melindungi daripada sebarang bentuk ancaman ke atas rangkaian UM. (b) Penggunaan Internet hendaklah untuk kegunaan rasmi sahaja. UM berhak menentukan pengguna yang dibenarkan menggunakan capaian Internet atau sebaliknya.	Pentadbir Rangkaian, Pentadbir Keselamatan ICT, Staf, Pembekal

5.7.16 Pengurusan Identiti

Kawalan ini bertujuan untuk memastikan setiap individu dan sistem yang mengakses maklumat dan aset Universiti dikenal pasti secara unik, bagi membolehkan pemberian hak akses yang bersesuaian dan terkawal.

(1) Proses Pengurusan Identiti	Tanggungjawab
Proses pengurusan identiti perlu memastikan perkara berikut dipatuhi: (a) Memastikan ID pengguna adalah unik dan pengguna bertanggungjawab ke atas akaun tersebut selepas pengesahan penerimaan dibuat; (b) Memastikan identiti yang diberikan kepada lebih dari seorang individu (identiti bersama) hanya dibenarkan jika ada keperluan dan tertakluk kepada kelulusan serta direkodkan; (c) Memastikan perkakasan yang memerlukan ID pengguna mendapatkan kelulusan serta pengawasan berterusan; (d) Merekodkan semua penggunaan dan pengurusan identiti pengguna; (e) Pewujudan ID pengguna hendaklah mendapat sokongan oleh Ketua; (f) Membatal, menamat dan menukar peranan akaun pengguna berdasarkan pemakluman oleh Ketua. (g) Proses semakan akses pengguna perlu dilaksanakan untuk mengkaji semula kebenaran dan pembatalan capaian pengguna ke atas semua aplikasi dan perkhidmatan; dan (h) Dilarang menggunakan nama atau menyamar sebagai individu lain dalam mana-mana perkhidmatan dalam talian.	Pentadbir Sistem ICT

(2) Prosedur Penyediaan atau Pembatalan Akses	Tanggungjawab
Prosedur bagi penyediaan atau pembatalan akses adalah berdasarkan prosedur yang berkuat kuasa. Perkara berikut perlu dipatuhi: (a) Memastikan identiti yang diwujudkan memenuhi keperluan tugasan berkaitan; (b) Mengesahkan identiti pengguna yang memohon sebelum pewujudan ID pengguna; (c) Mewujudkan ID pengguna; (d) Mengkonfigurasi dan mengaktifkan ID pengguna; dan (e) Menyediakan atau membatalkan hak akses berdasarkan kelulusan atau pemakluman.	Pentadbir Sistem ICT

5.7.17 Maklumat Pengesahan

Kawalan ini adalah bertujuan untuk memastikan pengesahan entiti yang betul bagi mengelakkan kegagalan capaian maklumat.

(1) Sistem Pengurusan Kata Laluan	Tanggungjawab
Sistem pengurusan kata laluan hendaklah mematuhi perkara berikut: (a) Penjanaan kata laluan peribadi sementara yang unik bagi setiap individu semasa proses pendaftaran. Pengguna diwajibkan menukar kata laluan apabila log masuk kali pertama. (b) Menghantar kata laluan kepada pengguna dengan cara yang selamat.	Pentadbir Rangkaian, Pentadbir Pusat Data, Pentadbir Sistem Aplikasi, Pentadbir Keselamatan ICT, Pemilik Proses

(c) Kata laluan default bagi Pembekal perlu ditukar serta-merta selepas selesai pemasangan sistem, perkakasan atau perisian.

(d) Kata laluan individu hendaklah diwujudkan bagi setiap pengguna teknikal atau pengguna akhir yang mengakses pelayan/ peranti rangkaian/ sistem aplikasi/ perisian.

(e) Menghadkan bilangan maksimum cubaan log masuk kepada lima (5) kali sahaja bagi mengelakkan capaian tidak sah. Selepas mencapai had maksimum, capaian akan disekat sehingga ID pengguna diaktifkan semula.

(f) Menguatkuasakan penggunaan kata laluan yang kukuh mengikut cadangan amalan baik.

(g) Kata laluan tidak dipaparkan di skrin semasa dimasukkan (contoh menggunakan simbol atau bintang).

(h) Kata laluan hendaklah disimpan dan dihantar dalam bentuk yang dilindungi menggunakan teknik seperti penyulitan dan *hashing*.

(i) Penggunaan Pengesahan Pelbagai Faktor (*Multi Factor Authentication*, MFA) adalah digalakkan.

(2) Tanggungjawab Pengguna	Tanggungjawab
Setiap individu yang mempunyai akses hendaklah memastikan perkara berikut: (a) Memilih kata laluan yang kukuh seperti berikut: (i) Mengandungi sekurang-kurangnya minimum lapan (8) gabungan aksara iaitu huruf besar, huruf kecil, simbol dan angka (contoh: a-z, A-Z, 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?/); (ii) Tidak menggunakan perkataan kamus, atau perkataan dalam mana-mana bahasa, slang, dialek, istilah khusus; (iii) Tidak berdasarkan maklumat peribadi seperti nama, nombor telefon, tarikh lahir, ahli keluarga dan seumpamanya; (iv) Tidak menggunakan corak perkataan atau nombor yang boleh dijangka seperti aaabbb, qwerty, zyxwvuts, 123321, atau perkataan dieja secara terbalik; dan (v) Mencipta kata laluan yang kukuh berdasarkan frasa unik seperti tajuk lagu atau afirmasi. Sebagai contoh, frasa "This May Be One Way To Remember", kata laluan "TmB1w2R!" atau "Tmb1W>r~" atau variasi lain yang sesuai. (b) Melindungi kata laluan dengan cara berikut: (i) Kata laluan adalah sulit, dan ia hendaklah diingat dan TIDAK BOLEH	Pengguna

dicatat, disimpan atau didedahkan dengan apa cara sekalipun;

(ii) Merahsiakan kata laluan dan tidak boleh dikongsikan dengan sesiapa melainkan ID pengguna bersama yang diberikan kebenaran sahaja;

(iii) Penggunaan fungsi “ingat kata laluan” (*remember password*) adalah tidak dibenarkan pada peranti atau komputer Universiti;

(iv) Tidak menggunakan kata laluan lalai (*default*) akaun; dan

(v) Tidak menggunakan kata laluan yang sama untuk akaun yang berbeza (contohnya akaun sistem aplikasi, pelayan, rangkaian).

(c) Kata laluan mesti ditukar secara berkala sekurang-kurangnya sekali setahun.

(d) Menukar kata laluan serta-merta dan melaporkan kejadian kepada UMCERT apabila disyaki berlaku kebocoran kata laluan atau dikompromi.

(e) Menggunakan pengurusan identiti secara berpusat yang selamat seperti Direktori Aktif (*Active Directory*), atau tidak menggunakan kata laluan yang sama untuk perkhidmatan dan sistem yang berlainan.

5.7.18 Hak Akses

Kawalan hak akses kepada maklumat dan aset lain yang berkaitan perlu disedia, disemak, diubah suai dan dikeluarkan mengikut peraturan atau

garis panduan yang berkuat kuasa. Ia bagi memastikan hak akses kepada maklumat dan aset lain dibenarkan mengikut keperluan.

(1) Pendaftaran dan Pembatalan Hak Akses	Tanggungjawab
Proses pendaftaran atau pembatalan hak akses fizikal dan logikal yang diberikan adalah seperti yang berikut: (a) Mendapatkan kebenaran daripada pemilik maklumat dan aset lain yang berkaitan untuk digunakan; (b) Mengambil kira polisi atau peraturan khas berkaitan hak akses; (c) Memastikan pengasingan peranan hak akses untuk mengelakkan percanggahan; (d) Memastikan hak akses dihentikan apabila pengguna tidak perlu mengakses maklumat; (e) Memberi hak akses sementara untuk staf kontrak atau staf yang memerlukan; (f) Akaun bagi kontraktor/penggunaan sementara mesti dinyahaktifkan 30 hari selepas kontrak/perjanjian/projek tamat. Pengesahan adalah tanggungjawab penjaga proses/peralatan. (g) Mengesahkan tahap akses yang diberikan mengikut had capaian dan selari dengan keperluan keselamatan maklumat lain; (h) Memastikan bahawa hak akses diaktifkan selepas diluluskan; (i) Menyelenggarakan rekod hak akses secara berpusat;	Pentadbir Rangkaian, Pentadbir Pusat Data, Pentadbir Sistem Aplikasi, Pentadbir Keselamatan ICT

(j) Melaksanakan perubahan hak akses pengguna yang telah bertukar peranan atau bertukar keluar; (k) Menamatkan atau mengemas kini hak akses fizikal dan/atau logikal kepada sistem, pelayan, peranti rangkaian serta premis universiti dalam tempoh yang ditetapkan apabila akses tersebut tidak lagi diperlukan; dan (l) Menyelenggarakan rekod perubahan hak akses fizikal dan logikal pengguna.	
(2) Semakan Hak Akses	**Tanggungjawab**
Semakan berkala terhadap hak akses perlu dilaksanakan seperti perkara berikut: (a) Selepas berlaku perubahan dalam UM seperti pertukaran kerja, kenaikan pangkat, penurunan pangkat atau penamatan; (b) Pengesahan hak akses istimewa (*privileged access rights*) selepas diluluskan; dan (c) Membuat semakan hak akses pengguna secara berkala atau sekurang-kurangnya **satu (1) kali setahun** atau mengikut keperluan. Pengesahan hak akses pengguna sistem aplikasi adalah tanggungjawab pemilik proses (*process owner*).	Pentadbir Rangkaian, Pentadbir Pusat Data, Pentadbir Sistem Aplikasi, Pentadbir Keselamatan ICT
(3) Pertimbangan Sebelum Pertukaran atau Penamatan Perkhidmatan	**Tanggungjawab**
Hak akses pengguna kepada maklumat dan aset lain yang berkaitan perlu disemak,	Pentadbir Rangkaian, Pentadbir Pusat Data,

diselaras atau dinyahaktifkan sebelum sebarang pertukaran atau penamatan berdasarkan penilaian faktor risiko seperti yang berikut: (a) Pengguna atau pengurusan mengemukakan sebarang permohonan pertukaran atau penamatan; (b) Tanggungjawab semasa pengguna; dan (c) Nilai aset yang boleh dicapai.	Pentadbir Sistem Aplikasi, Pentadbir Keselamatan ICT

5.7.19 Keselamatan Maklumat dengan Pembekal

Kawalan ini merangkumi proses dan prosedur yang perlu ditakrif dan dilaksanakan untuk mengurus risiko keselamatan maklumat yang berkaitan dengan penggunaan produk atau perkhidmatan pembekal. Kawalan ini bertujuan untuk mengekalkan tahap keselamatan maklumat yang dipersetujui dalam hubungan dengan pembekal.

(1) Keselamatan Maklumat untuk Hubungan dengan Pembekal	**Tanggungjawab**
Keperluan keselamatan maklumat hendaklah ditakrif, dilaksana, dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset ICT UM. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengenal pasti dan mendokumentasikan maklumat pembekal. (b) Memilih pembekal mengikut klasifikasi maklumat dan perkhidmatan yang disediakan oleh pembekal selaras dengan polisi atau peraturan yang berkuat kuasa.	Pengurus Projek, Pemilik Projek, Pentadbir Kewangan

(c) Menyatakan keperluan minimum keselamatan maklumat bagi setiap pembekal dalam dokumen perjanjian.

(d) Pembekal yang terpilih hendaklah menandatangani Perjanjian Tanpa Pendedahan (*Non-Disclosure Agreement,* NDA) semasa berurusan dengan maklumat sulit dan tidak boleh dalam apa-apa cara, sama ada secara langsung atau tidak, mendedahkan sebarang maklumat sulit kepada mana-mana pihak tanpa kebenaran bertulis daripada UM.

(e) Menentukan jenis-jenis obligasi kepada pembekal.

(f) Mengawal dan memantau capaian pembekal.

(g) Mengenal pasti maklumat, perkhidmatan dan infrastruktur fizikal yang boleh diakses, dipantau, dikawal atau digunakan oleh pembekal.

(h) Mengenal pasti risiko dan keperluan keselamatan maklumat serta kemudahan pemprosesan maklumat, seterusnya melaksanakan kawalan yang sesuai sebelum memberikan kebenaran akses atau penggunaan kepada pihak pembekal/luar.

(i) Bekerjasama dengan Ketua PTj atau wakil mengenai kerja-kerja yang perlu dilaksanakan di PTj oleh pembekal.

(j) Memantau pematuhan dan keperluan keselamatan maklumat yang ditetapkan kepada semua pembekal.

(k) Memastikan setiap projek yang dilaksanakan mengikut arahan atau peraturan yang berkuat kuasa.

Pengurus Projek atau Pemilik Projek hendaklah memastikan keselamatan maklumat semasa penamatan perkhidmatan pembekal merangkumi perkara berikut:

(a) Pembatalan hak capaian;

(b) Pengendalian maklumat;

(c) Menentukan pemilikan harta intelek yang dibangunkan semasa perjanjian dilaksanakan;

(d) Pemindahan maklumat sekiranya berlaku pertukaran pembekal atau penyumberan;

(e) Pengurusan rekod;

(f) Pemulangan aset;

(g) Pelupusan maklumat dan aset lain berkaitan secara selamat; dan

(h) Keperluan kerahsiaan yang berterusan.

5.7.20 Keselamatan Maklumat dalam Perjanjian Pembekal

Keperluan keselamatan maklumat yang berkaitan hendaklah diwujudkan dan dipersetujui dengan pembekal berdasarkan jenis hubungan. Ianya bagi mengekalkan tahap keselamatan maklumat yang dipersetujui dalam hubungan bersama pembekal.

(1) Keselamatan Maklumat ke Atas Pembekal	Tanggungjawab
Perjanjian dengan pembekal perlu diwujudkan bagi memastikan pemahaman yang jelas antara UM dan pembekal mengenai tanggungjawab kedua-dua pihak. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pemilihan pembekal perlu mematuhi Dokumen Induk Pengurusan Kewangan UM yang berkuat kuasa. (b) Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi. (c) Menetapkan maklumat yang akan diberikan atau dicapai, serta kaedah penyediaan atau capaian maklumat tersebut. (d) Pembekal hendaklah mematuhi pengklasifikasian maklumat yang ditetapkan. (e) Memastikan pematuhan keperluan undang-undang, peraturan kawal selia, dan kontrak termasuk perlindungan data, pengendalian maklumat pengenalan peribadi (PII), hak harta intelek dan hak cipta, serta penjelasan bagaimana pematuhan itu dipastikan. (f) Mewajibkan pembekal melaksanakan set kawalan yang dipersetujui, termasuk	Pengurus Projek, Pemilik Projek, Pembekal

kawalan capaian, semakan prestasi, pemantauan, pelaporan, pengauditan, dan pematuhan kepada keperluan keselamatan maklumat UM.

(g) Menetapkan keperluan keselamatan maklumat minimum bagi infrastruktur ICT pembekal, berdasarkan jenis maklumat dan jenis capaian selaras dengan keperluan perniagaan dan penilaian risiko UM. Tindakan penggantirugian dan pemulihan hendaklah diambil sekiranya kontraktor gagal memenuhi keperluan tersebut.

(h) Menetapkan tanggungjawab pembekal dalam aspek ganti rugi dan pemulihan sekiranya gagal memenuhi keperluan kontrak.

(i) Menyenaraikan nama staf pembekal, termasuk subkontraktor dan rakan kongsi yang diberi kuasa untuk capaian atau penerimaan maklumat serta kaedah pengurusan penyahaktifan capaian.

(j) Menetapkan keperluan dan prosedur pengurusan insiden keselamatan maklumat termasuk pemberitahuan dan kerjasama dalam proses pemulihan insiden.

(k) Menetapkan keperluan latihan dan kesedaran berkaitan prosedur keselamatan maklumat seperti pengendalian insiden dan kebenaran capaian.

(l) Menetapkan keperluan saringan terhadap kakitangan pembekal, termasuk tanggungjawab pembekal melaksanakan saringan dan pemberitahuan jika wujud keraguan.

(m) Memastikan penyediaan bukti dan jaminan pengesahan pihak ketiga terhadap keperluan keselamatan maklumat, termasuk laporan bebas berkaitan keberkesanan kawalan.

(n) Memastikan hak pengauditan proses dan kawalan pembekal berkaitan perjanjian.

(o) Jawatankuasa Penilaian Teknikal boleh melaksanakan penilaian teknikal atau menilai laporan penilaian pihak ketiga yang dikemukakan oleh pembekal.

(p) Mewajibkan pembekal menyediakan laporan berkala berkenaan keberkesanan kawalan serta mengambil tindakan pembetulan secara tepat pada masanya.

(q) Memastikan pelaksanaan kawalan keselamatan fizikal, pengurusan konflik, penyelesaian kecacatan, serta kawalan pemindahan maklumat mengikut klasifikasi maklumat.

(r) Menyediakan pelan sandaran mengikut keperluan dari aspek kekerapan, jenis dan lokasi simpanan.

(s) Memastikan kemudahan pemulihan bencana tidak tertakluk kepada ancaman yang sama dengan lokasi utama, serta

mempertimbangkan pelaksanaan kawalan sandaran (*fallback control*).

(t) Memastikan wujudnya proses pengurusan perubahan, termasuk keperluan pemberitahuan awal kepada UM dan hak UM untuk menolak perubahan.

(u) Menetapkan klausa penamatan termasuk pengurusan rekod, pemulangan aset, pelupusan maklumat secara selamat, dan pematuhan terhadap kerahsiaan berterusan selepas penamatan kontrak.

(v) Menyemak laporan penilaian pihak ketiga yang dikemukakan oleh syarikat pembekal berdasarkan faktor berikut:

  (i) Badan penilai bebas dan berintegriti.

  (ii) Badan penilai mempunyai kompetensi.

  (iii) Kriteria penilaian yang diguna pakai.

  (iv) Parameter pengujian yang dijalankan.

(w) Menetapkan kaedah pelupusan maklumat Universiti yang disimpan oleh pembekal dengan selamat sebaik sahaja ia tidak lagi diperlukan.

(x) Memastikan pembekal bersetuju dan mematuhi semua keperluan keselamatan maklumat yang berkaitan untuk mencapai, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT bagi keperluan UM.

(y) Memastikan semua capaian pembekal dibatalkan dalam tempoh tujuh (7) hari setelah tamat kontrak perkhidmatan.

5.7.21 Pengurusan Keselamatan Maklumat dalam Rantaian Bekalan ICT

Kawalan keselamatan ini bertujuan untuk mengekalkan tahap keselamatan maklumat yang dipersetujui dalam hubungan dengan Pembekal.

(1) Kawalan Rantaian Bekalan Maklumat dan Komunikasi	Tanggungjawab
Perjanjian dengan pembekal hendaklah merangkumi keperluan keselamatan maklumat bagi menangani risiko yang berkaitan dengan perkhidmatan ICT dan rantaian bekalan maklumat dan komunikasi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan ICT termasuk awan awam (*public cloud*). (b) Pembekal utama bertanggungjawab memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal lain yang terlibat dalam penyampaian perkhidmatan atau produk. (c) Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa boleh dibekalkan serta beroperasi dengan baik. (d) Melaksanakan proses pemantauan untuk mengesahkan bahawa produk dan perkhidmatan teknologi maklumat dan komunikasi yang diterima memenuhi keperluan keselamatan yang telah ditetapkan.	Pengurus Projek, Pemilik Proses, Pembekal

(e) Memastikan produk ICT mencapai tahap keselamatan yang diperlukan.	
(f) Mewujudkan kawalan perkongsian maklumat untuk meminimumkan risiko kompromi dalam hubungan antara UM dan pembekal.	
(g) Melaksanakan proses khusus untuk mengurus kitaran hayat dan risiko komponen teknologi maklumat dan komunikasi yang telah usang akibat perkembangan teknologi dan ekonomi.	
(2) Penempatan Laman Web secara *Webhosting*	**Tanggungjawab**
Dalam menguruskan penempatan laman web secara *webhosting*, perkara berikut hendaklah dipatuhi:	Ketua PTj, Pentadbir Pusat Data, Pengurus Web
(a) Semua permohonan penempatan laman web secara *webhosting* hendaklah mendapat kelulusan terlebih dahulu.	
(b) Menyediakan infrastruktur ICT yang diperlukan bagi menyokong penempatan laman web, termasuk sumber pelayan (CPU, memori, storan), sijil SSL, nama domain, keperluan akses dan rangkaian, imbasan keselamatan serta pemantauan tahap ketersediaan perkhidmatan.	
(c) Memastikan laman web sentiasa boleh dicapai (24 jam x 7 hari), serta memaklumkan sekiranya berlaku gangguan perkhidmatan.	

(d) Menyediakan redudansi (*redundancy*) laman web berdasarkan keperluan yang ditetapkan.

(e) Melaksanakan penyelenggaraan berkala pelayan *webhosting* seperti penampalan (*patching*), pemasangan SSL, serta pemantauan keselamatan pelayan secara berterusan.

(f) Memastikan kesediaan pelayan web dan pangkalan data sentiasa dalam keadaan optimum untuk menyokong capaian laman web.

Ketua PTj juga memainkan peranan penting dalam memastikan keselamatan maklumat sentiasa terjamin. Perkara yang perlu dipatuhi adalah seperti berikut:

(a) PTj hendaklah melantik pengurus web yang bertanggungjawab mengurus kandungan serta keselamatan laman web.

(b) Pengurus Web bertanggungjawab memasang laman web pada pelayan *webhosting* yang disediakan.

(c) Pengurus Web bertanggungjawab menjaga keselamatan kata laluan yang dibekalkan.

(d) Pengurus Web bertanggungjawab membangun dan mengurus operasi laman web.

(e) Pengurus Web perlu bekerjasama dengan Pentadbir Pusat Data bagi memulihkan data dan perkhidmatan laman web sekiranya berlaku insiden seperti

kehilangan data, kerosakan atau pencerobohan.

(f) Pengurus Web bertanggungjawab melaksanakan sandaran (*backup*) data laman web yang disimpan dalam pelayan *webhosting*.

(g) Pengurus Web hendaklah memantau dan mengemas kini versi bahasa pengaturcaraan, enjin CMS, plugin, dan perisian berkaitan secara berkala.

(h) Pengurus Web bertanggungjawab menyelesaikan isu keselamatan laman web dalam tempoh masa yang ditetapkan. UM berhak menutup laman web sekiranya tiada tindakan pembetulan diambil dalam tempoh yang ditetapkan.

(i) PTj hendaklah mengemukakan permohonan rasmi sekiranya ingin menamatkan perkhidmatan *webhosting* atau menutup laman web.

5.7.22 Pemantauan, Semakan dan Pengurusan Perubahan Perkhidmatan Pembekal

Tujuan utama kawalan ini adalah bagi memastikan pemantauan, penilaian dan pengurusan perubahan dilaksanakan ke atas Pembekal.

(1) Pemantauan dan Penilaian Perkhidmatan Pembekal	**Tanggungjawab**
UM hendaklah sentiasa memantau, mengkaji semula, mengaudit perkhidmatan pembekal secara berkala serta mengurus perubahan dalam amalan risiko keselamatan maklumat pembekal dan penyampaian perkhidmatan.	Pengurus Projek, Pemilik Projek, Pentadbir Sistem ICT

Perkara-perkara yang perlu diambil kira adalah seperti berikut:

(a) Memantau tahap prestasi perkhidmatan untuk mengesahkan pematuhan pembekal terhadap perjanjian perkhidmatan.

(b) Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal serta mengemukakan status kemajuan.

(c) Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.

(2) Pengurusan Perubahan Perkhidmatan Pembekal	**Tanggungjawab**
Sebarang perubahan kepada penyediaan perkhidmatan pembekal, termasuk pengekalan dan penambahbaikan polisi keselamatan maklumat, prosedur dan kawalan, hendaklah diuruskan dengan mengambil kira kepentingan maklumat, sistem dan proses pengoperasian Universiti, serta penilaian semula risiko. Perkara-perkara yang perlu diambil kira adalah seperti berikut: (a) Perubahan dalam perjanjian dengan pembekal. (b) Perubahan yang dilaksanakan oleh UM bagi meningkatkan perkhidmatan selaras dengan pembangunan dan penambahbaikan sistem serta aplikasi, pengubahsuaian dasar, prosedur dan kawalan keselamatan maklumat.	Pengurus Projek, Pemilik Projek, Pentadbir Sistem ICT

(c) Perubahan alat pembangunan dan persekitaran baharu.

(d) Perubahan perkhidmatan pembekal selaras dengan perubahan lokasi fizikal kemudahan perkhidmatan, rangkaian, teknologi baharu, produk baharu, kelengkapan (perkakasan/perisian) baharu, pertukaran pembekal dan subkontraktor.

UM adalah bertanggungjawab ke atas pembekal yang dilantik dengan memastikan perkara berikut dipatuhi:

(a) Memastikan dokumen perjanjian kontrak ditandatangani.

(b) Menyediakan senarai semak projek untuk tujuan pemantauan pelaksanaan projek dalam tempoh yang dirancang.

(c) Berbincang dengan PTj berkaitan skop kerja, mendapatkan persetujuan dan kebenaran bagi pelaksanaan kerja di PTj.

(d) Mengadakan lawatan tapak bersama pembekal untuk penerangan terperinci serta merakam gambar lokasi sebelum kerja dimulakan.

(e) Berada di lokasi bagi memantau pelaksanaan kerja pembekal ICT.

(f) Merakam gambar lokasi selepas kerja disiapkan (jika berkaitan).

(g) Mengenal pasti risiko dan keperluan keselamatan maklumat serta melaksanakan kawalan sewajarnya

sebelum memberi kebenaran akses atau penggunaan kepada pembekal.

(h) Memastikan akses kepada aset ICT UM dibuat berasaskan perjanjian kontrak.

(3) Tanggungjawab Pembekal	**Tanggungjawab**
Pihak pembekal yang berurusan dalam memberikan produk atau perkhidmatan juga bertanggungjawab dengan memastikan perkara berikut dipatuhi: (a) Membaca, memahami dan mematuhi dasar atau polisi yang ditetapkan dalam Dokumen Induk Pengurusan ICT UM. (b) Mengemas kini dan mengemukakan butiran staf projek kepada JTM. (c) Mendaftar dan mendapatkan Pas Pekerja Sementara dari Pejabat Polis Bantuan UM untuk semua staf terlibat. Pas perlu sentiasa dipamerkan semasa berada di kampus UM. (d) Mematuhi peraturan keselamatan yang berkuat kuasa sepanjang tempoh projek (contoh: kerja-kerja pembinaan). (e) Memastikan semua staf memakai pakaian kerja/seragam yang sesuai dan selamat serta memaparkan nama syarikat pada pakaian. (f) Memastikan semua staf memaparkan tag nama masing-masing. (g) Memastikan kerja dilaksanakan mengikut jadual yang dipersetujui. Sebarang perubahan perlu mendapatkan kelulusan bertulis.	Pembekal

(h) Melapor diri kepada pegawai bertanggungjawab sebelum memulakan kerja dan memaklumkan sebelum meninggalkan PTj.

(i) Menjaga tingkah laku, mematuhi peraturan UM termasuk larangan merokok di kampus.

(j) Memastikan semua staf memahami risiko dan ancaman keselamatan serta mengambil langkah pencegahan sewajarnya bagi mengelakkan kemalangan atau kejadian tidak diingini.

(k) Menjaga kebersihan tempat kerja seperti melapik lantai berkarpet dengan plastik sebelum melakukan kerja *drilling*, *hacking*, mengecat dan seumpamanya.

(l) Memasang papan tanda amaran secukupnya di kawasan berkaitan demi keselamatan warga kampus.

(m) Mengurus pembuangan sampah dan sisa kerja dengan cara yang sesuai. Sampah berlebihan atau berbahaya hendaklah dibawa keluar dari UM pada hari yang sama atau sebaik kerja selesai.

(n) Bagi projek melibatkan PTj, perlu mendapatkan pengesahan daripada wakil PTj bahawa kerja yang dilaksanakan telah selesai.

(o) Mengemukakan laporan lengkap berkaitan kerja yang dilaksanakan dalam bentuk bercetak dan digital apabila projek selesai.

(p) Melindungi maklumat UM serta tidak mendedah, mengedar atau menggunakannya tanpa kebenaran bertulis UM.

(q) Mematuhi semua peraturan UM yang dikeluarkan dari semasa ke semasa.

5.7.23 Keselamatan Maklumat bagi Penggunaan Perkhidmatan Awan

Kawalan ini merangkumi proses perolehan, penggunaan, pengurusan dan penamatan perkhidmatan awan harus diwujudkan selaras dengan keperluan keselamatan maklumat UM bertujuan untuk menentukan dan mengurus keselamatan maklumat untuk penggunaan perkhidmatan awan.

(1) Keselamatan Maklumat bagi Penggunaan Perkhidmatan Awan	Tanggungjawab
Pengurusan perkhidmatan awan melibatkan pelbagai aspek teknikal dan pentadbiran bagi memastikan perkhidmatan awan digunakan secara berkesan, selamat dan menepati keperluan Universiti. Penggunaan perkhidmatan awan melibatkan tanggungjawab bersama terhadap keselamatan maklumat serta usaha kolaboratif antara penyedia perkhidmatan awan dan UM selaku pelanggan perkhidmatan awan. Aspek-aspek berikut perlu ditentukan: (a) Keperluan keselamatan maklumat berkaitan dengan penggunaan perkhidmatan awan. (b) Kriteria pemilihan perkhidmatan awan dan skop penggunaannya.	Pembekal, Pemilik Projek

(c) Peranan dan tanggungjawab berkaitan dengan penggunaan dan pengurusan perkhidmatan awan.

(d) Pembahagian kawalan keselamatan maklumat yang diuruskan oleh penyedia perkhidmatan awan dan oleh UM.

(e) Kaedah untuk mendapatkan dan memanfaatkan keupayaan keselamatan maklumat yang disediakan oleh penyedia perkhidmatan awan.

(f) Kaedah untuk mendapatkan jaminan berkaitan kawalan keselamatan maklumat yang dilaksanakan oleh penyedia perkhidmatan awan.

(g) Pengurusan kawalan, antara muka dan perubahan perkhidmatan apabila UM menggunakan pelbagai perkhidmatan awan, terutamanya daripada penyedia perkhidmatan yang berbeza.

(h) Prosedur pengendalian insiden keselamatan maklumat berkaitan penggunaan perkhidmatan awan.

(i) Pendekatan pemantauan, semakan dan penilaian penggunaan berterusan perkhidmatan awan bagi pengurusan risiko keselamatan maklumat.

(j) Prosedur penukaran atau penamatan penggunaan perkhidmatan awan termasuk strategi penamatan perkhidmatan.

(2) Pengurusan Kontrak Perkhidmatan Awan	Tanggungjawab
Perjanjian antara penyedia perkhidmatan awan dan UM sebagai pelanggan perkhidmatan awan hendaklah merangkumi peruntukan-peruntukan berikut bagi memastikan perlindungan data UM dan ketersediaan perkhidmatan dipelihara: (a) Menyediakan penyelesaian berdasarkan piawaian industri berkaitan seni bina dan infrastruktur. (b) Mengurus kawalan capaian perkhidmatan awan selaras dengan keperluan UM. (c) Melaksanakan pemantauan keselamatan dan kawalan penyelesaian perlindungan perisian hasad (*malware*). (d) Memproses dan menyimpan maklumat sensitif UM di lokasi yang diluluskan, termasuk negara, wilayah atau bidang kuasa yang ditetapkan. (e) Menyediakan sokongan berkaitan insiden keselamatan maklumat dalam persekitaran perkhidmatan awan. (f) Memastikan keperluan keselamatan maklumat UM tetap dipatuhi sekiranya perkhidmatan awan disubkontrakkan kepada pihak ketiga, atau menetapkan larangan bagi subkontrak. (g) Menyediakan sokongan dan memastikan ketersediaan perkhidmatan mencukupi dalam tempoh peralihan sekiranya UM menamatkan perkhidmatan awan.	Pembekal, Pemilik Projek

(h) Menyediakan sandaran data dan maklumat konfigurasi serta menguruskan sandaran dengan selamat mengikut keperluan dan kemampuan penyedia perkhidmatan.

(i) Menyerahkan semula maklumat seperti fail konfigurasi, kod sumber, dan data milik UM apabila diminta, sama ada semasa tempoh perkhidmatan atau selepas penamatan perkhidmatan.

Selain itu, UM perlu mempertimbangkan sama ada perjanjian kontrak menetapkan keperluan pemberitahuan awal oleh penyedia perkhidmatan awan sebelum sebarang perubahan yang memberi kesan ketara kepada UM, termasuk:

(a) Perubahan terhadap infrastruktur teknikal seperti penempatan semula, konfigurasi semula, atau perubahan perkakasan dan perisian yang memberi kesan kepada penawaran perkhidmatan.

(b) Pemprosesan atau penyimpanan maklumat dalam bidang kuasa geografi atau undang-undang yang baharu.

(c) Penggunaan atau pertukaran rakan penyedia perkhidmatan awan atau subkontraktor yang sedia ada atau baharu.

5.7.24 Perancangan dan Penyediaan Pengurusan Insiden Keselamatan Maklumat

Kawalan ini disediakan bagi memastikan pengurusan insiden keselamatan maklumat yang dilaksanakan adalah konsisten dan teratur.

(1) Tugas dan Tanggungjawab	Tanggungjawab
Tanggungjawab dan prosedur hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat. Pengendalian insiden keselamatan siber UM adalah berdasarkan kepada Prosedur Pengurusan Insiden Keselamatan Maklumat yang sedang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Memberikan kesedaran berkaitan Prosedur Pengurusan Insiden Keselamatan Maklumat dan hebahan kepada warga UM. (b) Memastikan staf yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan: (i) UMCERT sebagai pengurus tunggal untuk semua aduan dan pelaporan insiden keselamatan siber; dan (ii) Senarai hubungan dengan pihak berkuasa, kumpulan pakar atau platform forum yang berkaitan insiden keselamatan maklumat diwujudkan dan dikemas kini.	UMCERT, Pentadbir Sistem ICT
(2) Prosedur Pengurusan Insiden	**Tanggungjawab**
Pengendalian insiden keselamatan siber UM adalah berdasarkan kepada Prosedur Pengurusan Insiden Keselamatan Maklumat yang sedang berkuat kuasa. Antara perkara yang perlu diambil kira seperti berikut:	UMCERT, Pentadbir Sistem ICT

(a) Penilaian risiko ke atas insiden yang berlaku.

(b) Pemantauan, pengelasan, analisis dan laporan insiden perlu disediakan sama ada secara manual atau melalui sistem.

(c) Memastikan log aktiviti insiden keselamatan direkodkan.

(d) Mengenal pasti punca insiden.

Prosedur pelaporan hendaklah termasuk:

(a) Menyediakan borang pelaporan kejadian keselamatan maklumat untuk tujuan perekodan, rujukan dan pemantauan.

(b) Prosedur yang perlu dilaksanakan sekiranya berlaku kejadian keselamatan maklumat contohnya mencatat dengan serta-merta semua butiran ketidakpatuhan atau pelanggaran polisi, kerosakan yang berlaku, mesej yang dipaparkan di skrin dan segera melaporkannya kepada pegawai bertanggungjawab.

(c) Merujuk kepada proses tindakan tatatertib yang ditetapkan untuk menangani individu yang melakukan pelanggaran keselamatan.

(d) Proses maklum balas yang sesuai untuk memastikan pelapor insiden keselamatan maklumat dimaklumkan tentang keputusan selepas isu tersebut diselesaikan.

5.7.25 Penilaian dan Tindakan Insiden Keselamatan Maklumat

Kawalan ini diwujudkan bagi mengenal pasti kategori dan penilaian berasaskan keutamaan ke atas semua insiden keselamatan maklumat.

(1) Penilaian dan Tindakan Insiden Keselamatan Maklumat	Tanggungjawab
Aktiviti keselamatan maklumat hendaklah dinilai dan dianalisis untuk diklasifikasikan sebagai insiden keselamatan maklumat. Perkara yang perlu diambil kira adalah seperti berikut: (a) Mengenal pasti dan mengesahkan kategori serta keutamaan insiden maklumat; dan (b) Merekod dan menyimpan semua tindakan serta keputusan insiden keselamatan maklumat untuk tujuan rujukan masa hadapan.	UMCERT

5.7.26 Tindak Balas Terhadap Insiden Keselamatan Maklumat

Insiden keselamatan maklumat hendaklah ditangani mengikut prosedur yang didokumenkan bagi membolehkan tindak balas yang cepat dan berkesan terhadap insiden dilaksanakan.

(1) Tindakan Balas pada Insiden Keselamatan Maklumat	Tanggungjawab
Perkara yang perlu diambil kira dalam pengumpulan dan pengurusan pengendalian insiden adalah seperti berikut: (a) Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku. (b) Menjalankan kajian forensik sekiranya perlu.	UMCERT, Pentadbir Sistem ICT

(c) *Escalation* sekiranya perlu.

(d) Memastikan semua aktiviti tindak balas yang terlibat dicatatkan dengan betul untuk analisa susulan.

(e) Memaklumkan insiden keselamatan maklumat yang berlaku atau sebarang butiran berkaitannya kepada pihak yang berkepentingan di dalam dan luar Universiti.

(f) Menghubungi pihak yang berkenaan dengan secepat mungkin.

(g) Menangani kelemahan keselamatan maklumat yang menyebabkan atau menyumbang kepada insiden.

(h) Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti.

(i) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan.

(j) Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan.

(k) Menyediakan tindakan pemulihan segera.

(l) Makluman atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.

5.7.27 Pembelajaran daripada Insiden Keselamatan Maklumat

Pengetahuan yang diperoleh daripada penganalisaan dan penyelesaian kejadian keselamatan yang telah dilaksanakan hendaklah diaplikasikan bagi mengelakkan insiden yang sama berulang.

(1) Pembelajaran daripada Insiden Keselamatan Maklumat	Tanggungjawab
Setiap insiden keselamatan maklumat perlu direkodkan dan penilaian ke atas insiden keselamatan maklumat perlu dilaksanakan untuk memastikan kawalan yang diambil adalah mencukupi atau perlu ditambah. Penilaian insiden yang perlu diambil kira adalah seperti berikut: (a) Menambah baik pelan pengurusan insiden; (b) Mengenal pasti punca insiden yang kerap berlaku bagi melaksanakan kawalan tambahan yang diperlukan untuk mengurangkan risiko; dan (c) Meningkatkan kesedaran keselamatan maklumat kepada warga UM.	UMCERT

5.7.28 Pengumpulan Bukti

UM harus mewujudkan dan melaksanakan prosedur untuk pengenalpastian, pengumpulan, pemerolehan dan pemeliharaan bukti yang berkaitan dengan peristiwa keselamatan maklumat. Ianya bagi pengurusan penyimpanan bukti direkodkan secara konsisten bagi insiden keselamatan maklumat untuk tindakan tatatertib dan undang-undang.

(1) Pengumpulan dan Pengendalian Bukti	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengenal pasti, mengumpul, menyimpan dan melindungi bahan bukti untuk mengelakkan pengubahsuaian tanpa kebenaran;	Pentadbir Keselamatan ICT

(b) Menyimpan jejak audit, sandaran (*backup*) secara berkala dan melindungi integriti bahan bukti; dan

(c) Merekodkan semua bukti insiden selaras dengan tarikh dan masa kejadian.

5.7.29 Keselamatan Maklumat semasa Gangguan

Keselamatan 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.

(1) Perancangan Keselamatan Maklumat dalam Kesinambungan Maklumat	**Tanggungjawab**
UM perlu mengambil kira keperluan dan jangkaan pihak berkepentingan serta pematuhan undang-undang dan peraturan yang berkuat kuasa dalam merancang keselamatan maklumat sebagai sebahagian daripada pengurusan kesinambungan perkhidmatan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Melantik pasukan tadbir urus Pelan Pengurusan Kesinambungan (PKP) Perkhidmatan ICT UM. (b) Menetapkan Pelan PKP ICT UM yang komprehensif dan bersesuaian dengan keperluan Universiti. (c) Mengenal pasti semua perkhidmatan ICT yang terlibat dalam Pelan PKP ICT UM. (d) Melaksanakan Analisis Impak Perniagaan (*Business Impact Analysis,* BIA) dan	ICTSO, DRT ICT, Pentadbir Keselamatan ICT, Pentadbir Pusat Data

Penilaian Risiko terhadap semua perkhidmatan ICT. (e) Membangunkan pelan berkaitan termasuk Pelan Pengurusan Kesinambungan Perkhidmatan ICT, Pelan Komunikasi Krisis, Pelan Pemulihan Bencana ICT dan Pelan Tindak Balas Kecemasan. (f) Melaksanakan program kesedaran dan latihan berkala kepada pasukan PKP dan warga UM. (g) Mengadakan simulasi berkala bagi menguji keberkesanan Pelan PKP ICT dan Pelan Pemulihan Bencana ICT. (h) Melaksanakan penyelenggaraan ke atas pelan-pelan berkaitan bagi memastikan ia sentiasa relevan dan berkesan.	
(2) Pelaksanaan Keselamatan Maklumat dalam Kesinambungan Perkhidmatan	**Tanggungjawab**
UM hendaklah menyedia, mendokumen, melaksana dan menyelenggara proses, prosedur serta kawalan yang sesuai bagi memastikan tahap kesinambungan keselamatan maklumat dapat dikekalkan sekiranya berlaku gangguan atau insiden yang menjejaskan operasi. Perkara-perkara yang perlu dipertimbangkan termasuk: (a) Melaksanakan PKP apabila berlaku gangguan terhadap perkhidmatan ICT kritikal UM yang telah dikenal pasti, berdasarkan pelan-pelan terkini. (b) Melaksanakan sesi pasca insiden (*post-mortem*) selepas berlakunya gangguan	ICTSO, DRT ICT, Pentadbir Keselamatan ICT, Pentadbir Pusat Data

serta mengemas kini pelan-pelan PKP berdasarkan penemuan.

(c) Mengemas kini pelan-pelan PKP sekiranya berlaku perubahan terhadap fungsi kritikal Universiti.

(d) Mengemas kini struktur tadbir urus PKP apabila berlaku pertukaran pegawai, termasuk persaraan atau pertukaran keluar.

(e) Memastikan ahli pasukan dalam PKP memiliki kompetensi yang bersesuaian dengan peranan dan tanggungjawab yang ditetapkan bagi melaksanakan pelan dengan berkesan.

5.7.30 Ketersediaan ICT bagi Kesinambungan Perkhidmatan

Kesediaan ICT hendaklah dirancang, dilaksanakan, diselenggara dan diuji secara berkala bagi memastikan ketersediaan maklumat dan aset ICT yang berkaitan dapat dikekalkan semasa berlakunya gangguan, selaras dengan Pelan Pemulihan Bencana (PPB) Perkhidmatan ICT.

(1) Pengenalpastian Ketersediaan Aset ICT semasa Gangguan	**Tanggungjawab**
Perkara yang perlu diambil kira adalah seperti berikut: (a) Mengenal pasti Objektif Masa Pemulihan (*Recovery Time Objective,* RTO) dan Objektif Titik Pemulihan (*Recovery Point Objective,* RPO) untuk sistem aplikasi kritikal mengikut keutamaan. (b) Menyediakan PPB Perkhidmatan ICT dan memastikan pelan ini diluluskan.	UMCERT, Pentadbir Keselamatan ICT, Pentadbir Pusat Data

(c) Menjalankan pengujian bagi memastikan ketersediaan aset ICT dapat berfungsi semasa gangguan.

(d) Menyediakan senarai lengkap maklumat yang memerlukan sandaran (*backup*) dan lokasi sebenar penyimpanannya.

5.7.31 Keperluan Perundangan dan Kontrak

Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti, didokumen dan dikemas kini bagi memastikan pematuhan terhadap semua keperluan tersebut.

(1) Pengenalpastian Keperluan Perundangan dan Perjanjian Kontrak	Tanggungjawab
Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh semua pihak yang terlibat dalam pembekalan perkhidmatan ICT di UM. Pihak yang melanggar mana-mana klausa dalam *Integrity Pact* boleh ditamatkan perkhidmatannya.	Pengurus Projek, Pemilik Projek, Pembekal

5.7.32 Hak Harta Intelek

Kawalan ini diwujudkan bagi memastikan pematuhan dengan keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan dengan hak harta intelek.

(1) Pematuhan terhadap Hak Harta Intelek	Tanggungjawab
Warga UM dan Pihak Ketiga perlu mengiktiraf dan menghormati harta intelek berkaitan dengan sistem maklumat. Perkara yang perlu dipatuhi:	Warga UM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UM

(a) Keperluan hak cipta yang berkaitan dengan bahan *proprietary,* perisian, dan reka bentuk yang diperoleh melalui UM;

(b) Keperluan pelesenan yang menghadkan penggunaan produk, perisian, reka bentuk dan bahan-bahan lain yang diperoleh oleh UM;

(c) Pematuhan yang berterusan dengan sekatan hak cipta produk dan keperluan pelesenan; dan

(d) Pengguna tidak dibenarkan menggunakan kemudahan pemprosesan maklumat bagi tujuan yang tidak dibenarkan.

(2) Perolehan Perisian Berlesen UM	**Tanggungjawab**
Perolehan bagi perisian berlesen untuk kegunaan rasmi staf dan pelajar UM tertakluk kepada perkara berikut: (a) Peruntukan JTM hanya boleh digunakan untuk memperoleh perisian untuk kegunaan pengajaran dan pembelajaran. Perisian tersebut mestilah digunakan oleh lebih dari dua (2) fakulti dan oleh sekurang-kurangnya 10% daripada jumlah keseluruhan pelajar UM. (b) Perisian yang digunakan oleh satu PTj hendaklah diperoleh menggunakan peruntukan PTj tersebut. (c) Perisian bukan untuk kegunaan pembelajaran dan pengajaran hendaklah diperoleh menggunakan peruntukan PTj. (d) Perolehan perisian yang digunakan untuk penyelidikan boleh menggunakan	Ketua PTj, Warga UM

peruntukan daripada geran penyelidikan dan Pejabat Timbalan Naib Canselor (Penyelidikan & Inovasi).

(e) Penggunaan perisian yang mempunyai lesen terhad, hendaklah mendapat kebenaran dari JTM.

(f) Maklumat perisian yang disediakan oleh JTM boleh dicapai di *Software Distribution Site* melalui portal pelajar UM (http://myum.um.edu.my) dan portal staf UM (http://portal.um.edu.my).

5.7.33 Perlindungan Rekod

Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, capaian tanpa izin dan capaian ke atas orang yang tidak berkenaan. Ini bagi memastikan pematuhan ke atas undang-undang berkaitan dengan rekod.

(1) Perlindungan Rekod	Tanggungjawab
Rekod ialah dokumen yang membuktikan aktiviti atau keputusan telah dilaksanakan. Semua rekod penting, sama ada dalam bentuk fizikal atau digital, perlu dilindungi daripada kehilangan, kerosakan, pemalsuan, capaian tanpa kebenaran, atau penyebaran tidak sah mengikut undang-undang, peraturan, kontrak dan keperluan perniagaan. Aspek yang perlu diambil kira termasuk: (a) Pengurusan penyimpanan, pengendalian dan pelupusan rekod; (b) Penentuan tempoh simpanan rekod; dan (c) Penyediaan inventori rekod.	Pentadbir Sistem ICT

5.7.34 Privasi dan Perlindungan Maklumat Peribadi

UM hendaklah mengenal pasti dan memenuhi keperluan berkaitan pemeliharaan privasi dan perlindungan PII selaras dengan undang-undang, peraturan dan keperluan kontrak yang berkuat kuasa.

Langkah ini bertujuan untuk memastikan pematuhan terhadap semua kehendak perundangan, berkanun dan kontrak yang berkaitan dengan aspek keselamatan maklumat dan perlindungan PII di UM.

(1) Perlindungan dan Privasi Data Peribadi	Tanggungjawab
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. Privasi dan perlindungan maklumat peribadi pengguna dijamin seperti yang tertakluk dalam undang-undang kerajaan dan peraturan yang berkenaan.	Pentadbir Sistem ICT, Pembekal, Warga UM

5.7.35 Semakan Bebas Keselamatan Maklumat

Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang bagi memastikan pendekatan yang digunakan oleh UM bersesuaian, cukup dan berkesan secara lebih efektif.

(1) Kajian Semula Keselamatan Maklumat secara Berkecuali	Tanggungjawab
Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan secara berkala atau apabila berlaku perubahan ketara pada sistem dan infrastruktur. Penilaian ini meliputi semakan terhadap objektif kawalan, kawalan	Pentadbir Sistem ICT

keselamatan, polisi, prosedur, serta perubahan produk atau perkhidmatan, dan perlu dijalankan secara bebas oleh pihak luar.

Pihak luar yang menjalankan penilaian hendaklah mempunyai kecekapan, kelayakan dan kepakaran yang sesuai.

5.7.36 Piawaian untuk Keselamatan Maklumat

Pematuhan dengan dasar keselamatan maklumat UM hendaklah sentiasa disemak bagi memastikan keselamatan maklumat dilaksanakan mengikut polisi keselamatan maklumat serta piawaian dan peraturan semasa.

(1) Pematuhan Dasar dan Piawaian	**Tanggungjawab**
UM hendaklah membuat kajian semula pematuhan berdasarkan piawaian yang berkaitan. Sekiranya kajian semula mendapati ketidakpatuhan, UM perlu: (a) Mengenal pasti punca ketidakpatuhan; (b) Menilai keperluan tindakan untuk mencapai pematuhan; (c) Melaksanakan tindakan pembetulan yang sewajarnya; dan (d) Mengkaji semula tindakan pembetulan yang diambil untuk mengesahkan keberkesanannya dan mengenal pasti apa-apa kekurangan dan kelemahan.	Pemilik Proses, Pentadbir Sistem ICT
(2) Penilaian Tahap Keselamatan	**Tanggungjawab**
Sistem maklumat hendaklah diuji selaras dengan pematuhan peraturan semasa yang berkuat kuasa.	Pentadbir Sistem Aplikasi, Pentadbir Rangkaian, Pentadbir Pusat Data, Pentadbir Keselamatan ICT

Penilaian ini perlu dilaksanakan sekurang-kurangnya sekali dalam setahun atau mengikut keperluan.

5.7.37 Pengendalian Prosedur yang Didokumenkan

Semua prosedur pengendalian dan pemprosesan maklumat hendaklah didokumen dan disediakan kepada staf yang memerlukan. Ini bagi memastikan operasi kemudahan pemprosesan maklumat disediakan dengan betul dan dapat diakses dengan selamat.

(1) Penyediaan Dokumen Prosedur	Tanggungjawab
Semua aktiviti operasi yang berkaitan dengan pemprosesan maklumat dan pengurusan kemudahan komunikasi hendaklah disokong dengan dokumen prosedur. Dokumen prosedur yang perlu disediakan meliputi perkara berikut: (a) Instalasi dan konfigurasi sistem. (b) Pemprosesan dan pengendalian maklumat secara automatik dan manual. (c) Sandaran data. Perkara berikut perlu dipatuhi bagi memastikan setiap prosedur mudah dicapai dan terkini: (a) Semua prosedur yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal. (b) Semua prosedur hendaklah disemak dan dikemas kini dari semasa ke semasa atau mengikut keperluan.	Pentadbir Sistem ICT
(2) Kandungan Dokumen Prosedur	**Tanggungjawab**
Dokumen posedur hendaklah diwujudkan, disemak dan dikemas kini mengikut keperluan.	Pentadbir Sistem ICT

Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Keperluan penjadualan setiap aktiviti perlu mengambil kira saling kebergantungan dengan sistem lain, keutamaan tugasan dan tempoh masa penyempurnaan tugasan.

(b) Mengandungi arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan prosedur pemulihan sekiranya pemprosesan tergendala atau terhenti.

(c) Senarai kontak sokongan dalaman dan/atau luaran sebagai rujukan semasa berlaku keadaan luar biasa, kesulitan operasi atau masalah teknikal yang tidak dijangka.

(d) Pengurusan jejak audit dan maklumat log sistem.

(e) Prosedur pemantauan.

5.8 KAWALAN SUMBER MANUSIA

Terdapat lapan (8) kawalan sumber manusia yang terpakai dan perlu dipatuhi dalam pengurusan data dan maklumat di UM.

5.8.1 Tapisan Keselamatan

Tapisan keselamatan perlu bagi memastikan semua staf dan pihak berkepentingan adalah layak dan sesuai untuk peranan yang dipertimbangkan serta kekal layak dan sesuai sepanjang tempoh penglibatan mereka dalam urusan perkhidmatan ICT di UM.

(1) Tapisan Keselamatan	Tanggungjawab
Tapisan keselamatan hendaklah dijalankan terhadap staf, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT yang terlibat selaras dengan keperluan perkhidmatan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab staf, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UM yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan. (b) Menjalankan tapisan keselamatan untuk staf, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UM yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai, selaras dengan keperluan perkhidmatan dan	Pentadbir Sistem ICT, Pegawai Pentadbiran JTM, Jabatan Sumber Manusia (JSM)

peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.

5.8.2 Terma dan Syarat Pelantikan

Penyediaan terma dan syarat pelantikan perlu dipatuhi oleh semua pihak bagi memastikan semua pihak termasuk staf UM, pihak ketiga dan pihak berkepentingan memahami tanggungjawab serta peranan dalam keselamatan ICT.

(1) Terma dan Syarat Pelantikan	Tanggungjawab
Persetujuan berkontrak dengan semua pihak yang mempunyai urusan dengan perkhidmatan ICT di UM hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab Universiti terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi ialah seperti yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan serta tanggungjawab staf, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT dan yang terlibat dalam menjamin keselamatan aset ICT. (b) Mematuhi semua terma dan syarat perkhidmatan serta peraturan yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan dan ditandatangani. (c) Memahami tindakan boleh diambil jika keselamatan maklumat tidak dipatuhi.	Pentadbir Sistem ICT, JSM

5.8.3 Program Kesedaran, Pendidikan dan Latihan Keselamatan

Semua pihak yang terlibat dengan urusan perkhidmatan ICT UM perlu menerima program kesedaran, pendidikan dan latihan yang bersesuaian mengenai pengurusan keselamatan maklumat di UM. Pendekatan ini

memastikan semua pihak termasuk staf, pelajar, pihak ketiga dan berkepentingan memahami dan jelas akan tanggungjawab mereka ke atas keselamatan maklumat.

(1) Program Kesedaran Keselamatan Maklumat	Tanggungjawab
Perkara-perkara yang perlu dipatuhi dalam melaksanakan program kesedaran adalah seperti berikut: (a) Memastikan kesedaran, pendidikan dan latihan diberikan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. (b) Memastikan kesedaran berkaitan dengan keselamatan siber diberikan kepada semua pihak secara berkala. (c) Memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat. (d) Memaklumkan senarai perhubungan sekiranya pelanggaran maklumat dikesan oleh warga UM dan pihak ketiga.	Pentadbir Sistem ICT

5.8.4 Tindakan Disiplin

Tindakan disiplin perlu dinyata dan disampaikan kepada warga UM atau pihak berkepentingan bagi memastikan semua pihak terlibat memahami kesan pelanggaran ke atas keselamatan maklumat mengikut perundangan atau peraturan yang sedang berkuat kuasa.

(1) Tindakan Pelanggaran Perundangan dan Peraturan	Tanggungjawab
Tindakan boleh dikenakan ke atas warga UM dan pihak ketiga yang tidak mematuhi keselamatan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan adanya proses tindakan disiplin dan/atau perundangan sekiranya berlaku pelanggaran terhadap polisi, perundangan dan peraturan yang ditetapkan oleh UM atau Kerajaan. (b) Tindakan tatatertib atau tindakan sewajarnya akan dikenakan bagi sebarang pelanggaran kepada peraturan yang berkuat kuasa.	Unit Integriti, JSM

5.8.5 Tanggungjawab selepas Pertukaran atau Penamatan Perkhidmatan

Peranan dan tanggungjawab berkaitan keselamatan maklumat yang masih berkuat kuasa selepas penamatan atau pertukaran perjawatan hendaklah dikenal pasti, dikuat kuasa dan disampaikan kepada warga UM dan semua pihak yang terlibat. Ia bertujuan untuk melindungi kepentingan Universiti semasa proses pertukaran atau penamatan perkhidmatan.

(1) Pertukaran atau Penamatan	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua aset ICT dikembalikan kepada UM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan. (b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut	Staf, Pihak Ketiga, Pentadbir Sistem ICT

peraturan dan/atau terma perkhidmatan yang ditetapkan.

(c) Maklumat rasmi dalam aset maklumat tidak dibenarkan dibawa keluar dari UM.

Staf yang bertukar kerja atau jabatan hendaklah mematuhi perkara berikut:

(a) Memastikan semua aset ICT berkaitan dengan tugas terdahulu dikembalikan kepada jabatan 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) Menyedia dan menyerahkan nota serahan tugas dan myPortfolio kepada penyelia berkaitan.

5.8.6 Perjanjian Kerahsiaan atau Tidak Mendedahkan

Perjanjian kerahsiaan atau tidak mendedahkan mencerminkan keperluan Universiti untuk memastikan maklumat yang boleh diakses oleh staf atau pihak ketiga dikenal pasti, didokumen, disemak secara berkala dan disahkan melalui tandatangan.

(1) Kerahsiaan atau *Non-Disclosure Agreement* (NDA)	**Tanggungjawab**
Perjanjian kerahsiaan perlu melindungi maklumat berdasarkan perundangan yang berkuat kuasa terhadap pihak yang berkepentingan dan warga UM. Perkara yang perlu dipatuhi adalah seperti berikut:	Pentadbir Sistem ICT

(a) Syarat-syarat Perjanjian Tanpa Pendedahan atau *Non-Disclosure Agreement* (NDA) perlu mengambil kira keperluan UM dan hendaklah disemak dan didokumentasikan dari semasa ke semasa.

(b) Pihak luar hendaklah bersetuju dan mematuhi semua keperluan keselamatan yang terkandung di dalam dokumen NDA bagi kemudahan akses ICT.

5.8.7 Bekerja Jarak Jauh

Langkah keselamatan hendaklah dilaksanakan apabila staf bekerja dari jarak jauh untuk melindungi maklumat yang dicapai, diproses atau disimpan secara jarak jauh.

(1) Kerja secara Jarak Jauh	Tanggungjawab
Kerja secara jarak jauh merujuk kepada situasi di mana staf melaksanakan tugasan dari lokasi di luar premis, dengan mengakses maklumat sama ada dalam bentuk cetakan atau elektronik melalui peralatan ICT. Persekitaran kerja jarak jauh ini termasuk bentuk-bentuk seperti "telekerja", "telecommuting", "tempat kerja fleksibel", "persekitaran kerja maya", dan "penyelenggaraan jarak jauh". Staf yang bekerja jarak jauh hendaklah mematuhi perkara berikut: (a) Memastikan keselamatan maklumat UM dipatuhi dan tidak disebarkan kepada pihak luar. (b) Mematuhi dasar atau peraturan yang berkuat kuasa.	Staf UM

5.8.8 Pelaporan Insiden Keselamatan Maklumat

Pelaporan insiden keselamatan maklumat perlu dilaksanakan untuk memastikan insiden dikendalikan dengan berkesan bagi meminimumkan impak dan tidak menjejaskan sistem penyampaian perkhidmatan.

(1) Pelaporan Insiden Keselamatan Maklumat	Tanggungjawab
Insiden keselamatan merangkumi insiden, pelanggaran dan kerentanan sistem. Pengguna dan pihak luar yang menggunakan sistem dan perkhidmatan maklumat UM dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT. Insiden perlu dilaporkan apabila berlaku perkara seperti berikut: (a) Kawalan keselamatan maklumat yang tidak berkesan. (b) Pelanggaran sebarang kerahsiaan, integriti atau ketersediaan maklumat. (c) Kesilapan manusia. (d) Ketidakpatuhan terhadap polisi keselamatan maklumat. (e) Pelanggaran keselamatan fizikal. (f) Perubahan sistem yang tidak melalui proses pengurusan perubahan. (g) Perisian atau perkakasan yang rosak atau tidak berfungsi. (h) Penyalahgunaan hak akses. (i) Kerentanan (*vulnerablity*). (j) Percubaan serangan perisian hasad (*malware*).	Staf, Pelajar, Pihak Ketiga

5.9 KAWALAN FIZIKAL

Terdapat 14 kawalan fizikal yang terpakai dan perlu dipatuhi oleh semua pihak yang terlibat dalam pengurusan data dan maklumat di UM.

5.9.1 Perimeter Keselamatan Fizikal

Kawalan ini bertujuan untuk menghalang capaian tanpa kebenaran, gangguan secara fizikal dan kerosakan terhadap maklumat, premis dan kemudahan ICT UM.

(1) Perimeter Keselamatan Maklumat	Tanggungjawab
Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh premis. Langkah-langkah keselamatan fizikal adalah seperti yang berikut: (a) Menetapkan perimeter kawasan keselamatan fizikal dan keperluan keselamatan bagi melindungi aset. (b) Memastikan perimeter kawasan yang dilindungi atau mempunyai kemudahan pemprosesan maklumat dikawal menggunakan kawalan yang bersesuaian (halangan seperti pagar kawalan, dinding, pintu, kad akses, pengawal keselamatan). (c) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan staf yang diberi kebenaran sahaja boleh melalui pintu masuk tersebut. (d) Memasang alat penggera atau CCTV. (e) Menyediakan tempat atau bilik khas untuk pelawat.	Pentadbir Bangunan, Pentadbir Keselamatan ICT, Pentadbir Pusat Data, Pentadbir Rangkaian

(f) Mereka bentuk dan melaksanakan perlindungan fizikal di dalam pejabat, bilik dan kemudahan daripada ancaman bencana.

(g) Melaksana perlindungan fizikal dan menyediakan garis panduan untuk staf yang bekerja di dalam kawasan terhad.

(h) Mewujudkan kawalan di kawasan penghantaran, pemunggahan dan kawasan larangan.

5.9.2 Kemasukan Fizikal

Kawalan kemasukan fizikal bertujuan untuk melaksanakan kawalan akses masuk kepada maklumat, premis dan kemudahan ICT UM.

(1) Kawalan Akses Masuk Fizikal	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan pemakaian pas keselamatan sepanjang berada di premis UM. (b) Menghadkan akses masuk ke kawasan yang berkaitan kepada staf yang dibenarkan sahaja berdasarkan kelulusan. (c) Menyedia dan menyemak log audit *trail* akses ke Pusat Data secara berkala. (d) Menggunakan kad akses untuk kemasukan fizikal ke kawasan penyimpanan maklumat atau kawasan larangan. (e) Menyediakan kawasan menunggu atau penerimaan yang boleh dipantau oleh pegawai bertanggungjawab.	Pentadbir Bangunan, Pentadbir Sistem ICT, Staf, Pembekal

(f) Memberikan akses yang terhad dan pemantauan kepada staf pembekal ke kawasan pemprosesan maklumat atau kawasan larangan apabila diperlukan sahaja. (g) Memastikan keselamatan akses ke atas peralatan UM yang ditempatkan di lokasi berkongsi dengan jabatan lain. (h) Mengemas kini kawalan keselamatan fizikal dengan lebih kukuh bagi insiden yang kerap berlaku atau meningkat. (i) Memastikan pintu masuk lain seperti pintu kecemasan dikawal daripada akses tanpa kebenaran.	
(2) Kawasan Penghantaran dan Pemunggahan	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Mempunyai akses terhad kepada kawasan penghantaran dan pemunggahan oleh pihak luar. (b) Memastikan pihak luar tidak dibenarkan masuk ke lokasi lain tanpa kebenaran. (c) Memastikan kawasan penghantaran dan pemunggahan atau tempat lain dikawal semasa proses penghantaran dan pemunggahan. (d) Memeriksa dan memastikan barang yang dihantar tidak mengandungi bahan letupan atau bahan berbahaya yang lain.	Pemilik Aset, Pentadbir Bangunan, Pentadbir Sistem ICT

(e) Semua penghantaran barang perlu diselaras dan didaftarkan mengikut prosedur yang ditetapkan.

(f) Memastikan barang yang diterima tidak diubah suai tanpa kebenaran.

5.9.3 Keselamatan Pejabat, Bilik dan Kemudahan ICT

Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah direka bentuk dan dilaksanakan. Ianya bertujuan untuk memastikan keselamatan dan perlindungan daripada sebarang bentuk pencerobohan, ancaman, kerosakan, kecuaian serta akses yang tidak dibenarkan.

(1) Keselamatan Pejabat, Bilik dan Kemudahan	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Memastikan kawasan larangan dihadkan daripada akses tanpa kebenaran. (b) Memastikan penunjuk ke lokasi bilik operasi atau kawasan larangan tidak didedahkan atau hanya memberi petunjuk yang minimum. (c) Memastikan maklumat kawasan larangan tidak dapat dilihat oleh pihak luar. (d) Memastikan maklumat perhubungan atau lokasi kawasan larangan tidak didedahkan tanpa kebenaran.	Pentadbir Bangunan, Pentadbir Pusat Data, Staf

5.9.4 Pemantauan Keselamatan Fizikal

Premis fizikal harus dipantau secara berterusan untuk memastikan keselamatan fizikal dikawal.

(1) Pemantauan Premis Fizikal	Tanggungjawab
Pemantauan kepada bangunan yang menempatkan sistem kritikal perlu dipantau secara berterusan untuk mengesan capaian yang tidak dibenarkan atau tingkah laku yang mencurigakan dengan cara berikut: (a) Memasang sistem pemantauan video seperti CCTV untuk melihat dan merakam capaian ke kawasan sensitif di dalam dan luar premis UM. (b) Memastikan pemasangan pengesan mengikut piawaian yang berkaitan dan diuji keberkesanannya secara berkala. (c) Memastikan pemasangan penggera merangkumi semua pintu yang boleh diakses termasuk kawasan yang menempatkan aset Universiti, kawasan sensitif dan tidak berpenghuni. (d) Menghadkan akses berdasarkan peranan dan tanggungjawab individu melalui sistem yang diguna pakai. (e) Memastikan reka bentuk sistem pemantauan dirahsiakan atau tidak boleh didedahkan tanpa kebenaran untuk mengelakkan kebocoran maklumat dan dipecah masuk.	Pentadbir Bangunan, Pentadbir Keselamatan ICT, Pentadbir Pusat Data

5.9.5 Perlindungan daripada Ancaman Fizikal dan Persekitaran

Perlindungan fizikal terhadap bencana alam, serangan niat jahat atau kemalangan hendaklah dirangka dan dilaksanakan bagi memastikan infrastruktur ICT yang direka bentuk dilindungi.

(1) Perlindungan terhadap Ancaman Fizikal dan Bencana Alam	Tanggungjawab
Penilaian risiko ke atas ancaman fizikal dan alam sekitar perlu dilaksanakan secara berkala. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Mereka bentuk dan melaksanakan pelan perlindungan fizikal daripada kebakaran dan bencana alam. (b) Memastikan pelan tindakan perlindungan bagi ancaman berbahaya seperti letupan, kacau-bilau, rusuhan dan sebagainya. (c) Pelan tindakan perlindungan perlu merangkumi kawalan seperti bencana alam, kebakaran, gangguan bekalan elektrik dan letupan. Nasihat pakar perlu diperoleh bagi memastikan pengurusan risiko daripada ancaman fizikal dapat dikendalikan dengan teratur dan berkesan.	Pentadbir Bangunan, Pentadbir Sistem ICT

5.9.6 Bekerja di Kawasan Selamat

Langkah keselamatan untuk bekerja di kawasan selamat hendaklah direka bentuk dan dilaksanakan bagi memastikan maklumat dan aset ICT berada di kawasan yang selamat daripada gangguan atau kerosakan daripada staf yang bekerja di sekitar kawasan.

(1) Kawasan Larangan	Tanggungjawab
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pihak yang dibenarkan sahaja. Kawalan ini dilaksanakan bagi melindungi aset maklumat yang terdapat dalam premis UM termasuk Pusat Data. Kawasan seperti ini perlu dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Langkah kawalan keselamatan ke atas kawasan tersebut adalah seperti berikut: (a) Memastikan individu yang bekerja di kawasan tersebut memahami tanggungjawab mereka. (b) Memantau dan mengawasi setiap kerja yang dijalankan di kawasan larangan. (c) Kawasan larangan perlu sentiasa berkunci dan ruangan kosong yang ada sentiasa diperiksa. (d) Fotografi, video, audio dan peralatan rakaman lain tidak dibenarkan dibawa masuk melainkan dengan kebenaran. (e) Mengawal peranti yang dibenarkan dibawa masuk ke dalam kawasan larangan. (f) Pelayan, peralatan komunikasi dan storan perlu ditempatkan di Pusat Data, bilik pelayan atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegahan kebakaran.	Pentadbir Bangunan, Pentadbir Pusat Data, Pentadbir Keselamatan ICT

(g) Capaian terhad kepada pihak yang telah diberi kuasa sahaja dan dipantau pada setiap masa.

(h) Peralatan keselamatan seperti CCTV, log capaian dan seumpamanya perlu diperiksa secara berjadual.

(i) Butiran pelawat keluar masuk ke kawasan larangan perlu direkodkan.

(j) Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan.

(k) Lokasi premis yang menempatkan aset maklumat serta infrastruktur, peralatan atau perkakasan yang berkaitan hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam.

(l) Memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan.

(m) Menghadkan jalan keluar masuk.

(n) Memaparkan papan tanda keluar kecemasan yang mudah dilihat atau diakses.

5.9.7 Polisi Meja Bersih dan Skrin Bersih

Polisi 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.

(1) Polisi Meja Bersih dan Skrin Bersih	Tanggungjawab
Polisi Meja Bersih dan Skrin Bersih ialah satu set panduan yang digunakan dalam pengurusan keselamatan maklumat dan	Warga UM, Pihak Ketiga

keberkesanan dalam UM untuk melindungi maklumat sensitif dan menjaga privasi staf.

Polisi ini bermaksud tidak meninggalkan dan mendedahkan bahan-bahan yang sensitif sama ada atas meja pengguna, pada paparan skrin komputer, mesin pencetak, mesin faks atau mesin pengimbas apabila pengguna tidak berada di tempatnya.

Perkara yang perlu dipatuhi seperti berikut:

(a) Menggunakan kemudahan kata laluan *screen saver* atau log keluar apabila meninggalkan komputer.

(b) Menetapkan paparan skrin akan tertutup selepas 15 minit tidak digunakan.

(c) Dokumen terperingkat hendaklah disimpan di dalam laci atau kabinet fail yang berkunci.

(d) Membersihkan maklumat sensitif atau kritikal pada papan putih dan jenis paparan lain apabila tidak diperlukan lagi.

(e) Memastikan semua dokumen diambil segera dari pencetak, pengimbas dan mesin fotostat. Pencetak dan pengimbas yang dikongsi hendaklah dikonfigurasi dengan fungsi kod PIN atau kawalan lain supaya hanya pemilik dokumen sahaja yang boleh mengambil cetakan mereka.

(f) Menghalang penggunaan tanpa kebenaran mesin fotostat dan teknologi penghasilan semula seperti mesin pengimbas atau kamera digital.

(g) Memastikan dokumen rahsia berbentuk fizikal dicincang sebelum dibuang.

(2) Peralatan Pengguna Tanpa Kawalan	Tanggungjawab
Pengguna hendaklah memastikan kelengkapan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya. Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara yang berikut: (a) Menamatkan sesi aktif apabila selesai tugas. (b) Log keluar (*log off*) daripada komputer meja, komputer riba dan pelayan apabila selesai penggunaan. (c) Memastikan komputer meja, komputer riba atau terminal sentiasa selamat daripada pengguna yang tidak dibenarkan.	Pengguna

5.9.8 Penempatan dan Perlindungan Aset ICT

Kawalan keselamatan ini bertujuan untuk memastikan aset ICT ditempatkan di kawasan yang selamat dan dilindungi daripada sebarang bentuk pencerobohan dan ancaman.

(1) Penempatan dan Perlindungan Aset ICT	Tanggungjawab
Peralatan ICT hendaklah ditempatkan dengan selamat dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran dan peluang kemasukan yang tidak dibenarkan. Langkah keselamatan yang perlu diambil adalah seperti berikut:	Warga UM, Pegawai Aset, Pemilik Aset, Pentadbir Sistem ICT, Pentadbir Bangunan

(a) Kemudahan penyimpanan perlu dilindungi untuk menghalang akses yang tidak dibenarkan.

(b) Kemudahan pemprosesan maklumat yang melaksanakan pengendalian maklumat rahsia rasmi harus ditempatkan dengan teliti untuk mengurangkan risiko maklumat tersebut dapat dilihat oleh pihak yang tidak berkaitan.

(c) Mengadaptasi kawalan untuk mengurangkan risiko potensi ancaman fizikal dan bencana alam seperti kecurian, kebakaran, gangguan bekalan elektrik, dan lain-lain.

(d) Menetapkan larangan makan, minum dan merokok di kedudukan berhampiran dengan kemudahan pemprosesan maklumat.

(e) Pemantauan terhadap keadaan persekitaran seperti suhu dan kelembapan serta keadaan yang boleh menjejaskan operasi kemudahan pemprosesan maklumat.

(f) Pemasangan alat perlindungan kilat.

(g) Peralatan yang memerlukan perlindungan khas perlu dilindungi daripada bahaya atau kerosakan dengan langkah yang sesuai.

(h) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik.

(i) Mewujudkan rekod senarai peralatan yang mengandungi maklumat penting bagi memudahkan jejakan.

(j) Memastikan perisian antivirus di komputer sentiasa aktif dan dikemas kini selain melakukan imbasan ke atas media storan yang digunakan.

(k) Sambungan dan akses kepada peralatan daripada persekitaran rangkaian tidak rasmi organisasi adalah tidak dibenarkan kecuali dengan kelulusan ketua ~~jabatan~~ dan pelaksanaan sambungan serta akses dari luar mestilah dalam persekitaran yang dipantau dan selamat.

(l) Jika peralatan mempunyai sokongan daripada pihak ketiga, mohon bantuan pihak ketiga untuk proses pemulihan.

(m) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada Pegawai Aset.

5.9.9 Keselamatan Aset di Luar Premis

Sebarang peranti yang digunakan di luar Universiti perlu mendapatkan kebenaran pengurusan dan direkodkan. Ianya bagi memastikan keselamatan aset yang dibawa keluar dari premis dilindungi.

(1) Peralatan ICT di Luar Premis	**Tanggungjawab**
Penggunaan sebarang peranti di luar premis UM yang menyimpan atau memproses maklumat, termasuk peranti mudah alih kepunyaan Universiti atau peranti di bawah konsep *Buy Your Own Device* (BYOD), hendaklah mematuhi keperluan perlindungan	Pemilik Aset, Warga UM

keselamatan maklumat yang ditetapkan. Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Melindungi dan mengawal selia peralatan ICT sepanjang masa daripada kerosakan, kehilangan atau akses yang tidak dibenarkan.

(b) Memastikan maklumat peminjaman atau penggunaan aset ICT/media storan di luar pejabat direkodkan dan data rahsia rasmi dihapuskan sebelum pemulangan.

(c) Memastikan kawalan keselamatan diambil kira semasa penggunaan aset ICT di tempat awam.

(d) Mengemukakan permohonan dan mendapatkan kelulusan dari Ketua terlebih dahulu bagi aset ICT yang hendak dibawa keluar dari premis UM.

5.9.10 Media Storan

Kawalan keselamatan bagi media storan hendaklah diurus dan dilindungi bagi memastikan media storan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan.

(1) Pengurusan Media Storan	**Tanggungjawab**
Media storan digunakan untuk menyimpan data dan maklumat seperti *thumb drive*, *external drive* dan media storan lain. Pengendalian media storan perlu mematuhi perkara berikut: (a) Media storan mudah alih hendaklah disimpan di ruang penyimpanan yang baik	Pentadbir Sistem ICT, Warga UM

dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat. (b) Melabelkan semua media mengikut tahap sensitiviti maklumat. (c) Memastikan media storan mudah alih boleh berfungsi sekiranya diperlukan. (d) Memastikan maklumat rahsia rasmi yang disimpan melebihi satu media storan mudah alih mengambil kira risiko kerosakan atau kehilangan maklumat. (e) Menghad dan menentukan capaian media kepada kepada staf yang dibenarkan sahaja. (f) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja. (g) Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelakkan daripada kerosakan dan pendedahan yang tidak dibenarkan. (h) Hanya maklumat rasmi dibenarkan untuk disimpan dalam media storan yang dibekalkan oleh Universiti.	
(2) Pelupusan dan Penggunaan Semula Media	**Tanggungjawab**
Prosedur pelupusan dan penggunaan semula media storan hendaklah diwujudkan untuk meminimumkan risiko kebocoran maklumat. Perkara yang perlu dipatuhi adalah seperti berikut:	Pentadbir Pusat Data, Staf

(a) Media storan yang akan dilupuskan dan digunakan semula perlu disanitasi atau diformat terlebih dahulu.

(b) Media storan yang tidak berjaya disanitasi atau diformat semula untuk penggunaan semula hendaklah dilupuskan menggunakan kaedah yang dibenarkan.

(c) Melupuskan media storan yang mengandungi maklumat sulit menggunakan kaedah yang dibenarkan sekiranya tidak diperlukan lagi.

(d) Pelupusan media storan oleh pihak luar hendaklah mematuhi kawalan keselamatan dan dilaksanakan oleh pihak yang berpengalaman.

(e) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan.

(f) Pelupusan media storan hendaklah direkodkan.

(g) Semua media storan yang hendak dilupuskan mesti dirujuk kepada JTM bagi yang berkaitan ICT.

(h) Pengguna hendaklah menghapuskan atau memindahkan semua maklumat rasmi/terperingkat dari media storan sendiri apabila bersara/bertukar jabatan/penamatan perkhidmatan.

5.9.11 Utiliti Sokongan

Kawalan ke atas perkhidmatan sokongan ICT perlu dilindungi bagi mengelakkan kehilangan, kerosakan atau kompromi maklumat dan aset atau gangguan kepada operasi akibat kegagalan bekalan kuasa dan gangguan fasiliti.

(1) Perkhidmatan Sokongan ICT	Tanggungjawab
UM bergantung kepada perkhidmatan utiliti seperti bekalan elektrik dan air, telekomunikasi, gas, kumbahan, pengudaraan dan penyaman udara untuk menyokong kemudahan pemprosesan maklumat. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan peralatan di dalam fasiliti perkhidmatan sokongan beroperasi, dikonfigurasi dan diselenggara mengikut spesifikasi pengeluar yang berkaitan. (b) Memastikan fasiliti perkhidmatan sokongan dinilai semula keupayaannya secara berkala bagi memenuhi keperluan UM. (c) Memastikan peralatan sokongan disemak dan diselenggarakan dari semasa ke semasa mengikut Perjanjian Tahap Perkhidmatan (SLA). (d) Menyediakan fasiliti sokongan kedua. (e) Memastikan peralatan di dalam fasiliti perkhidmatan sokongan sentiasa disokong oleh *Uninterruptible Power Supply* (UPS). (f) Memastikan bekalan kuasa berterusan disalurkan kepada fasiliti sokongan seperti UPS dan penjana kuasa (*generator*) bagi membolehkan Pusat Data sentiasa beroperasi dengan optimum. (g) Memastikan peralatan sokongan diperiksa dan diuji secara berkala oleh pihak berkaitan.	Pentadbir Pusat Data, Pentadbir Bangunan

(h) Memastikan peralatan sokongan utiliti berada pada rangkaian yang berasingan daripada pemprosesan maklumat kemudahan jika disambungkan ke rangkaian.

(i) Memastikan peralatan sokongan utiliti disambungkan ke internet menggunakan kaedah yang dibenarkan hanya apabila diperlukan.

5.9.12 Keselamatan Pengkabelan

Kawalan keselamatan ke atas pengkabelan perlu diwujudkan bagi memastikan kabel rangkaian dan kuasa elektrik dilindungi daripada gangguan dan pencerobohan.

(1) Keselamatan Kabel	Tanggungjawab
Kabel yang membawa tenaga elektrik, data, atau yang menyokong perkhidmatan maklumat hendaklah dilindungi daripada sebarang gangguan atau pencerobohan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Kabel kuasa elektrik dan rangkaian yang disambungkan ke sistem maklumat diberi perlindungan yang bersesuaian untuk mengelakkan pemotongan kabel tanpa sengaja. (b) Mengasingkan kabel kuasa elektrik dan rangkaian untuk mencegah gangguan penghantaran data. (c) Memastikan kabel bagi sistem kritikal mempunyai kawalan tambahan seperti berikut:	Pentadbir Pusat Data, Pentadbir Rangkaian

(i) Pemasangan saluran pelindung berlapis (*conduit*) dan dalam bilik berkunci.

(ii) Semakan dan pemeriksaan teknikal secara berkala untuk mengenal pasti sambungan kabel yang tidak dibenarkan terhadap peranti.

(iii) Kawalan akses ke bilik telekomunikasi atau bilik kabel.

(iv) Memastikan semua sambungan kabel dilabelkan bagi membolehkan pengenalan fizikal dan pemeriksaan kabel terlibat.

(v) Mendapatkan nasihat pakar berkaitan kaedah pengurusan risiko yang timbul daripada insiden atau kerosakan kabel.

5.9.13 Penyelenggaraan Peralatan

Peralatan ICT hendaklah diselenggara dengan betul bagi memastikan ketersediaan dan keutuhannya berterusan. Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti.

(1) Penyelenggaraan Peralatan	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan yang diselenggara hendaklah mematuhi spesifikasi dan tempoh penyelenggaraan yang ditetapkan oleh pengeluar berkaitan. (b) Pemantauan pelaksanaan penyelenggaraan secara berkala atau atas keperluan.	Pentadbir Pusat Data, Pentadbir Rangkaian, Pemilik Aset, Pembekal

(c) Memastikan peralatan hanya boleh diselenggara oleh staf atau pihak yang dibenarkan sahaja.

(d) Menyimpan rekod penyelenggaraan pencegahan dan pemulihan.

(e) Melaksanakan kawalan yang sesuai bagi tujuan penyelenggaraan pencegahan dan pemulihan sama ada di dalam atau luar premis UM.

(f) Menyelia kerja-kerja penyelenggaraan yang dilakukan oleh Pihak Pembekal.

(g) Mengawal akses bagi penyelenggaraan yang dilaksanakan secara jarak jauh (*remote*).

(h) Melaksanakan kawalan keselamatan ke atas penyelenggaraan peralatan di luar premis UM.

(i) Menyemak dan menguji semua peralatan selepas proses penyelenggaraan bagi memastikan tiada pengubahsuaian yang tidak dibenarkan.

(j) Melaksanakan kaedah yang bersesuaian untuk pelupusan atau penggunaan semua peralatan.

5.9.14 Pelupusan atau Penggunaan Semula Peralatan

Semua peralatan yang mengandungi media storan hendaklah disahkan bagi memastikan kaedah pelulusan dan penggunaan semula peralatan dilaksanakan mengikut peraturan yang berkuat kuasa.

(1) Pelupusan Peralatan	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Maklumat pelupusan hendaklah direkod, dikemas kini dan dilaporkan mengikut keperluan. (b) Peralatan aset maklumat yang hendak dilupuskan perlu mematuhi prosedur pelupusan yang berkuat kuasa dan dilaksanakan secara terkawal dan lengkap. (c) Peralatan ICT yang akan dilupuskan sebelum dipindah milik, data-data dalam storan hendaklah dipastikan telah dihapuskan dengan cara yang selamat. (d) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan. (e) Peralatan yang hendak dilupus hendaklah disimpan di tempat khas yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan. (f) Maklumat rasmi Universiti perlu disalin pada media storan pendua sebelum maklumat dihapuskan bagi peralatan yang hendak dilupuskan. (g) Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal kecuali bagi maklumat yang perlu disimpan, ianya boleh dibuat salinan.	Pegawai Aset, Pentadbir Pusat Data, Warga UM, Pembekal

Warga UM **DILARANG SAMA SEKALI** melakukan perkara-perkara seperti berikut:

(a) Menyimpan mana-mana peralatan yang hendak dilupuskan untuk tujuan peribadi.

(b) Menanggalkan komponen peralatan seperti RAM, *hard disk, motherboard* dan sebagainya.

(c) Melupuskan sendiri tanpa kebenaran.

(d) Memindah keluar peralatan yang dilupuskan tanpa kelulusan.

(2) Penggunaan Semula Peralatan	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua maklumat di dalam peralatan hendaklah disanitasi atau dihapuskan secara selamat terlebih dahulu sebelum penggunaan semula atau dipindah milik. (b) Maklumat peralatan yang diguna semula atau dipindah milik hendaklah direkodkan dan dikemas kini. (c) Warga UM **DILARANG** melakukan perkara berikut: (i) Menyimpan peralatan berlebihan untuk tujuan peribadi. (ii) Menanggalkan komponen peralatan seperti RAM, *hard disk*, *motherboard* dan sebagainya. (iii) Menggunakan semula peralatan tanpa kelulusan.	Pentadbir Sistem ICT, Pegawai Aset, Warga UM

5.10 KAWALAN TEKNOLOGI

Terdapat 34 kawalan teknologi yang utama dan perlu dipatuhi oleh semua pihak yang terlibat dalam pengurusan data dan maklumat di UM.

5.10.1 Keselamatan Peranti Pengguna

Kawalan keselamatan hendaklah dilaksanakan bagi melindungi maklumat Universiti yang disimpan, diproses atau diakses melalui aset ICT pengguna, khususnya peranti titik akhir (*endpoint*) daripada risiko ancaman keselamatan yang mungkin timbul akibat penggunaannya.

(1) Peranti Mudah Alih	Tanggungjawab
Langkah-langkah keselamatan sokongan hendaklah digunakan bagi mengurus risiko yang timbul melalui penggunaan peranti mudah alih. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan jenis dan klasifikasi maklumat yang boleh diakses, diproses atau disimpan dalam peranti. (b) Memastikan peranti pengguna didaftarkan. (c) Memastikan perisian yang boleh dipasang pada peranti telah mendapat kebenaran. (d) Memastikan peranti dikonfigurasi dengan perisian atau *patches* terkini. (e) Menetapkan peraturan (*rules*) bagi sambungan ke rangkaian awam, atau rangkaian lain di luar premis menggunakan peranti. (f) Memastikan pengguna mematuhi kawalan capaian penggunaan aset ICT pengguna.	Pentadbir Sistem ICT

(g) Memastikan pengguna menggunakan kata laluan bagi penyimpanan maklumat terperingkat.

(h) Memastikan aset ICT pengguna mempunyai perisian antivirus.

(i) Memastikan pengguna melaksanakan sandaran bagi maklumat yang disimpan dalam aset ICT.

(j) Menggunakan perkhidmatan web dan aplikasi yang dibenarkan sahaja.

(k) Memastikan pengasingan (*hard disk partition*) data dan perisian pada peranti pengguna.

(l) UM berhak mengambil tindakan sekiranya didapati tidak mematuhi peraturan yang berkuat kuasa.

5.10.2 Hak Capaian Istimewa

Peruntukan dan penggunaan hak capaian istimewa hendaklah dihadkan dan dikawal. Ianya bertujuan untuk memastikan akses pengguna, komponen perisian dan perkhidmatan yang disediakan hanya diberikan kepada pengguna yang dibenarkan.

(1) Hak Capaian	**Tanggungjawab**
Penetapan dan penggunaan ke atas hak akses hendaklah mengambil kira perkara berikut: (a) Memastikan hak akses untuk sistem aplikasi, sistem pengoperasian dan pengurusan pangkalan data diberikan kepada pengguna yang sah dan dibenarkan oleh Ketua. (b) Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan	Pentadbir Sistem ICT

penyeliaan yang ketat, atas dasar keperluan untuk mengetahui (*need-to-know-basis*);

(c) Keperluan capaian hendaklah sentiasa dipantau dan dikemas kini bagi memastikan hak capaian ini diberikan kepada pengguna yang dibenarkan sahaja;

(d) Memastikan pengguna mengetahui tanggungjawab hak akses yang diterima;

(e) Memastikan perbezaan peranan akses untuk pentadbir dan pengguna;

(f) Sekiranya berlaku perubahan struktur organisasi di UM, penetapan dan penggunaan ke atas hak akses perlu disemak semula berdasarkan keperluan skop tugas;

(g) Melarang penggunaan ID pentadbir seperti *root* bagi akses ke konfigurasi sistem;

(h) Memberikan hak akses sementara untuk perubahan atau penyelenggaraan yang dilaksanakan oleh pihak pembekal;

(i) Merekodkan semua log masuk untuk kegunaan jejak audit;

(j) Menggunakan ID pengguna berdasarkan skop tugas (melaksanakan tugasan harian) dan tidak menggunakan ID pentadbir; dan

(k) Sebarang perubahan capaian mestilah mendapat kebenaran secara bertulis dan direkodkan.

5.10.3 Sekatan Capaian Maklumat

Capaian kepada fungsi maklumat dan sistem ICT hendaklah dihadkan berdasarkan kawalan akses yang ditetapkan bagi memastikan hanya akses yang dibenarkan ke atas maklumat dan aset yang berkaitan.

(1) Sekatan Capaian Maklumat	Tanggungjawab
Capaian kepada fungsi maklumat dan sistem ICT hendaklah dihadkan mengikut kawalan capaian yang ditetapkan merangkumi perkara berikut: (a) Menghadkan had capaian maklumat terperingkat kepada pengguna yang berdaftar sahaja. (b) Menyediakan mekanisme konfigurasi untuk mengawal capaian kepada maklumat dalam sistem, aplikasi dan perkhidmatan. (c) Mengawal data yang boleh dicapai oleh pengguna tertentu. (d) Mengawal identiti atau kumpulan identiti yang mempunyai hak capaian, seperti membaca, menulis, memadam dan melaksanakan (*execute*). (e) Memapar maklumat yang diperlukan sahaja. (f) Melaksana pengujian sistem dalam persekitaran pembangunan untuk mengelakkan sebarang ralat ke atas sistem sedia ada. (g) Memastikan sesi tidak aktif dilog keluar (*log-off*) secara automatik untuk mengelakkan capaian tidak sah.	Pentadbir Sistem Aplikasi, Pemilik Proses, Ketua PTj

(h) Menyahaktif pengguna yang tidak aktif (BUKAN MENGHAPUSKAN) untuk memudahkan siasatan susulan dilaksanakan.

5.10.4 Capaian kepada Kod Sumber

Akses kepada kod sumber dan persekitaran pembangunan hendaklah dikawal. Ini adalah untuk mengelakkan perubahan yang tidak dibenarkan bagi mengekalkan kerahsiaan.

(1) Kawalan Capaian kepada Kod Sumber	Tanggungjawab
Capaian kepada kod sumber program hendaklah dihadkan. Perkara berikut perlu dipatuhi untuk mengawal akses kepada kod sumber bagi meminimumkan potensi kegagalan sistem aplikasi: (a) Menguruskan akses kepada kod sumber dan program. (b) Akses kepada kod sumber hendaklah dikawal dan dihadkan kepada pengguna yang diberi kuasa sahaja. (c) Segala perubahan atau pengubahsuaian kepada sistem dan aplikasi mestilah dikawal dan direkodkan. Sebarang perubahan kepada kod sumber adalah tertakluk kepada keperluan yang telah diluluskan. (d) Kod sumber sistem aplikasi yang bukan *propriety* dan dibangunkan secara dalaman atau penyumberan bersama (*co-source*) adalah hak milik UM. (e) Sistem atau aplikasi baharu serta sebarang perubahan atau	Pengarah Projek, Pengurus Projek, Pentadbir Sistem Aplikasi, Pentadbir Pusat Data

pengubahsuaian kepada kod sumber hendaklah melalui proses pengujian dan pengesahan sebelum dilaksanakan dalam persekitaran produksi.

(f) Memberi kebenaran kepada individu tertentu untuk membaca dan mengubah (tulis) kod sumber mengikut keperluan tugas mereka, dan pada masa yang sama memastikan kawalan secukupnya dikenakan bagi mengelakkan sebarang risiko seperti pengubahsuaian tanpa kebenaran atau penyalahgunaan kod sumber tersebut, selaras dengan prosedur yang telah ditetapkan.

5.10.5 Pengesahan Selamat (*Secure Authentication*)

Teknologi dan prosedur pengesahan selamat hendaklah dilaksanakan berdasarkan sekatan capaian maklumat dan topik khusus mengenai kawalan capaian bagi memastikan pengguna atau individu menggunakan pengesahan yang sah untuk akses kepada sistem aplikasi dan perkhidmatan yang disediakan.

(1) Pengesahan Prosedur Log Masuk yang Selamat	**Tanggungjawab**
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.	Pentadbir Sistem Aplikasi

(b) Menjana amaran (*alert*) sekiranya berlaku perlanggaran semasa proses log masuk terhadap aplikasi sistem.

(c) Mengawal capaian ke atas aplikasi sistem mengikut prosedur yang ditetapkan.

(d) Mewujudkan teknik pengesahan pelbagai faktor (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) Menamatkan sesi tidak aktif selepas tempoh tidak aktif yang ditetapkan.

(g) Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.

(h) Menghadkan masa tempoh sambungan untuk menyediakan keselamatan tambahan untuk aplikasi berisiko tinggi dan mengurangkan tetingkap peluang untuk akses tanpa kebenaran.

5.10.6 Pengurusan Kapasiti (*Capacity Management*)

Penggunaan sumber hendaklah dipantau dan diselaraskan secara berterusan agar selari dengan keperluan kapasiti semasa serta jangkaan keperluan masa hadapan. Ini termasuk sumber seperti tenaga, ruang penyimpanan, dan sumber manusia, bagi memastikan keberkesanan dan kecekapan pengoperasian sistem ICT Universiti.

(1) Pengurusan Kapasiti	**Tanggungjawab**
Perkara yang perlu diambil kira seperti berikut: (a) Kapasiti sistem ICT hendaklah dirancang, diurus dan dikawal dengan terperinci bagi	Pentadbir Sistem ICT

memastikan keperluannya adalah mencukupi serta bersesuaian untuk pembangunan dan operasi sistem ICT semasa atau pada masa akan datang;

(b) Keperluan kapasiti perlu mengambil kira ciri-ciri keselamatan bagi meminimumkan risiko gangguan kepada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang;

(c) Pemantauan kapasiti sistem ICT perlu dilaksanakan untuk memastikan ketersediaan dan kecekapan sistem;

(d) Pengujian prestasi (*performance test*) ke atas sistem dan perkhidmatan hendaklah dilaksanakan untuk memastikan kapasiti mencukupi terutamanya semasa waktu puncak; dan

(e) Dokumen pengurusan kapasiti sumber perlu disediakan terutamanya untuk sistem kritikal.

(2) Peningkatan Kapasiti	**Tanggungjawab**
Perkara berikut perlu dipatuhi untuk meningkatkan kapasiti sumber: (a) Memastikan sumber manusia mencukupi; (b) Menyediakan kemudahan dan ruang kerja yang kondusif; (c) Melaksanakan perolehan bagi kapasiti yang tidak mencukupi agar sesuai dengan keperluan semasa dan masa hadapan; dan (d) Menggunakan pengkomputeran awan (*cloud computing*) sekiranya perlu.	Pentadbir Sistem ICT

(3) Pengurangan Kapasiti	Tanggungjawab
Perkara berikut perlu dipatuhi untuk mengurangkan kapasiti sumber: (a) Menghapuskan data lama (*disk space*) yang tidak digunakan lagi; (b) Melupuskan rekod fizikal secara terancang dan berkala; (c) Melupuskan sistem aplikasi, pangkalan data atau perkhidmatan ICT yang tidak digunakan lagi; (d) Mengoptimumkan proses *batch* dan *scheduler*; (e) Mengoptimumkan kod aplikasi dan kuiri pangkalan data; dan (f) Menghadkan *bandwidth* bagi perkhidmatan ICT yang menggunakan kapasiti yang tinggi (jika perlu).	Pentadbir Sistem ICT

5.10.7 Perlindungan Terhadap Perisian Hasad (*Malware*)

Perlindungan terhadap perisian hasad harus dilaksanakan dan disokong oleh kesedaran pengguna bagi memastikan perisian dan aset ICT dilindungi daripada perisian hasad (*malware*). Perlindungan terhadap perisian hasad hendaklah berdasarkan maklumat pengesanan dan pembaikan perisian hasad tersebut, kesedaran keselamatan, akses sistem yang sesuai serta kawalan pengurusan perubahan.

(1) Perlindungan daripada Perisian Hasad	Tanggungjawab
Perkara yang perlu dilaksanakan bagi memastikan aset maklumat dilindungi daripada perisian hasad adalah seperti berikut:	Pentadbir Sistem ICT

(a) Melaksanakan kawalan untuk mencegah dan mengesan perisian yang tidak sah, tidak diketahui, atau disyaki berbahaya.

(b) Mengurangkan kerentanan sistem yang boleh dieksploitasi oleh perisian hasad.

(c) Melaksanakan pengesahan berkala ke atas perisian dan maklumat sistem, terutamanya sistem kritikal.

(d) Melaksanakan kawalan terhadap fail dan perisian yang diperoleh dari sumber luaran atau medium storan lain.

(e) Memastikan perisian keselamatan sentiasa dikemas kini dan melaksanakan pengimbasan ke atas:

(i) Data yang diterima melalui rangkaian atau media storan sebelum digunakan;

(ii) E-mel dan lampiran sebelum dibuka; dan

(iii) Laman web yang diakses.

(f) Menetapkan konfigurasi perisian keselamatan untuk mengesan dan menyekat ancaman, termasuk mengguna pakai amalan terbaik (*best practise*).

(g) Melindungi sistem semasa penyelenggaraan dengan kawalan yang sesuai. Sekiranya perlu menutup perisian pengesanan secara sementara atau kekal, kelulusan hendaklah diperolehi dan direkodkan.

(h) Menyediakan proses pemulihan daripada serangan perisian hasad, termasuk

pemulihan data dan perisian sandaran (*backup*).

(i) Mengasingkan persekitaran berisiko tinggi untuk mengurangkan kesan bencana.

(j) Menyediakan prosedur kawalan serangan, termasuk latihan, pemulihan, dan pelaporan.

(k) Menyediakan program kesedaran dan latihan berkaitan ancaman perisian hasad.

(l) Mengumpul dan mengemas kini maklumat ancaman perisian hasad bagi tujuan pencegahan.

(m) Mengesahkan maklumat berkaitan serangan perisian hasad daripada sumber yang sahih.

(n) Memasukkan klausa tanggungan dalam kontrak pembekal perisian bagi tujuan tuntutan baik pulih sekiranya perisian mengandungi perisian berbahaya.

5.10.8 Pengurusan Kerentanan Teknikal

Maklumat berkaitan kerentanan (*vulnerability*) teknikal sistem maklumat hendaklah diperoleh tepat pada masanya, diikuti dengan penilaian tahap pendedahan organisasi terhadap kerentanan tersebut. Langkah-langkah bersesuaian perlu diambil untuk menangani risiko yang dikenal pasti bagi mencegah kelemahan sistem maklumat daripada dieksploitasi.

(1) Mengenal Pasti Kerentanan Teknikal	**Tanggungjawab**
Inventori aset hendaklah mengandungi maklumat sistem seperti nama sistem, perisian yang digunakan, nombor versi dan pemilik yang bertanggungjawab ke atas perisian tersebut.	Pentadbir Sistem Aplikasi, Pentadbir Pusat Data, Pentadbir Rangkaian, Pentadbir Keselamatan ICT

Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Menetapkan peranan dan tanggungjawab untuk mengurus kelemahan teknikal seperti pemantauan kelemahan, penilaian risiko, pengemaskinian *patches* dan lain-lain.

(b) Mengenal pasti sumber maklumat yang akan digunakan untuk mengesan kelemahan teknikal yang berkaitan dan sentiasa mengemas kini senarai aset sekiranya ada perubahan teknologi atau perisian yang digunakan.

(c) Menjalankan pengujian keselamatan untuk mengenal pasti kelemahan yang ada dan memastikan baik pulih dilaksanakan.

(d) Merancang, merekod dan menguji penilaian keselamatan secara berkala oleh pegawai atau pihak luar yang berkelayakan.

(e) Memastikan penggunaan perpustakaan (*libraries*) dan kod sumber luar yang selamat.

(2) Penilaian Kelemahan Teknikal	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi. (b) Menyemak dan mengesahkan laporan pengujian penilaian keselamatan.	Pentadbir Sistem Aplikasi

	(c) Mengenal pasti risiko dan mengambil tindakan pemulihan ke atas penemuan daripada pengujian keselamatan yang telah dilaksanakan.	
(2)	**Panduan Menangani Kelemahan Teknikal**	**Tanggungjawab**
	Proses pengurusan mengemas kini perisian hendaklah dilaksanakan untuk memastikan *patches* terkini yang diluluskan telah dipasang pada semua perisian yang dibenarkan. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Mengambil tindakan yang bersesuaian mengikut tempoh masa yang ditetapkan setelah kelemahan dikenal pasti. (b) Tindakan mengatasi kelemahan teknikal berdasarkan kategori risiko merujuk kepada pengurusan perubahan atau prosedur pengurusan pengendalian insiden keselamatan. (c) Menggunakan perisian yang terkini daripada sumber yang sah. (d) Menguji dan menilai pengemaskinian *patches* yang telah dilaksanakan sebelum dipasang pada persekitaran sebenar. (e) Memastikan *patches* sentiasa dikemas kini terutamanya kepada sistem kritikal. (f) Menguji keberkesanan ke atas tindakan pemulihan yang telah dilaksanakan. (g) Sekiranya pengemaskinian tidak berjaya dilaksanakan, kawalan berikut perlu dipatuhi:	Pentadbir Sistem Aplikasi, Pentadbir Pusat Data, Pentadbir Rangkaian, Pentadbir Keselamatan ICT

(i) Menggunakan cadangan lain yang diberikan oleh sumber yang sahih (sekiranya ada);

(ii) Menutup perkhidmatan yang terdedah akibat daripada kelemahan teknikal;

(iii) Menambah polisi kawalan akses di segmen rangkaian untuk melindungi sistem, peranti atau aplikasi yang terdedah daripada serangan;

(iv) Meningkatkan pemantauan untuk mengesan serangan sebenar; dan

(v) Meningkatkan kesedaran berkaitan dengan kelemahan teknikal.

(h) Proses pengurusan kelemahan teknikal harus dipantau dan dinilai secara berkala.

5.10.9 Pengurusan Konfigurasi

Pengurusan konfigurasi merangkumi kawalan dan pengurusan konfigurasi semua perkhidmatan, perisian, perkakasan, dan rangkaian yang digunakan oleh UM untuk memastikan keselamatan dan integriti sistem maklumat. Proses ini penting bagi mengekalkan keberkesanan, keselamatan, dan kelancaran operasi ICT.

(1) Kawalan Konfigurasi	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Konfigurasi bagi semua perkhidmatan, perisian, dan perkakasan hendaklah ditetapkan mengikut keperluan keselamatan, operasi dan fungsi yang telah ditentukan serta mematuhi peraturan yang berkuat kuasa.	Pentadbir Sistem ICT

(b) Peranan, tanggungjawab serta prosedur yang jelas hendaklah diwujudkan bagi mengawal, meluluskan, dan merekod sebarang perubahan konfigurasi bagi menjamin integriti dan ketelusan dalam pengurusan perubahan.

5.10.10 Penghapusan Maklumat

Maklumat yang disimpan dalam aset maklumat hendaklah dilupuskan mengikut prosedur yang ditetapkan. Ini bagi memastikan penghapusan maklumat dilaksanakan mematuhi keperluan perundangan dan peraturan yang berkuat kuasa.

(1) Penghapusan Maklumat	**Tanggungjawab**
Perkara berikut hendaklah dipatuhi semasa menghapuskan maklumat pada sistem, aplikasi dan perkhidmatan: (a) Memilih kaedah penghapusan yang sesuai; (b) Merekodkan keputusan penghapusan sebagai bukti; (c) Bukti penghapusan maklumat perlu disediakan oleh Pembekal sekiranya menggunakan perkhidmatan Pembekal untuk penghapusan maklumat; dan (d) Memastikan klausa penghapusan maklumat dimasukkan dalam perjanjian bersama pembekal bagi memastikan penguatkuasaan semasa dan selepas penamatan perkhidmatan.	Pentadbir Sistem ICT

(2) Kaedah Penghapusan Maklumat	**Tanggungjawab**
Kaedah penghapusan maklumat perlu dipatuhi berdasarkan perundangan dan peraturan yang	Pentadbir Sistem ICT

berkaitan. Maklumat terperingkat perlu dihapuskan sekiranya tidak diperlukan lagi mengikut kaedah berikut:

(a) Menghapuskan versi, salinan dan fail sementara yang tidak boleh digunakan lagi;

(b) Menggunakan pembekal yang diluluskan dan diperakui untuk melaksanakan perkhidmatan pelupusan;

(c) Menggunakan perisian yang diiktiraf untuk pelupusan maklumat;

(d) Menggunakan mekanisme pelupusan yang bersesuaian untuk melupuskan media storan;

(e) Sebarang media storan mudah alih seperti CDR, CDRW dan pemacu USB yang perlu dimusnahkan tidak boleh dibuang ke dalam tong sampah, sebaliknya hendaklah dilupuskan menggunakan kaedah yang selamat;

(f) Semua dokumen bercetak yang tidak diperlukan hendaklah dicincang dan dilupuskan secara selamat mengikut kesesuaian keadaan dengan kelulusan Ketua;

(g) Penyedia perkhidmatan pengkomputeran awan perlu melaksanakan penghapusan maklumat mengikut peraturan yang ditetapkan;

(h) Semasa peralatan dipulangkan kepada pembekal, media storan perlu disanitasi

dan data dihapuskan untuk mengelakkan maklumat terperingkat terdedah; dan

(i) Kaedah penghapusan maklumat perlu ditetapkan untuk menghapuskan maklumat yang disimpan dalam beberapa peranti mengikut klasifikasi maklumat yang dikendalikan oleh peranti tersebut.

5.10.11 Penopengan Data

Penopengan data ialah satu kaedah kawalan keselamatan yang digunakan untuk melindungi maklumat sensitif seperti PII daripada pendedahan tanpa kebenaran, khususnya apabila data digunakan bagi tujuan pembangunan, ujian atau latihan. Teknik ini bertujuan untuk menyembunyikan identiti sebenar prinsip data serta mencegah pemautan semula kepada individu yang boleh dikenal pasti.

(1) Teknik Penopengan Data	Tanggungjawab
Antara teknik yang digunakan untuk penyembunyian data dalam sistem aplikasi termasuk: (a) Penyulitan, iaitu data dilindungi melalui kaedah kriptografi. (b) Penopengan aksara, iaitu menghalang pengguna yang tidak dibenarkan daripada melihat mesej atau data penuh dengan menyembunyikan sebahagian kandungan, sebagai contoh, nombor kad kredit: **** **** **** 1234. (c) Penggantian nilai, iaitu menukar satu nilai kepada nilai lain yang sah dalam konteks bagi menyembunyikan maklumat sebenar tanpa menjejaskan struktur data.	Pentadbir Sistem ICT

(d) Cincangan (*hashing*), iaitu menukar data kepada bentuk unik melalui fungsi *hash* yang tidak boleh dipulihkan kepada bentuk asal, bagi tujuan pengesahan atau semakan integriti data.

(2) Pelaksanaan Penopengan Data	**Tanggungjawab**
Semasa melaksanakan penopengan data, perkara-perkara berikut hendaklah dipatuhi: (a) Akses kepada data hendaklah dihadkan mengikut keperluan. Sistem aplikasi hanya perlu memaparkan maklumat minimum yang diperlukan kepada pengguna. (b) Memastikan pematuhan terhadap semua keperluan undang-undang dan peraturan yang berkuat kuasa. (c) Menyediakan kawalan akses yang sesuai bagi melindungi data yang diproses. (d) Menyediakan jejak audit untuk merekodkan aktiviti penyediaan dan penerimaan data yang diproses.	Pentadbir Sistem ICT

5.10.12 Pencegahan Kebocoran Data

Pencegahan kebocoran data merupakan elemen penting dalam pengurusan keselamatan maklumat di Universiti Malaya. Ia merangkumi pelaksanaan langkah-langkah kawalan yang terpakai kepada semua sistem, rangkaian dan peranti yang memproses, menyimpan atau menyebarkan maklumat sensitif. Tujuannya adalah untuk memastikan kawalan pencegahan dilaksanakan secara berkesan bagi mengelakkan kebocoran atau pendedahan tidak sah ke atas maklumat terperingkat.

(1) Pelaksanaan Pencegahan Kebocoran Data	Tanggungjawab
Perkara yang perlu dilaksanakan adalah seperti berikut: (a) Mengenal pasti dan mengklasifikasikan maklumat berdasarkan tahap sensitiviti. (b) Memantau saluran atau medium berisiko yang berpotensi menjadi punca kebocoran data seperti e-mel, pemindahan fail, atau peranti storan mudah alih. (c) Melaksanakan kawalan pencegahan yang sesuai untuk menghalang kebocoran maklumat, termasuk sistem kuarantin e-mel atau sekatan capaian. (d) Menghadkan capaian pengguna kepada data sensitif berdasarkan keperluan tugas dan peranan yang ditetapkan. (e) Memastikan data yang disandarkan dilindungi dengan langkah keselamatan seperti penyulitan (*encryption*), kawalan akses dan perlindungan fizikal media storan. (f) Memastikan penggunaan mesin faksimili dilakukan dengan berhati-hati bagi mengelakkan capaian tidak sah kepada storan dalaman atau penghantaran maklumat ke nombor yang salah. (g) Memastikan individu yang mengendalikan maklumat sensitif sentiasa berhati-hati agar tidak mendedahkan maklumat sulit kepada pihak yang tidak sepatutnya.	Pentadbir Sistem ICT, Pemilik Data

(h) Individu tidak dibenarkan mengadakan komunikasi berkenaan hal-hal sulit di tempat awam, saluran komunikasi tidak selamat, pejabat atau ruang terbuka bagi mengelakkan pendedahan maklumat kepada pihak yang tidak dibenarkan.

(i) Dalam apa jua keadaan, pegawai atau mana-mana individu yang mempunyai akses tidak dibenarkan mendedahkan maklumat sulit termasuk tetapi tidak terhad kepada kod sumber, konfigurasi pelayan dan rangkaian, alamat IP, konfigurasi firewall serta maklumat teknikal lain yang seumpamanya. Peraturan ini tidak mempunyai had masa dan kekal terpakai walaupun selepas penamatan perkhidmatan atau hubungan dengan universiti.

5.10.13 Sandaran Maklumat

Salinan sandaran maklumat (*information backup*), perisian dan sistem hendaklah diambil dan diuji secara berkala mengikut prosedur sandaran yang dipersetujui. Ianya bagi memastikan semua data diselenggara dan penyimpanan data diuruskan dengan baik.

(1) Pengurusan Sandaran	**Tanggungjawab**
Melaksanakan proses sandaran dan pemulihan maklumat di Pusat Data UM, Pusat Pemulihan Bencana atau lokasi yang dibenarkan serta perlu memastikan perkara berikut dipatuhi: (a) Memastikan prosedur sandaran dan pemulihan direkodkan dengan lengkap.	Pentadbir Sistem Aplikasi, Pentadbir Pusat Data, Pentadbir Keselamatan ICT

(b) Memastikan keperluan keselamatan maklumat bagi proses sandaran dan pemulihan dipenuhi ke atas sistem kritikal yang telah dikenal pasti.

(c) Memastikan salinan sandaran disimpan di lokasi dan jarak yang selamat untuk mengelakkan sebarang kerosakan akibat bencana di Pusat Data UM.

(d) Memastikan perlindungan yang sesuai diberikan ke atas maklumat sandaran selari dengan Pusat Data UM.

(e) Menguji sistem sandaran dan pemulihan bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan.

(f) Menetapkan tempoh simpanan maklumat sandaran yang disimpan dan maklumat tersebut perlu dihapus setelah melepasi tempoh yang ditetapkan.

(g) Menyediakan prosedur pengurusan sandaran dan pemulihan.

(h) Membuat aktiviti klon ke atas semua maklumat dan sistem perisian mengikut keperluan atau apabila berlaku perubahan versi.

(i) Menyimpan salinan sandaran melebihi satu (1) media storan secara berasingan.

5.10.14 Lewahan Kemudahan Pemprosesan Maklumat

Kemudahan pemprosesan maklumat hendaklah direka bentuk dengan tahap lewahan (*redundancy*) yang mencukupi bagi memenuhi keperluan ketersediaan sistem. Tujuan utama adalah untuk memastikan

kesinambungan dan ketersediaan operasi ICT melalui penyediaan kemudahan alternatif atau sokongan tambahan.

(1) Ketersediaan Kemudahan Pemprosesan Maklumat	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Menyediakan ketersediaan lewahan (*redundancy*) rangkaian bagi kemudahan operasi ICT. (b) Menyediakan lebih daripada satu (1) kemudahan pusat data yang berlainan lokasi. (c) Menggunakan bekalan kuasa atau sumber yang berlebihan secara fizikal. (d) Menggunakan perkakasan atau perisian yang mempunyai fungsi pengimbangan beban automatik (*automatic load balancing*). (e) Mempunyai komponen pendua dalam pelayan atau rangkaian.	Pentadbir Pusat Data, Pentadbir Rangkaian

5.10.15 Penjanaan Log

Sistem yang dibangunkan hendaklah berkeupayaan merekod aktiviti dan menjana log bagi memastikan integriti maklumat serta menyediakan bahan bukti sekiranya berlaku insiden keselamatan maklumat. Log berkaitan aktiviti, pengecualian, ralat, dan peristiwa penting lain perlu dijana, disimpan, dilindungi, dan dianalisis dengan sewajarnya bagi mengelakkan akses yang tidak dibenarkan.

(1) Pengurusan Log	Tanggungjawab
Log peristiwa hendaklah diwujudkan bagi merekod aktiviti pengguna, pengecualian, ralat dan insiden keselamatan maklumat. Log	Pentadbir Sistem ICT

berfungsi sebagai bukti yang sah dan hendaklah sekurang-kurangnya merekodkan maklumat berkaitan capaian tidak sah, aktiviti luar kebiasaan serta tindakan mencurigakan.

Log perlu direkod, disimpan dan dilindungi mengikut prosedur keselamatan maklumat yang berkuat kuasa bagi mengekalkan integriti dan kerahsiaan data. Perkara yang perlu dilaksanakan adalah seperti berikut:

(a) Mewujudkan sistem log untuk merekod semua aktiviti harian pengguna dan sistem.

(b) Menyemak log secara berkala bagi mengesan ralat atau gangguan sistem, serta melaksanakan tindakan pembaikan segera.

(c) Melaporkan sebarang aktiviti tidak sah seperti pencerobohan atau kecurian maklumat kepada UMCERT.

5.10.16 Aktiviti Pemantauan

Rangkaian, sistem dan aplikasi hendaklah dipantau secara berterusan bagi mengesan sebarang tingkah laku anomali serta menilai kemungkinan berlakunya insiden keselamatan maklumat, seterusnya membolehkan tindakan sewajarnya diambil.

(1) Aspek Pemantauan	Tanggungjawab
Tahap pemantauan ditetapkan mengikut keperluan keselamatan maklumat, dasar dan polisi undang-undang yang sedang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti yang berikut:	Pentadbir Sistem ICT

(a) Trafik keluar masuk rangkaian dan sistem aplikasi;

(b) Akses ke sistem, pelayan, peranti rangkaian dan sebagainya;

(c) Fail konfigurasi bagi aplikasi dan peralatan kritikal;

(d) Log daripada peranti keselamatan;

(e) Log aktiviti sistem aplikasi dan rangkaian;

(f) Memastikan kod sumber yang sahih digunakan dan tidak diubah suai; dan

(g) Penggunaan dan keupayaan sumber seperti CPU, memori, dan *bandwidth*.

(2) Pemantauan Aktiviti Anomali	**Tanggungjawab**
Perkara yang perlu dipantau adalah seperti yang berikut: (a) Proses yang ditamatkan tanpa kebenaran; (b) Trafik aktiviti yang mengandungi perisian hasad (*malware*) atau meragukan daripada alamat domain atau alamat IP yang telah dikenal pasti terjejas; (c) Ciri-ciri serangan yang dikenal pasti seperti Serangan Penafian-Perkhidmatan Teragih (*Distributed Denial-of-Services,* DDOS); (d) Aktiviti sistem yang luar biasa seperti process *injection*; (e) Proses yang melebihi kebiasaan dan menyebabkan kesesakan trafik; (f) Akses yang tidak dibenarkan ke atas sistem;	Pentadbir Sistem ICT

(g) Pengimbasan tanpa kebenaran ke atas sistem dan rangkaian;

(h) Cubaan akses sama ada berjaya atau tidak kepada kemudahan ICT yang dilindungi seperti pelayan DNS;

(i) Aktiviti pengguna atau sistem yang luar daripada kebiasaan; dan

(j) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), spam, pemalsuan (*forgery, phishing*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*).

(3) Kawalan Pemantauan Aktiviti Anomali	**Tanggungjawab**
Perkara yang boleh dilaksanakan dalam pemantauan aktiviti anomali adalah seperti yang berikut: (a) Memanfaatkan atau menggunakan sistem risikan ancaman (*threat intelligence*); (b) Menggunakan kaedah senarai yang disekat atau dibenarkan; (c) Menggunakan penilaian teknikal keselamatan untuk mengenal pasti garis panduan ciri keselamatan yang dibenarkan; (d) Menggunakan sistem pemantauan untuk mengesan trafik yang meragukan; dan (e) Menggunakan sistem log untuk tujuan pemantauan.	Pentadbir Sistem ICT

5.10.17 Penyeragaman Waktu

Waktu bagi semua sistem pemprosesan maklumat dalam domain UM atau domain keselamatan hendaklah diseragamkan mengikut Waktu Piawai Malaysia (*Malaysia Standard Time,* MST). Penyeragaman ini bagi memastikan keselarasan rekod aktiviti keselamatan dan data lain yang direkodkan, serta menyokong proses penyiasatan insiden keselamatan maklumat.

(1) Penyelarasan Waktu	Tanggungjawab
Perkara yang boleh dilaksanakan dalam penyelarasan waktu adalah seperti berikut: (a) Memastikan waktu bagi sistem pemprosesan maklumat atau peralatan hendaklah diselaraskan dengan Waktu Piawai Malaysia (MST); dan (b) Penyelerasan waktu bagi perkhidmatan awan hendaklah mengikut Penyedia Perkhidmatan Awan (*Cloud Service Provider*) dan perbezaannya perlu dipantau dan direkodkan untuk mengurangkan risiko percanggahan.	Pentadbir Pusat Data

5.10.18 Penggunaan Program Utiliti yang Mempunyai Hak Istimewa

Penggunaan program utiliti yang mempunyai hak istimewa (*privileged utilities*) dan mampu mengatasi kawalan sistem serta aplikasi hendaklah dikawal dan dihadkan bagi mengelakkan penyalahgunaan dan pelanggaran keselamatan.

(1) Penggunaan Program Utiliti yang Mempunyai Hak Istimewa	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti berikut:	Pentadbir Sistem ICT

(a) Menghad dan mengawal bilangan pengguna yang dibenarkan untuk menggunakan program utiliti.

(b) Memastikan penggunaan ID yang unik untuk pengesahan dan kebenaran akses.

(c) Mengenal pasti dan mendokumentasikan program utiliti yang diberikan kebenaran.

(d) Memastikan penggunaan program utiliti secara *ad-hoc* adalah dengan kelulusan rasmi.

(e) Menghapuskan atau menyahaktif semua program utiliti yang tidak diperlukan.

(f) Mengasingkan repositori, ketersediaan atau capaian program utiliti daripada perisian aplikasi.

(g) Menghadkan ketersediaan program utiliti kepada hanya peranan yang memerlukan.

(h) Tidak membenarkan pengguna yang mempunyai capaian ke aplikasi menggunakan utiliti sekiranya pemisahan tugas diperlukan.

(2) Pengurusan Perisian Percuma dan Utiliti Tidak Rasmi	**Tanggungjawab**
Bagi mengelakkan ancaman keselamatan akibat pemasangan dan penggunaan perisian percuma atau utiliti tidak sah, perkara berikut hendaklah dipatuhi dan difahami: (a) Memastikan semua staf JTM, pelajar latihan industri dan staf *On-Job-Training* (OJT) yang mengendalikan komputer atau peralatan ICT (termasuk BYOD) mematuhi panduan ini.	Pentadbir Sistem ICT

(b) Memastikan komputer hanya mengandungi dan menggunakan program yang dibenarkan sahaja.

(c) Tidak membenarkan pemasangan perisian percuma yang tidak berkaitan dengan tugasan rasmi.

(d) Membenarkan pemasangan perisian percuma hanya bagi tujuan tugas rasmi dan dengan kebenaran yang sewajarnya.

(e) Memastikan perisian percuma yang dimuat turun diimbas terlebih dahulu bagi mengesan sebarang kod berbahaya seperti virus, trojan atau *malware.*

(f) Menyahpasang (*uninstall*) semua program utiliti atau perisian yang tidak lagi digunakan daripada peralatan ICT yang terlibat.

5.10.19 Pemasangan Perisian pada Operasi

Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi bagi memastikan integriti sistem operasi dan mencegah eksploitasi kelemahan teknikal.

(1) Pemasangan Perisian pada Sistem Beroperasi	**Tanggungjawab**
Pemasangan dan pengemaskinian perisian pada sistem operasi hendaklah dikawal dengan prosedur yang jelas serta dilaksanakan hanya selepas mendapat kelulusan oleh Pihak Berkuasa Melulus. Langkah-langkah berikut perlu dipatuhi:	Pentadbir Sistem Aplikasi

(a) Pengemaskinian versi sistem pengoperasian hanya boleh dilaksanakan oleh Pentadbir Sistem Aplikasi.

(b) Memastikan hanya kod boleh laksana (*executable code*) yang diluluskan dan tiada kod pembangunan atau pengkompil (*compilers*) dipasang pada sistem operasi.

(c) Memasang dan mengemas kini perisian yang telah diuji keberkesanan sahaja.

(d) Memastikan semua perpustakaan sumber program (*source code library*) adalah terkini.

(e) Mengawal dan mendokumentasikan setiap konfigurasi ke atas sistem dan perisian dengan teratur.

(f) Melaksanakan strategi *rollback* sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian.

(g) Memastikan log audit direkodkan bagi semua pengemaskinian dalam perpustakaan sumber program (*source code library*).

(h) Mengarkibkan versi lama perisian bersama-sama dengan semua maklumat dan parameter, prosedur, butiran konfigurasi dan perisian sokongan yang diperlukan sebagai langkah luar jangka (*contigency*), dan selagi perisian itu diperlukan untuk membaca atau memproses data yang diarkibkan.

(2) Sekatan ke atas Pemasangan Perisian	Tanggungjawab
Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Hanya perisian yang diperaku sahaja dibenarkan bagi kegunaan warga UM, pembekal serta pihak yang mempunyai urusan dengan perkhidmatan ICT UM. (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana perundangan bertulis yang berkuat kuasa. (c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya.	Warga UM, Pentadbir Sistem ICT

5.10.20 Keselamatan Rangkaian

Infrastruktur rangkaian hendaklah dilindungi, dikawal dan diurus bagi memastikan maklumat dalam sistem dan aplikasi sentiasa selamat daripada sebarang ancaman atau kompromi. Langkah ini penting bagi melindungi infrastruktur rangkaian serta kemudahan pemprosesan maklumat yang berkaitan.

(1) Kawalan Rangkaian	Tanggungjawab
Kawalan hendaklah dilaksanakan untuk memastikan keselamatan maklumat dalam rangkaian dan untuk melindungi perkhidmatan yang disambungkan daripada capaian yang tidak dibenarkan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Tahap pengelasan maklumat yang diuruskan dalam rangkaian UM.	Pentadbir Rangkaian

(b) Menetapkan tanggungjawab dan prosedur bagi pengurusan peranti rangkaian.

(c) Memastikan pengemaskinian maklumat rangkaian secara berterusan seperti diagram rangkaian dan fail konfigurasi peranti.

(d) Mengasingkan tanggungjawab operasi untuk rangkaian daripada operasi sistem ICT sekiranya perlu.

(e) Menetapkan kawalan untuk melindungi kerahsiaan dan integriti maklumat yang melalui rangkaian awam, rangkaian pihak ketiga atau rangkaian tanpa wayar.

(f) Memantau secara berkala log masuk untuk mengesan insiden keselamatan.

(g) Melaksanakan aktiviti pengurusan rangkaian secara berterusan memastikan perkhidmatan yang optimum.

(h) Melaksanakan pengesahan pengguna sebelum mengakses rangkaian.

(i) Menghadkan dan mengawal akses ke rangkaian mengikut peranan dan keperluan.

(j) Memastikan tindakan pengukuhan ke atas peranti rangkaian.

(k) Mengasingkan sementara segmen rangkaian yang terjejas sehingga dipulihkan semula.

(l) Melumpuhkan protokol rangkaian yang terdedah kepada ancaman.

(m) Peralatan rangkaian hendaklah diletakkan di lokasi yang bebas daripada risiko seperti banjir, gegaran dan habuk.

(n) Semua trafik rangkaian hendaklah melalui peranti keselamatan rangkaian UM termasuk rangkaian persendirian maya (VPN) atau rangkaian tanpa wayar (WiFi).

(o) Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi SLA yang telah ditetapkan.

5.10.21 Keselamatan Perkhidmatan Rangkaian

Mekanisme keselamatan, tahap perkhidmatan dan keperluan perkhidmatan rangkaian hendaklah dikenal pasti, dilaksanakan dan dipantau secara berterusan bagi memastikan penggunaan perkhidmatan rangkaian adalah selamat, terkawal dan memenuhi keperluan organisasi.

(1) Perkhidmatan Rangkaian	**Tanggungjawab**
Penggunaan dan perkhidmatan rangkaian hendaklah dilaksanakan meliputi: (a) Mempunyai kawalan akses kepada perkhidmatan rangkaian yang disediakan. (b) Melaksanakan pengesahan identiti bagi mengakses perkhidmatan rangkaian. (c) Mengawal akses kepada perkhidmatan rangkaian mengikut peranan yang diluluskan. (d) Menyediakan prosedur pengurusan rangkaian bagi kawalan keselamatan kepada perkhidmatan rangkaian. (e) Menggunakan kaedah yang selamat bagi mengakses perkhidmatan rangkaian seperti penggunaan rangkaian	Pentadbir Rangkaian, Pentadbir Keselamatan ICT

	persendirian maya (VPN) atau rangkaian tanpa wayar. (f) Merekodkan maklumat seperti masa, lokasi dan lain-lain semasa penggunaan perkhidmatan rangkaian. (g) Memantau penggunaan perkhidmatan rangkaian. (h) Pengurusan perkhidmatan rangkaian hendaklah dikenal pasti dan dinyatakan dalam perjanjian perkhidmatan rangkaian. (i) Pentadbir Rangkaian dan Keselamatan bertanggungjawab ke atas insiden keselamatan yang melibatkan perkhidmatan rangkaian.	
(2)	**Aspek Keselamatan Perkhidmatan Rangkaian**	**Tanggungjawab**
	Aspek keselamatan perkhidmatan rangkaian yang perlu diambil adalah seperti berikut: (a) Menggunakan teknologi keselamatan perkhidmatan rangkaian seperti pengesahan identiti, kawalan akses atau penggunaan enkripsi. (b) Memastikan peralatan rangkaian mematuhi polisi parameter yang ditetapkan bagi menjamin keselamatan sambungan rangkaian. (c) Memastikan kawalan akses keapda perkhidmatan rangkaian dan sistem aplikasi mengikut peranan yang diluluskan. (d) Memastikan trafik rangkaian dipantau dan dikawal oleh peralatan keselamatan.	Pentadbir Rangkaian

5.10.22 Pengasingan Rangkaian

Pengasingan rangkaian bertujuan untuk mewujudkan sempadan keselamatan antara kumpulan sistem, perkhidmatan dan pengguna yang berbeza, serta mengawal trafik antara domain rangkaian mengikut keperluan keselamatan dan operasi.

(1) Panduan Pengasingan Rangkaian	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengasingkan akses rangkaian mengikut tahap kritikal dan sensitiviti atau lain-lain keperluan. (b) Memastkan penggunaan peralatan keselamatan seperti firewall atau router bagi mengawal segmen rangkaian. (c) Melaksanakan polisi kawalan akses melalui *gateway*. (d) Mengasingkan rangkaian tanpa wayar dengan rangkaian dalaman kecuali dengan menggunakan kawalan keselamatan seperti *firewall*. (e) Mengasingkan akses rangkaian tanpa wayar untuk pelawat dan warga UM. (f) Mengawal akses kepada peralatan rangkaian bagi pengguna yang dibenarkan sahaja. (g) Mengemas kini hak akses pengguna dan pentadbir sekiranya berlaku perubahan tanggungjawab.	Pentadbir Sistem ICT

5.10.23 Penapisan Web

Kawalan penapisan web hendaklah dilaksanakan bagi menyekat capaian ke laman web yang tidak selamat dan tidak sesuai. Langkah ini penting

untuk melindungi sistem maklumat Universiti daripada ancaman siber serta memastikan penggunaan internet yang terkawal dan beretika.

(1) Kawalan Penapisan Web	Tanggungjawab
UM hendaklah mengurangkan risiko mencapai laman web yang mengandungi maklumat yang dilarang atau diketahui mengandungi virus atau data pancingan (*phishing*) data oleh pengguna. UM hendaklah mengenal pasti jenis laman web yang patut atau tidak boleh dicapai oleh warga Universiti. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Menyekat alamat IP atau domain laman web yang tidak sah. (b) Memantau laman web yang mempunyai fungsi muat naik maklumat. (c) Menyekat laman web berbahaya seperti *phishing* dan *malicious code*. (d) Mengemas kini pangkalan data (*signature database*) peralatan keselamatan web melalui sumber yang sahih. (e) Menyekat laman web perkongsian maklumat yang tidak sah (*illegal*). (f) Memberikan latihan teknikal kepada staf teknikal mengenai pengendalian peralatan penapisan laman web. (g) Memberikan program kesedaran kepada pengguna mengenai tatacara akses laman web yang selamat.	Pentadbir Rangkaian, Pentadbir Keselamatan ICT

5.10.24 Penggunaan Kriptografi

Penggunaan kriptografi hendaklah dikawal melalui peraturan yang jelas dan pelaksanaan yang berkesan. Langkah ini bertujuan untuk memastikan kerahsiaan, ketulenan dan integriti maklumat dilindungi berdasarkan keperluan keselamatan maklumat serta keperluan perundangan, peraturan dan kontrak yang berkaitan.

(1) Penggunaan Kawalan Kriptografi	Tanggungjawab
Penggunaan kriptografi perlu mematuhi perkara seperti berikut: (a) Data sulit atau sensitif semasa penghantaran, dan yang disimpan hendaklah disulitkan. (b) Mengenal pasti tahap perlindungan penggunaan kriptografi dengan mengambil kira jenis, kekuatan dan kualiti algoritma yang diperlukan, seperti SHA, dengan kekuatan sekurang-kurangnya 256 bit. (c) Memaksimumkan faedah, meminimumkan risiko dan mengelak penyalahgunaan kriptografi berdasarkan kepada peraturan yang berkuat kuasa. (d) Menetapkan kesesuaian penggunaan kriptografi berdasarkan keperluan di UM. (e) Media storan perlu dilaksanakan kata laluan bagi mengelakkan pencerobohan maklumat. (f) Semua pelayan yang digunakan untuk pengesahan (contohnya RADIUS, TACACS atau CAS) mesti mempunyai sijil	Pentadbir Rangkaian, Pentadbir Pusat Data, Pentadbir Sistem Aplikasi, Pentadbir Keselamatan ICT

yang sah dan ditandatangani oleh penyedia yang dikenali dan dipercayai.

(g) Semua pelayan dan aplikasi yang menggunakan SSL atau TLS mesti mempunyai sijil yang ditandatangani oleh penyedia yang dikenali dan dipercayai.

(h) Kunci kriptografi mesti dijana dan disimpan secara selamat bagi mengelakkan kehilangan, kecurian atau kompromi.

(i) Sekiranya kunci persendirian dan sijil terkompromi, kelemahan keselamatan yang menyebabkan kompromi tersebut hendaklah diperbaiki, kemudian cipta semula kunci persendirian dan kod Permintaan Penandatanganan Sijil (CSR) serta keluarkan semula atau gantikan sijil tersebut.

(j) Penggunaan SSL adalah diwajibkan bagi semua sistem aplikasi atau pertukaran maklumat dengan pihak ketiga.

5.10.25 Kitaran Hayat Pembangunan Selamat

Prosedur bagi pembangunan sistem aplikasi hendaklah disedia dan digunakan untuk memastikan pembangunan sistem aplikasi mengguna pakai kitar hayat pembangunan yang selamat.

(1) Pembangunan Sistem yang Selamat	Tanggungjawab
Prosedur pembangunan dan penyelenggaran sistem aplikasi adalah berdasarkan prosedur yang berkuat kuasa. Perkara yang perlu dipertimbangkan adalah seperti berikut:	Pentadbir Sistem Aplikasi, Pentadbir Keselamatan ICT, Pentadbir Pusat Data

(a) Keselamatan dalam fasa spesifikasi dan reka bentuk, serta persekitaran pembangunan, ujian dan produksi.

(b) Pelaksanaan pengujian sistem dan keselamatan sebelum dilaksanakan dalam persekitaran produksi.

(c) Repositori selamat untuk kod sumber dan konfigurasi.

(d) Keselamatan dalam kawalan versi.

(e) Keperluan pengetahuan keselamatan dalam pembangunan sistem aplikasi.

(f) Keupayaan pembangun untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem.

(g) Memastikan pematuhan keperluan pelesenan dan mengenal pasti alternatif yang sesuai bagi menjamin penyelesaian yang kos efektif serta mengelakkan isu pelesenan pada masa hadapan.

5.10.26 Keperluan Keselamatan Aplikasi

Keperluan keselamatan maklumat hendaklah dikenal pasti, dinyatakan dengan jelas dan mendapat kelulusan sewajarnya bagi memastikan aspek keselamatan seperti kerahsiaan, integriti dan ketersediaan maklumat ditangani secara menyeluruh sepanjang kitar hayat aplikasi.

(1) Keperluan Keselamatan Aplikasi	Tanggungjawab
Keperluan keselamatan aplikasi yang perlu diambil kira adalah seperti berikut: (a) Memastikan pengguna mempunyai tahap akses yang dibenarkan.	Pentadbir Sistem Aplikasi

(b) Mengenal pasti jenis maklumat dan tahap klasifikasi yang akan diproses oleh sistem aplikasi.

(c) Memastikan sistem aplikasi berdaya tahan terhadap ancaman siber seperti *malware* dan *SQL injections*.

(d) Memastikan transaksi dan data yang dijana, diproses atau disimpan adalah dilindungi serta mematuhi peraturan yang berkuat kuasa.

(e) Memastikan maklumat sulit dilindungi.

(f) Melaksanakan pengesahan input.

(g) Melaksanakan pengendalian mesej ralat.

(2) Transaksi Perkhidmatan dalam Talian	**Tanggungjawab**
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 yang perlu dipertimbangkan adalah seperti yang berikut: (a) Memastikan pengguna mempunyai tahap akses yang dibenarkan. (b) Memastikan penggunaan mekanisme seperti tandatangan digital, *hashing* dan lain-lain untuk mengesahkan identiti penghantar dan penerima semasa pertukaran data.	Pentadbir Sistem Aplikasi, Pemilik Proses

(3) Aplikasi Pesanan dan Pembayaran Elektronik	Tanggungjawab
Perkara berikut perlu dipatuhi: (a) Mengekalkan kerahsiaan dan integriti maklumat pesanan atau pembayaran; (b) Mengesahkan maklumat pembayaran oleh pelanggan; (c) Mengelakkan kehilangan atau pertindihan maklumat transaksi; (d) Menyimpan maklumat transaksi di lokasi yang selamat dan tidak boleh diakses oleh umum; dan (e) Menggunakan tandatangan atau sijil digital yang sah dan dikeluarkan oleh pihak yang diberi kuasa (*authority*).	Pentadbir Sistem Aplikasi, Pemilik Proses

5.10.27 Prinsip Reka Bentuk dan Kejuruteraan Sistem yang Selamat

Prinsip kejuruteraan keselamatan sistem hendaklah diwujudkan, didokumenkan, dikaji dan diguna pakai ke atas semua pembangunan sistem aplikasi. Ianya bagi memastikan sistem maklumat direka bentuk, dilaksanakan dan dikendalikan dengan selamat dalam kitar hayat pembangunan.

(1) Kriteria Kejuruteraan Sistem yang Selamat	Tanggungjawab
Prinsip kejuruteraan sistem memberikan panduan tentang teknik pengesahan pengguna, kawalan sesi selamat dan pengesahan dan sanitasi data. Prinsip kejuruteraan sistem selamat harus merangkumi analisis: (a) Menyediakan kawalan keselamatan yang diperlukan untuk melindungi maklumat	Pentadbir Sistem Aplikasi

dan sistem aplikasi daripada ancaman yang dikenal pasti.

(b) Mempunyai keupayaan kawalan keselamatan untuk mencegah, mengesan atau melaksanakan tindakan ke atas insiden keselamatan.

(c) Mempunyai kawalan keselamatan khusus mengikut keperluan proses perkhidmatan.

(d) Memastikan prinsip kejuruteraan mengaplikasikan reka bentuk keselamatan.

(e) Mempunyai kepakaran untuk membangunkan dan menyelenggarakan sistem aplikasi selari dengan teknologi yang digunakan atau dipilih.

(f) Mengguna pakai konsep amalan terbaik (*best practise*).

(g) Melaksanakan pengukuhan (*hardening*) ke atas sistem aplikasi.

(2) Prinsip "Zero Trust"	**Tanggungjawab**
Perkara yang perlu diambil kira adalah seperti yang berikut: (a) Kawalan keselamatan tidak boleh bergantung sepenuhnya kepada peralatan keselamatan rangkaian. (b) Menyemak dan mengesahkan identiti bagi semua akses ke sistem aplikasi. (c) Memastikan sistem aplikasi menggunakan fungsi enkripsi. (d) Menyemak dan mengesahkan semua permohonan akses yang diterima.	Pentadbir Sistem Aplikasi

(e) Memberikan kategori akses paling minimum kepada pengguna.

(f) Menggunakan pengesahan keselamatan ketika log masuk atau transaksi yang melibatkan sistem aplikasi.

5.10.28 Pengekodan Selamat

Prinsip pengekodan selamat hendaklah diterapkan dalam pembangunan sistem aplikasi bagi meminimumkan potensi kelemahan keselamatan maklumat. Pemantauan terhadap ancaman keselamatan semasa serta penambahbaikan berterusan perlu dilaksanakan bagi mengekalkan keberkesanan amalan ini.

(1) Fasa Perancangan Pengekodan Selamat	**Tanggungjawab**
Perkara yang perlu diambil kira adalah seperti berikut: (a) Pembangunan sistem aplikasi sama ada secara dalaman (*in-house*) atau luaran (*outsource*) hendaklah menggunakan pengekodan selamat berdasarkan kepada peraturan dan keperluan yang dikuatkuasakan. (b) Penggunaan persekitaran pembangunan semasa fasa pembangunan sistem aplikasi. (c) Memastikan penggunaan perisian pembangunan yang terkini. (d) Memastikan pengaturcaraan atau pihak ketiga yang dilantik mempunyai kemahiran dalam pembangunan sistem aplikasi menggunakan pengekodan selamat.	Pentadbir Sistem Aplikasi

(e) Memastikan arkitektur, reka bentuk dan piawaian pengekodan digunakan dalam persekitaran yang selamat.

(2) Fasa Semasa Pengekodan Selamat	**Tanggungjawab**
Perkara yang perlu diambil kira adalah seperti berikut: (a) Memastikan penggunaan teknik dan struktur pengekodan selamat bagi bahasa pengaturcaraan yang digunakan seperti pengaturcaraan pasangan, pemfaktoran semula (*refactoring*), semakan rakan sebaya (*peer review*), ulangan keselamatan (*security iteration*) dan pembangunan dipacu ujian (*test-driven development*). (b) Merekod dan memperbetulkan kelemahan kod sumber yang boleh terdedah kepada ancaman daripada dieksploitasi. (c) Menggunakan perisian yang terkini dan tidak tamat tempoh *End of Support* (EOS). (d) Memastikan tidak menggunakan teknik pembangunan yang tidak selamat seperti kata laluan *hard-coded*, sampel kod yang tidak diluluskan dan perkhidmatan web yang tidak disahkan. (e) Melaksanakan pengujian keselamatan maklumat dan tindakan pembaikan. (f) Memastikan keupayaan integrasi dengan sistem maklumat yang lain.	Pentadbir Sistem Aplikasi

(3) Fasa Penyelenggaraan dan Kajian Semula	Tanggungjawab
Perkara yang perlu diambil kira adalah seperti berikut: (a) Memastikan *patches* dan *security updates* perisian sentiasa dikemas kini. (b) Kelemahan keselamatan maklumat yang dilaporkan hendaklah diambil tindakan. (c) Ralat dan cubaan serangan hendaklah direkodkan serta disemak secara berkala bagi penambahbaikan ke atas kod pengaturcaraan sekiranya perlu. (d) Kod sumber hendaklah dilindungi daripada akses dan gangguan yang tidak dibenarkan seperti menggunakan fungsi kawalan akses dan kawalan versi.	Pentadbir Sistem Aplikasi

5.10.29 Pengujian Keselamatan Semasa Pembangunan dan Penerimaan

Proses pengujian keselamatan hendaklah dilaksanakan sepanjang kitaran hayat pembangunan sistem bagi memastikan keperluan keselamatan maklumat dipenuhi sebelum aplikasi digunakan dalam persekitaran sebenar.

(1) Pengujian Keselamatan Sistem Aplikasi	Tanggungjawab
Pengujian keselamatan hendaklah merangkumi perkara berikut: (a) Fungsi keselamatan sistem aplikasi hendaklah diuji semasa fasa pembangunan seperti pengesahan pengguna, kawalan akses, penggunaan kriptografi dan pengekodan selamat;	Pembangun Sistem, Pentadbir Sistem Aplikasi, Pentadbir Pusat Data, Pentadbir Keselamatan ICT

(b) Konfigurasi keselamatan yang melibatkan sistem pengoperasian, *firewalls* dan komponen keselamatan lain hendaklah diuji;

(c) Menyemak dan mengesahkan data sebelum dikunci masuk dalam sistem aplikasi bagi menjamin ketepatan maklumat; dan

(d) Melaksanakan semakan dan pengesahan ke atas output data yang dihasilkan oleh sistem aplikasi.

(2) Pelan Pengujian Penerimaan Sistem	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Menyediakan jadual aktiviti pengujian; (b) Menyediakan input dan output yang dijangka supaya memenuhi senarai syarat yang telah ditentukan; (c) Menetapkan kriteria untuk menilai keputusan; (d) Memastikan proses kerja sistem aplikasi memenuhi keperluan pengguna; (e) Melaksanakan pengujian fungsi ke atas sistem aplikasi menggunakan data palsu (*dummy input*); (f) Melaksanakan keputusan pengujian yang memerlukan tindakan lanjut sekiranya diperlukan; (g) Melaksanakan integrasi dan pengujian dengan sistem aplikasi yang lain sekiranya berkaitan; dan	Pembangun Sistem, Pentadbir Sistem Aplikasi, Pentadbir Pusat Data, Pentadbir Keselamatan ICT

	(h) Melaksanakan ujian prestasi (*performance test*) dan ujian tekanan (*stress test*).	
(3)	**Pengujian Bebas bagi Pembangunan Dalaman dan Luaran**	**Tanggungjawab**
	Pengujian perlu dilaksanakan oleh selain daripada pasukan pembangunan sistem aplikasi. Perkara berikut perlu diambil kira seperti: (a) Melaksanakan aktiviti semakan kod pengaturcaraan untuk mengenal pasti kelemahan termasuk input dan ralat yang tidak dijangka; (b) Melaksanakan pengimbasan kelemahan untuk mengenal pasti konfigurasi yang tidak selamat dan kelemahan sistem aplikasi; (c) Melaksanakan pengujian penembusan (*penetration testing*) untuk mengenal pasti reka bentuk dan kod sumber tidak selamat; (d) Penilaian produk dan perkhidmatan hendaklah dilaksanakan sebelum perolehan dilaksanakan; (e) Perjanjian bersama pihak ketiga perlu mengandungi keperluan keselamatan; (f) Pembangunan secara luaran (*outsource*) atau pembelian komponen hendaklah mengikut tatacara perolehan; dan (g) Persekitaran pengujian hendaklah sama dengan persekitaran sebenar supaya pengujian tersebut tidak boleh disangkal dan boleh dipercayai.	Pembangun Sistem, Pentadbir Sistem Aplikasi, Pentadbir Pusat Data, Pentadbir Keselamatan ICT

5.10.30 Pembangunan Sistem secara Luaran

UM hendaklah menetapkan, memantau dan menilai pematuhan keperluan keselamatan maklumat oleh pihak ketiga bagi pembangunan sistem melalui penyumberan luar, bagi memastikan langkah keselamatan yang diperlukan dilaksanakan sepanjang proses pembangunan.

(1) Pembangunan secara Luaran	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Memastikan perjanjian lesen, *Intellectual Property Rights* (IPR) dan kod sumber menjadi hak milik Universiti; (b) Memastikan spesifikasi perolehan mengandungi klausa berhubung keperluan keselamatan reka bentuk, keselamatan pengaturcaraan, pengujian, pensijilan keselamatan produk, ketersediaan kod sumber, keperluan pelupusan data, keutamaan terhadap teknologi dan kepakaran tempatan serta keperluan kompetensi pasukan pembangunan; (c) Menyediakan penilaian keselamatan oleh pihak ketiga; (d) Melaksanakan pengujian penerimaan untuk memastikan kualiti dan output memenuhi keperluan; (e) Memastikan pembuktian risiko penilaian keselamatan dan privasi di tahap minimum yang boleh diterima; (f) Memastikan pengujian keselamatan, kelemahan yang dikenal pasti dan	Pembangun Sistem, Pentadbir Sistem Aplikasi, Pentadbir Pusat Data, Pentadbir Keselamatan ICT

tindakan pembetulan dilaksanakan adalah mencukupi sebelum penyerahan projek;

(g) Menguatkuasakan bon perjanjian sekiranya pihak ketiga tidak memenuhi perkhidmatan;

(h) Memasukkan klausa dalam kontrak yang membenarkan pelaksanaan audit terhadap proses pembangunan dan kod sumber;

(i) Melaksanakan keperluan keselamatan untuk persekitaran pembangunan;

(j) Mengambil kira perundangan yang berkuat kuasa seperti Akta Perlindungan Data Peribadi (APDP); dan

(k) Pembangunan sistem aplikasi perlu mendapatkan kelulusan teknikal dan kebolehlaksanaan sistem sebelum dibangunkan.

5.10.31 Pengasingan Persekitaran Pembangunan, Pengujian dan Produksi

Persekitaran pembangunan, pengujian dan produksi hendaklah diasingkan dan dilindungi dengan langkah keselamatan yang sesuai bagi memastikan keselamatan maklumat terpelihara serta mengelakkan akses tidak dibenarkan.

(1) Aspek Pengasingan Persekitaran ICT	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Mengasingkan persekitaran sebenar dengan pembangunan dalam domain yang berbeza secara maya atau fizikal;	Pembangun Sistem, Pentadbir Sistem Aplikasi, Pentadbir Pusat Data, Pentadbir Keselamatan ICT

	(b) Menetapkan, merekodkan dan melaksanakan peraturan serta pengesahan untuk migrasi sistem aplikasi atau perisian daripada persekitaran pembangunan kepada persekitaran produksi; (c) Melaksanakan pengujian ke atas perubahan sistem aplikasi di persekitaran pengujian sebelum digunakan dalam produksi; (d) Tidak menggunakan maklumat sebenar atau sensitif pada persekitaran pembangunan atau pengujian kecuali dengan kawalan keselamatan yang setara disediakan dan diluluskan; (e) Memastikan penyusun (*compilers*), penyunting dan alat-alat pembangunan atau program utiliti lain tidak boleh diakses daripada persekitaran produksi apabila tidak diperlukan lagi; (f) Memaparkan label yang bersesuaian dengan persekitaran pada menu untuk mengurangkan risiko ralat; (g) Merekodkan semua penggunaan sumber yang dilaksanakan; dan (h) Memantau pelaksanaan penggunaan sumber bagi tujuan perancangan kapasiti.	
(2)	**Langkah Keselamatan bagi Persekitaran Pembangunan, Pengujian dan Produksi**	**Tanggungjawab**
	Perkara yang perlu dipatuhi adalah seperti yang berikut:	Pembangun Sistem, Pentadbir Sistem

(a) Mengemas kini *patches*, pembangunan sistem aplikasi, integrasi dan alat-alat pengujian seperti *builders, integrators, compilers*, sistem konfigurasi dan *libraries*; (b) Memastikan keselamatan konfigurasi sistem aplikasi dan operasi perisian selamat; (c) Memantau dan memastikan kawalan akses persekitaran; (d) Memantau kawalan perubahan persekitaran dan kod yang disimpan; dan (e) Menyediakan sandaran *(backup*) persekitaran produksi secara berkala.	Aplikasi, Pentadbir Pusat Data, Pentadbir Keselamatan ICT

5.10.32 Pengurusan Perubahan

Perubahan terhadap kemudahan pemprosesan maklumat, sistem maklumat dan proses berkaitan hendaklah dikawal melalui prosedur yang didokumenkan dan dikuatkuasakan bagi memastikan pengurusan perubahan dalam persekitaran ICT mengambil kira kawalan keselamatan maklumat.

(1) Pengurusan Perubahan	**Tanggungjawab**
Penyedia dokumen perlu memastikan pengurusan perubahan yang didokumenkan mematuhi perkara-perkara seperti yang berikut: (a) Merancang dan menilai impak yang mungkin berlaku ke atas pihak lain yang mempunyai kepentingan atau kebergantungan; (b) Memastikan perubahan yang dilaksanakan telah mendapat kelulusan;	Pentadbir Sistem Aplikasi, Pentadbir Pusat Data, Pentadbir Keselamatan ICT, Pentadbir Rangkaian, Pemilik Proses

(c) Memastikan perubahan yang dilaksanakan dimaklumkan kepada pihak berkepentingan;

(d) Memastikan semua aktiviti pengubahsuaian seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem aplikasi dikendalikan oleh pihak yang dibenarkan;

(e) Memastikan semua aktiviti pengubahsuaian komponen sistem ICT mematuhi spesifikasi perubahan yang telah ditetapkan; dan

(f) Memastikan semua aktiviti perubahan atau pengubahsuaian direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau tidak sengaja.

(2) Prosedur Kawalan Perubahan Sistem	**Tanggungjawab**
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 adalah seperti yang berikut: (a) Perubahan atau pengubahsuaian ke atas perkakasan, perisian atau sistem aplikasi hendaklah diuji, direkodkan dan disahkan sebelum diguna pakai; (b) Memastikan pelaksanaan perubahan mengambil kira perancangan pembangunan;	Pentadbir Sistem Aplikasi, Pemilik Proses

(c) Memastikan prosedur pembentukan semula (*fallback*) dilaksanakan sebagai pelan perancangan luar jangka (*contingency*);	
(d) Merekodkan semua perubahan yang dilaksanakan;	
(e) Memastikan manual operasi pengguna dan sistem aplikasi diubah mengikut keperluan;	
(f) Memastikan prosedur pelan kesinambungan perkhidmatan dan pemulihan ICT diubah mengikut keperluan;	
(g) Setiap perubahan kepada sistem pengoperasian perlu dikaji semula dan diuji untuk memastikan tiada sebarang masalah yang timbul terhadap keselamatan maklumat;	
(h) Perubahan kepada kod pengaturcaraan (*source code*) perlu dihadkan kepada Pentadbir Sistem Aplikasi yang dibenarkan; dan	
(i) Memastikan aktiviti seperti memasang, menyenggara, menghapus dan mengemas kini mana-mana komponen ICT mendapatkan kelulusan.	
(3) Kawalan Perubahan kepada Platform	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:	Pentadbir Sistem Aplikasi, Pentadbir Pusat Data, Pentadbir Keselamatan ICT, Pemilik Proses
(a) Perubahan platform hendaklah dikaji bagi membolehkan pengujian yang	

bersesuaian dilakukan sebelum pelaksanaan;

(b) Memastikan sistem aplikasi, integriti data dan kawalan akses disemak supaya operasi sistem tidak terjejas apabila perubahan platform dilaksanakan;

(c) Ujian penerimaan pengguna perlu dilaksanakan setelah perubahan platform selesai dilaksanakan; dan

(d) Memastikan perubahan yang sesuai diselaraskan kepada pelan kesinambungan perkhidmatan.

(4) Kawalan Perubahan kepada Perisian	**Tanggungjawab**
Pengubahsuaian ke atas pakej perisian tidak digalakkan dan terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal dengan ketat. Antara perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan pakej perisian mengambil kira aspek keselamatan maklumat; (b) Perubahan pakej perisian hanya dilaksanakan oleh pihak yang dibenarkan sahaja; (c) Melaksanakan pengujian ke atas pakej perisian yang terkini sebelum memaklumkan kepada pengguna; dan (d) Memastikan perubahan pakej perisian tidak menjejaskan perkhidmatan operasi sistem maklumat.	Pentadbir Sistem Aplikasi

5.10.33 Data Pengujian

Maklumat ujian hendaklah dipilih, dilindungi dan diurus dengan sewajarnya bagi memastikan data yang digunakan semasa pengujian dikawal selaras dengan keperluan keselamatan dan peraturan yang ditetapkan.

(1) Perlindungan Data Ujian	Tanggungjawab
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 berikut: (a) Melaksanakan kawalan yang sama di persekitaran produksi dan pengujian; (b) Menyediakan hak akses yang berlainan setiap kali maklumat digunakan ke persekitaran pengujian; (c) Menyimpan log penyalinan dan penggunaan maklumat operasi bagi tujuan jejak audit; (d) Memastikan data input dan output bagi pengujian sistem aplikasi disahkan akan ketepatannya; (e) Melindungi maklumat sensitif dengan pelaksanaan penyembunyian data dan menghapuskan data selepas pengujian selesai; dan (f) Menghapuskan data sebenar dari persekitaran pengujian selepas pengujian selesai untuk mengelakkan data digunakan oleh pihak yang tidak dibenarkan.	Pembangun Sistem, Pentadbir Sistem Aplikasi, Pentadbir Pusat Data, Pentadbir Keselamatan ICT, Pemilik Proses

5.10.34 Perlindungan Sistem Maklumat semasa Ujian Audit

Ujian audit dan aktiviti jaminan lain yang melibatkan penilaian sistem operasi hendaklah dirancang dengan teliti dan dipersetujui oleh pihak pengurusan dan penguji bagi meminimumkan kesan terhadap sistem operasi dan kelangsungan perkhidmatan.

(1) Panduan Ujian Audit	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Mendapatkan kebenaran untuk capaian kepada sistem aplikasi dan data bagi ujian audit; (b) Mendapatkan kebenaran untuk melaksanakan ujian audit berdasarkan kawalan dan skop yang dibenarkan; (c) Memastikan data yang dibenarkan hanya berstatus *read only* semasa ujian audit dilaksanakan; (d) Jika terdapat keperluan capaian kepada sistem aplikasi, pengujian hendaklah dilaksanakan oleh pentadbir yang dibenarkan bagi membantu juruaudit; (e) Memastikan keperluan keselamatan perkakasan juruaudit dipatuhi seperti penggunaan antivirus sebelum kebenaran diberikan; (f) Membenarkan capaian kepada sistem fail oleh juruaudit dan menghapuskan data tersebut setelah audit selesai atau melaksanakan kawalan keselamatan yang bersesuaian;	Pembangun Sistem, Pentadbir Sistem Aplikasi, Pentadbir Pusat Data, Pentadbir Keselamatan ICT, Pemilik Proses

(g) Memastikan penggunaan peralatan audit (*audit tools*) mendapat kelulusan terlebih dahulu;

(h) Melaksanakan ujian audit di luar waktu bekerja sekiranya menyebabkan gangguan perkhidmatan; dan

(i) Menyimpan dan memantau semua akses semasa ujian audit.

6.0 TADBIR URUS PERKHIDMATAN ICT

6.1 PENGENALAN

Perkhidmatan ICT merangkumi penyediaan infrastruktur dan infostruktur ICT yang disediakan kepada warga Universiti bagi menyokong aktiviti pengajaran, pembelajaran, penyelidikan, dan pengurusan operasi pentadbiran. Skop perkhidmatan ini meliputi keselamatan siber, pengurusan sistem dan aplikasi, rangkaian, pelayan, serta pengurusan perkakasan ICT, bagi memastikan maklumat dapat disimpan, diproses, dan dihantar secara cekap, berintegriti dan selamat.

JTM bertanggungjawab sebagai penyedia utama perkhidmatan ICT Universiti kepada PTj dan seluruh warga kampus, selaras dengan garis panduan serta arahan kerja yang berkuat kuasa.

Antara perkhidmatan ICT yang ditawarkan adalah termasuk:

(1) Keselamatan Siber;

(2) Perolehan ICT;

(3) Pembangunan/Perolehan Sistem Aplikasi;

(4) Perkhidmatan Rangkaian;

(5) Perkhidmatan Pelayan;

(6) Pengurusan Perkakasan dan Perisian ICT; dan

(7) Perkhidmatan Sokongan ICT.

6.2 TUJUAN

Perkhidmatan ICT disediakan bagi memudahkan pertukaran maklumat, meningkatkan kecekapan operasi dan akses kepada data, serta menyediakan pelbagai perkhidmatan teknologi yang membantu Universiti mencapai misi dan visi. Tujuan utama perkhidmatan ICT termasuklah:

(1) Peningkatan kecekapan melalui penyediaan alat dan perisian yang membolehkan pengguna menjalankan tugas dengan lebih cekap dan pantas.

(2) Pertukaran maklumat yang berkesan bagi membolehkan pertukaran maklumat yang pantas dan efisien di dalam Universiti atau dengan pihak yang berkepentingan.

(3) Penyediaan akses kepada teknologi dan perkhidmatan bagi membantu dalam pencapaian misi dan visi Universiti.

(4) Penyelenggaraan sistem dan rangkaian bagi memastikan keselamatan, kebolehpercayaan dan kelancaran operasi ICT Universiti terjamin.

(5) Menyokong inovasi dan pembangunan teknologi baharu, penyelidikan, dan penggunaan teknologi terkini untuk memperkukuhkan daya saing.

(6) Menyediakan kepelbagaian perkhidmatan termasuk sokongan teknikal, analisis data dan pembangunan aplikasi bagi memenuhi keperluan yang berbeza.

(7) Melindungi maklumat daripada ancaman seperti penggodaman dan serangan siber.

(8) Meningkatkan komunikasi dalam dan luar Universiti menerusi penyediaan pelbagai platform komunikasi.

6.3 PENGURUSAN PERKHIDMATAN ICT

6.3.1 Keselamatan Siber

Perkhidmatan keselamatan siber disediakan bagi membantu PTj dan pengguna dalam melindungi aset ICT daripada sebarang ancaman yang boleh menjejaskan kerahsiaan, integriti, dan ketersediaan sistem serta data. Melalui penyediaan kawalan teknikal, dasar keselamatan, pemantauan dan pengurusan insiden, ia membantu memastikan operasi

pengajaran, pembelajaran, penyelidikan dan pentadbiran Universiti dapat dilaksanakan secara selamat dan berterusan.

Perkhidmatan yang ditawarkan meliputi perkara berikut:

(1) Program Kesedaran Keselamatan Siber

Pelaksanaan program kesedaran secara berkala bagi meningkatkan tahap pemahaman dan kepekaan pengguna terhadap kepentingan perlindungan maklumat dan aset ICT.

(2) Khidmat Nasihat dan Konsultansi Keselamatan ICT

Penyediaan bantuan kepakaran dalam perancangan dan pelaksanaan kawalan keselamatan ICT, pembangunan sistem serta pematuhan dasar keselamatan Universiti.

(3) Pengurusan Insiden Keselamatan Siber

Sokongan teknikal bagi menangani insiden seperti serangan hasad (*malware*), *phishing,* pencerobohan sistem atau kebocoran data. Tatacara pengurusan insiden keselamatan merujuk kepada arahan kerja yang berkuat kuasa di laman web QMED (https://qmec.um.edu.my).

(4) Pemantauan Sistem Keselamatan ICT

Penyediaan pemantauan keselamatan secara berterusan untuk mengesan aktiviti mencurigakan dan mengambil tindakan awal bagi mencegah insiden keselamatan.

(5) Perlindungan Infrastruktur ICT

Pelaksanaan kawalan keselamatan seperti *firewall,* antivirus, pengurusan tampalan keselamatan (*patching*), dan sistem pengesanan pencerobohan bagi melindungi infrastruktur ICT.

(6) Pelan Pemulihan Bencana

Perkhidmatan penyediaan dan pengujian pelan pemulihan bencana untuk memastikan kesinambungan operasi ICT sekiranya berlaku insiden keselamatan.

Semua kawalan keselamatan yang dilaksanakan adalah selaras dengan keperluan keselamatan ICT Universiti serta mematuhi keperluan piawaian ISMS.

6.3.2 Perolehan ICT

Perkhidmatan perolehan ICT disediakan bagi membantu PTj dalam melaksanakan proses perolehan bekalan, perkhidmatan dan kerja ICT selaras dengan kaedah dan prosedur yang ditetapkan. Melalui perkhidmatan ini, JTM menyediakan khidmat sokongan teknikal dan nasihat bagi memastikan perolehan ICT yang dibuat memenuhi keperluan fungsi, keselamatan dan strategi Universiti.

Perkhidmatan yang ditawarkan meliputi perkara berikut:

(1) Khidmat Nasihat Perolehan ICT

JTM memberikan khidmat nasihat teknikal kepada PTj berkaitan kesesuaian spesifikasi dan keperluan sistem bagi memastikan ia menepati keperluan strategik Universiti dan mematuhi syarat dan kriteria yang ditetapkan.

(2) Penyediaan Spesifikasi Teknikal

JTM akan membantu dalam penyediaan spesifikasi teknikal bagi memastikan peralatan, perisian atau perkhidmatan ICT yang diperoleh menepati keperluan fungsi, keselamatan dan kesesuaian teknologi Universiti.

(3) Permohonan Kelulusan Teknikal

Staf JTM di PTj bersedia membantu dalam mengemukakan permohonan kepada jawatankuasa yang berkaitan sebelum proses perolehan boleh dilaksanakan. Tatacara permohonan adalah

merujuk kepada arahan dan garis panduan yang berkuat kuasa dan boleh diakses melalui pautan ICT Info > Jawatankuasa ICT (JKICT) di Portal Staf (https://portal.um.edu.my).

(4) Pengurusan Pelaksanaan Perolehan

Staf JTM di PTj membantu dalam melaksanakan pengurusan perolehan seperti yang telah ditetapkan dalam Dokumen Induk Pengurusan Kewangan UM.

6.3.3 Pembangunan/Perolehan Sistem Aplikasi

Perkhidmatan pembangunan/perolehan sistem aplikasi disediakan bagi membantu PTj dalam memenuhi keperluan pengajaran, pembelajaran, penyelidikan dan operasi pentadbiran melalui penggunaan sistem aplikasi yang bersesuaian. Setiap pembangunan atau perolehan sistem aplikasi yang akan digunakan perlu mematuhi keperluan teknikal, keselamatan, tadbir urus dan dasar yang ditetapkan oleh Universiti.

Perkara-perkara berikut perlu diambil perhatian:

(1) Kelulusan Pembangunan Sistem Aplikasi

Setiap cadangan pembangunan, penaiktarafan atau perolehan sistem aplikasi perlu melalui proses penilaian bagi menilai keperluan integrasi antara platform, infrastruktur, perkakasan serta kos pembangunan dari aspek masa, sumber manusia dan kewangan. Penilaian ini penting bagi mengelakkan duplikasi, memastikan keselarasan dengan pelan strategik Universiti, serta pematuhan kepada peraturan yang berkuat kuasa.

Tatacara permohonan merujuk kepada garis panduan dan arahan kerja yang berkuat kuasa yang boleh diakses melalui Portal Staf: ICT Info > Jawatankuasa Penilaian Sistem Aplikasi (JPSA) (https://portal.um.edu.my).

(2) Pentadbiran Profil Keselamatan Pengguna

Setiap sistem aplikasi perlu ditadbir dengan pengurusan profil keselamatan pengguna yang menetapkan ciri-ciri kawalan akses, kebenaran capaian, dan keistimewaan berdasarkan peranan serta keperluan pengguna.

Pengurusan profil keselamatan pengguna perlu dilaksanakan mengikut tatacara yang berkuat kuasa di laman web QMED (https://qmec.um.edu.my).

(3) Penyerahan Sistem kepada JTM daripada Pihak Ketiga

Bagi pembangunan sistem aplikasi melalui penyumberan luar (*outsourcing*), proses pemantauan dan penilaian sistematik dilaksanakan bagi memastikan keperluan keselamatan maklumat serta syarat Universiti dipatuhi sepenuhnya. Semua komunikasi dan persetujuan berkaitan keperluan serta jangkaan projek perlu dimuktamadkan antara pihak Universiti dan pembekal sebelum dan sepanjang tempoh pelaksanaan projek.

Setiap penyerahan sistem kepada JTM hendaklah mematuhi tatacara penyerahan sistem aplikasi yang ditetapkan dalam arahan kerja berkuat kuasa di laman web QMED (https://qmec.um.edu.my).

6.3.4 Perkhidmatan Rangkaian

Perkhidmatan rangkaian disediakan oleh JTM di kampus utama dan kampus cawangan UM, merangkumi rangkaian berwayar dan tanpa wayar, bagi menyokong kelancaran aktiviti pengajaran, pembelajaran, penyelidikan dan pentadbiran Universiti. Perkhidmatan ini bertujuan memastikan infrastruktur rangkaian Universiti beroperasi secara cekap, stabil dan selamat.

Perkhidmatan yang disediakan meliputi perkara berikut:

(1) Pengurusan *Virtual Private Network* (VPN)

Perkhidmatan *Virtual Private Network* (VPN) membolehkan sambungan rangkaian persendirian secara selamat dari luar kampus ke rangkaian dalaman Universiti melalui rangkaian awam. Perkhidmatan ini disediakan kepada staf UM yang memerlukan akses bagi tujuan tugasan rasmi seperti pentadbiran, penyelidikan atau tugasan jarak jauh. Permohonan perkhidmatan VPN perlu dikemukakan mengikut tatacara yang ditetapkan dalam arahan kerja yang berkuat kuasa di laman web QMED (https://qmec.um.edu.my).

(2) Pengurusan Capaian Port Rangkaian

Capaian port rangkaian merujuk kepada pembukaan atau penyekatan port komunikasi dalam protokol rangkaian bagi membolehkan sistem, aplikasi atau peranti berkomunikasi melalui rangkaian tempatan (LAN) atau Internet. Permohonan capaian port perlu dikemukakan mengikut tatacara yang ditetapkan dalam arahan kerja yang berkuat kuasa di laman web QMED (https://qmec.um.edu.my).

(3) Pengurusan Rangkaian Tanpa Wayar (WiFi)

JTM menyediakan kemudahan rangkaian tanpa wayar (WiFi) di kampus utama dan cawangan UM bagi kegunaan staf, pelajar dan tetamu Universiti. Permohonan capaian tambahan atau sokongan teknikal berkaitan WiFi perlu dikemukakan mengikut tatacara yang berkuat kuasa di laman web QMED (https://qmec.um.edu.my).

(4) Pemantauan dan Penyelenggaraan Infrastruktur Rangkaian

JTM melaksanakan pemantauan prestasi rangkaian secara berterusan serta aktiviti penyelenggaraan infrastruktur rangkaian bagi memastikan kelancaran operasi serta kestabilan sistem rangkaian Universiti.

6.3.5 Perkhidmatan Pelayan

Perkhidmatan pelayan (*server*) disediakan bagi menyokong operasi pengajaran, pembelajaran, penyelidikan, pentadbiran, dan keselamatan maklumat Universiti. Pelayan berfungsi sebagai pusat penyimpanan, pemprosesan, dan pengurusan data serta aplikasi yang digunakan oleh warga UM.

Perkhidmatan pelayan yang ditawarkan meliputi perkara berikut:

(1) Penempatan Laman Web

Dua (2) kaedah utama disediakan untuk penempatan laman web PTj, iaitu:

(a) **Platform bersepadu/berpusat:** Kemudahan bagi PTj mengurus dan mengemas kini kandungan laman web (statik atau dinamik), manakala penyelenggaraan teknikal dikendalikan oleh JTM.

(b) **Perkhidmatan *webhosting*:** Penyediaan ruang *hosting* bagi laman web yang memerlukan ciri tambahan mengikut keperluan teknikal yang ditetapkan. Penempatan ini tertakluk kepada spesifikasi dan keperluan yang diluluskan. Tatacara permohonan boleh dirujuk di laman web QMED (https://qmec.um.edu.my).

(2) Penempatan Pelayan di Pusat Data UM

PTj ditawarkan kemudahan untuk menempatkan pelayan masing-masing di Pusat Data UM bagi membolehkan pengurusan, pemantauan dan penyelenggaraan infrastruktur dilaksanakan secara berpusat, teratur dan selamat. Tatacara pengurusan penempatan pelayan boleh dirujuk di laman web QMED (https://qmec.um.edu.my).

(3) Pendaftaran Nama Domain

Nama domain ialah alamat unik yang digunakan bagi mengenal pasti laman web dan perkhidmatan di dalam rangkaian internet, yang berfungsi sebagai pengganti kepada alamat IP. JTM menyediakan perkhidmatan pendaftaran nama domain menggunakan domain rasmi *.um.edu.my sebagai identiti rasmi Universiti. Tatacara pengurusan pendaftaran dan pengemaskinian nama domain di Sistem Nama Domain (DNS) Universiti boleh dirujuk di laman web QMED (https://qmec.um.edu.my).

6.3.6 Perkhidmatan Pengurusan Perkakasan dan Perisian ICT

Bagi memenuhi keperluan persekitaran dan kaedah kerja moden dan dinamik, UM melaksanakan kaedah BYOD dan guna sama komputer untuk meningkatkan kecekapan dan fleksibiliti operasi. Selain itu, perolehan perisian turut dikawal selia bagi memastikan keseragaman penggunaan dan pematuhan kepada keperluan keselamatan ICT Universiti.

(1) *Buy Your Own Device* (BYOD)

Kaedah BYOD membolehkan staf membeli peranti atau peralatan teknologi sendiri bagi melaksanakan tugasan rasmi dengan lebih fleksibel dan sesuai mengikut keperluan masing-masing. Universiti menyediakan kemudahan peruntukan pembelian yang tertakluk kepada garis panduan dan kelulusan yang berkuat kuasa. Tatacara permohonan boleh dirujuk melalui pautan: ICT Info > Polisi dan Prosedur di Portal Staf (https://portal.um.edu.my).

(2) Guna Sama Desktop/Komputer Riba

Kemudahan guna sama peranti disediakan bagi membolehkan PTj menggunakan komputer desktop atau komputer riba untuk tujuan pengajaran, pembelajaran, penyelidikan dan pentadbiran. Pembelian dan pengurusan peranti ini dikendalikan secara berpusat oleh JTM mengikut spesifikasi yang ditetapkan.

(3) Perolehan Perisian (*Off-the-Shelf*)

Perisian *off-the-shelf* merujuk kepada perisian sedia ada yang boleh digunakan tanpa pengubahsuaian atau pembangunan khas. Setiap perolehan baharu perisian perlu melalui proses permohonan dan penilaian oleh jawatankuasa yang dilantik sebelum diuruskan oleh JTM. Tatacara pengurusan perolehan perisian *off-the-shelf* boleh dirujuk di laman web QMED (https://qmec.um.edu.my).

6.3.7 Perkhidmatan Sokongan ICT

Bagi memastikan kelancaran operasi pengajaran, pembelajaran, penyelidikan dan pentadbiran di seluruh kampus, JTM menyediakan perkhidmatan sokongan ICT peringkat pertama yang meliputi bantuan teknikal harian, penyelenggaraan peralatan ICT serta penyelarasan keperluan ICT di peringkat PTj. Bagi memperkukuhkan keupayaan penyampaian perkhidmatan ICT di PTj, staf JTM daripada Skim F telah ditempatkan di PTj melalui inisiatif pemusatan. Maklumat berkaitan penempatan staf serta zon bertugas boleh dirujuk melalui pautan pantas *Centralization of Scheme F* di laman web JTM (https://it.um.edu.my).

Perkhidmatan sokongan ICT yang disediakan merangkumi perkara berikut:

(1) Pengurusan Aduan dan Bantuan ICT

Bantuan teknikal asas ditawarkan bagi menyokong operasi harian di PTj meliputi sistem aplikasi, capaian rangkaian, keselamatan ICT, penyelenggaraan perkakasan dan perisian, serta kemudahan makmal komputer. Semua aduan atau pertanyaan berkaitan ICT boleh dikemukakan melalui Sistem Helpdesk (https://helpdesk.um.edu.my).

(2) Penyelenggaraan dan Pemantauan Infrastruktur ICT

Penyelenggaraan berkala dilaksanakan terhadap peralatan ICT termasuk komputer desktop, komputer riba, pencetak, peralatan rangkaian, peralatan multimedia serta kemudahan bilik kuliah bagi

memastikan peralatan sentiasa berada dalam keadaan baik dan menyokong kelancaran aktiviti pengajaran, pembelajaran dan penyelidikan di PTj. Di samping itu, pemantauan juga dibuat ke atas peralatan ICT yang diperoleh secara berpusat melalui kontrak penyelenggaraan sedia ada.

(3) Pengurusan Perisian dan Lesen ICT

JTM memastikan pemasangan, konfigurasi, pengemaskinian, pengurusan lesen dan latihan penggunaan perisian dilaksanakan mengikut dasar dan keperluan Universiti.

(4) Penyelarasan Keperluan ICT PTj

JTM membantu merancang dan menyelaras keperluan perkakasan, perisian, perkhidmatan ICT dan kepakaran sumber manusia di PTj agar selaras dengan dasar, spesifikasi dan perancangan strategik ICT Universiti.

SENARAI INDUK DOKUMEN ICT UM

LAMPIRAN A

Status Dokumen : A(Aktif), T(Tidak Aktif)

No	Ser#	Standard/ Annex		No. DIPICT	Dokumen							Borang							Catatan
					Nama Dokumen	No.Dokumen	No. Semakan	Tarikh Kuatkuasa	Status	Klasifikasi	Pemilik	Nama Borang	No. Borang	No. Semakan	Tarikh Kuatkuasa	Status	Pemilik	Pengguna	
1	1	Tidak Berkenaan		4.3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
2	2	Keperluan Piawaian		5.4	Manual Sistem Pengurusan Keselamatan Maklumat (ISMS)	UM02-PT04-PK04-5.4 MI001	5.0	19.8.2025	A	Terhad	Jawatankuasa Kerja ISMS	Borang Pemantauan dan Pengukuran Objektif Keselamatan ISMS	UM02-PT04-PK04-5.4 BR001	3.0	20.6.2025	A	Jawatankuasa Kerja ISMS	Semua Pusat	-
												Borang Komunikasi Dalaman dan Luaran ISMS	UM02-PT04-PK04-5.4 BR002	3.0	20.6.2025	A	Jawatankuasa Kerja ISMS	Semua Pusat	-
												Borang Pemantauan dan Pengukuran Kawalan ISMS	UM02-PT04-PK04-5.4 BR003	3.0	20.6.2025	A	Jawatankuasa Kerja ISMS	Semua Pusat	-
												Borang Mesyuarat Kajian Semula Pengurusan ISMS	UM02-PT04-PK04-5.4 BR004	3.0	20.6.2025	A	Jawatankuasa Kerja ISMS	Urusetia ISMS	-
	2A	Keperluan Piawaian		5.4	Lampiran Manual Sistem Pengurusan Keselamatan Maklumat (ISMS)	UM02-PT04-PK04-5.4 MI001A	5.0	19.8.2025	A	Terhad	Jawatankuasa Kerja ISMS	Borang Antara Muka & Kebergantungan Antara Aktiviti yang Dilaksanakan oleh UM dan Organisasi Lain	UM02-PT04-PK04-5.4 BR005	3.0	20.6.2025	A	Jawatankuasa Kerja ISMS	Semua Pusat	-
3	3	Keperluan Piawaian		5.4	Prosedur Pengurusan Risiko	UM02-PT04-PK04-5.4 MI002	3.0	20.6.2025	A	Terhad	Jawatankuasa Kerja ISMS	Borang Laporan Penilaian dan Pelan Rawatan Risiko (RA/RTP)	UM02-PT04-PK04-5.4 BR006	2.0	24.6.2025	A	Jawatankuasa Kerja ISMS	Semua Pusat	-
4	4	Keperluan Piawaian		5.4	Pernyataan Kebolehgunaan (Statement of Applicability), SOA	UM02-PT04-PK04-5.4 MI003	4.0	19.9.2025	A	Sulit	Jawatankuasa Kerja ISMS	Senarai Induk Dokumen ICT	UM02-PT04-PK04-5.4 BR007	3.0	24.6.2025	A	Jawatankuasa Kerja ISMS	Urusetia ISMS	-
5	5	Keperluan Piawaian		5.4	Prosedur Tindakan Pembetulan dan Pencegahan	UM02-PT04-PK04-5.4 MI004	3.0	20.6.2025	A	Terhad	Jawatankuasa Kerja ISMS	Borang Permintaan Tindakan Pembetulan/Pencegahan (CAR/PAR)	UM02-PT04-PK04-5.4 BR008	3.0	20.6.2025	A	Jawatankuasa Kerja ISMS	Semua Pusat	-
6	6	5.01	Polisi keselamatan maklumat	5.7.1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
7	7	5.02	Peranan dan tanggungjawab keselamatan maklumat.	5.7.2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
8	8	5.03	Pengasingan Tugas	5.7.2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
9	9	5.04	Tanggungjawab Pengurusan	5.7.4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
10	10	5.05	Hubungan Dengan Pihak Berkuasa	5.7.5	-	-	-	-	-	-	-	Borang Senarai Nombor Hubungan Penting (Dalaman Dan Luaran)	UM02-PT04-PK04-5.7.5 BR001	2.0	24.6.2025	A	Jawatankuasa Kerja ISMS	Semua Pusat	-
11	11	5.06	Hubungan Dengan Kumpulan Berkepentingan Khas	5.7.6	-	-	-	-	-	-	-	Borang Senarai Hubungan Dengan Kumpulan Kepentingan Khas	UM02-PT04-PK04-5.7.6 BR001	2.0	24.6.2025	A	Jawatankuasa Kerja ISMS	Semua Pusat	-
12	12	5.07	Risikan Ancaman	5.7.7	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
13	13	5.08	Keselamatan Maklumat Dalam Pengurusan Projek	5.7.8	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
14	14	5.09	Inventori Maklumat Dan Aset Lain Yang Berkaitan	5.7.9	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
15	15	5.10	Penggunaan Maklumat Yang Boleh Diterima Dan Aset Yang Berkaitan	5.10	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
16	16	5.11	Pemulangan Aset	5.7.11	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
17	17	5.12	Klasifikasi Maklumat	5.7.12	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
18	18	5.13	Pelabelan Maklumat	5.7.13	Prosedur Pengendalian Aset Maklumat	UM02-PT04-PK04-5.7.13 PR001	2.0	7.6.2025	A	Terhad	Jawatankuasa Kerja ISMS	Borang Akuan Pengambilan/Penerimaan Komputer	UM02-PT04-PK04-5.7.13 BR001	2.1	30.12.2025	A	PID-SPPB-UPK	PID-SPPB-UPK	-
												Borang Bawa Peralatan Keluar	UM02-PT04-PK04-5.7.13 BR002	3.0	12.8.2025	A	Jawatankuasa Kerja ISMS	Semua Pusat	-
19	19	5.14	Pemindahan Maklumat	5.7.14	Garis Panduan Penggunaan Emel dan Storan	UM02-PT04-PK04-5.7.14 GP001	2.0	30.4.2025	A	Terhad	PID	-	-	-	-	-	-	-	-
					Garis Panduan Penggunaan Mesin Fotokopi/ Pencetak Pelbagai Fungsi (MFP)	UM02-PT04-PK04-5.7.14 GP002	2.0	3.2.2024	A	Terhad	PID	-	-	-	-	-	-	-	-
20	20	5.15	Kawalan Capaian	5.7.15								Borang Semakan Hak Akses	UM02-PT04-PK04-5.7.15 BR001	2.0	24.6.2025	A	Jawatankuasa Kerja ISMS	Semua Pusat	-
												Borang Capaian Pintu JTM	UM02-PT04-PK04-5.7.15 BR002	2.0	24.6.2025	A	UnIt Pentadbiran	Semua Pusat	-
21	21	5.16	Pengurusan Identiti	5.7.16	Prosedur Pentadbiran Profil Keselamatan Pengguna Sistem	UM02-PT04-PK04-5.7.16 PR001	2.0	9.6.2025	A	Terhad	PPPD-SDTP & SDKP PIDi-UTB & UPKt	Borang Permohonan Profil Pengguna dan Pentadbir Sistem	UM02-PT04-PK04-5.7.16 BR001	2.0	24.6.2025	A	PPPD-SDKP/SDTP & PIDi-STB	PTj	-
												Borang Permohonan Profil Pentadbir Sistem Teknikal (JTM)	UM02-PT04-PK04-5.7.16 BR002	2.0	24.6.2025	A	PPPD-SDKP/SDTP & PIDi-STB	JTM	-
22	22	5.17	Maklumat Pengesahan	5.7.17	-	-	-	-	-	-	-								-

No	Ser#	Standard/ Annex		No. DIPICT	Dokumen						Borang							Catatan
					Nama Dokumen	No.Dokumen	No. Semakan	Tarikh Kuatkuasa	Status	Klasifikasi	Pemilik	Nama Borang	No. Borang	No. Semakan	Tarikh Kuatkuasa	Status	Pemilik	Pengguna	
23	23	5.18	Hak Akses	5.7.18	-	-	-	-	-	-	-	Borang Permohonan Capaian SharePoint	UM02-PT04-PK04-5.7.18 BR001	2.0	24.6.2025	A	PID-SPPB-UPK	LPU & Semua Pusat	-
24	24	5.19	Keselamatan Maklumat Dalam Hubungan Dengan Pembekal	5.7.19	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
25	25	5.20	Menangani Keselamatan Maklumat Dalam Hubungan Dengan Pembekal	5.7.20	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
26	26	5.21	Mengurus Keselamatan Maklumat Dalam Rantaian Bekalan ICT	5.7.21	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
27	27	5.22	Memantau, Menyemak Dan Mengubah Pengurusan Perkhidmatan Pembekal	5.7.22	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
28	28	5.23	Keselamatan Maklumat Untuk Pengunaan Perkhidmatan Awan	5.7.23	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
29	29	5.24	Perancangan Dan Penyediaan Pengurusan Insiden Keselamatan Maklumat	5.7.24	Prosedur Pengurusan Insiden Keselamatan Siber	UM02-PT04-PK04-5.7.24 MI001	2.0	19.6.2025	A	Terhad	PIDi-SKS	Borang Laporan Insiden Keselamatan Siber	UM02-PT04-PK04-5.7.4 BR001	2.0	24.6.2025	A	PIDi-SKS	Semua Pusat	-
30	30	5.25	Penilaian dan Tindakan Insiden Keselamatan Maklumat	5.7.25	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
31	31	5.26	Tindakbalas Terhadap Insiden Keselamatan Maklumat	5.7.26	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
32	32	5.27	Pengajaran daripada Insiden Keselamatan Maklumat	5.7.27	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
33	33	5.28	Pengumpulan Bukti	5.7.28	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
33	33	5.29	Keselamatan Maklumat semasa Gangguan	5.7.29	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
34	34	5.30	Ketersediaan ICT bagi Kesinambungan Perkhidmatan	5.7.30	Manual Pengurusan Kesinambungan Perkhidmatan (PKP)	UM02-PT04-PK04-5.7.30 MI001	4.0	19.6.2025	A	Terhad	Jawatankuasa Kerja ISMS	Borang Laporan Insiden Pelan Kesinambungan Perkhidmatan	UM02-PT04-PK04-5.7.30 BR001	2.0	24.6.2025	A	Jawatankuasa Kerja ISMS	Semua Pusat	-
												Borang Kehadiran Mesyuarat Pelan Kesinambungan Perkhidmatan	UM02-PT04-PK04-5.7.30 BR002	2.0	24.6.2025	A	Jawatankuasa Kerja ISMS	Semua Pusat	-
	34A				Pelan Pemulihan Bencana Perkhidmatan ICT (PPB)	UM02-PT04-PK04-5.7.30 MI001A	2.0	19.6.2025	A			Borang Penilaian dan Pengisytiharan Penamatan Situasi Bencana ICT	UM02-PT04-PK04-5.7.30 BR003	2.0	24.6.2025	A	Jawatankuasa Kerja ISMS	Semua Pusat	-
												Borang Pentaksiran Bencana ICT	UM02-PT04-PK04-5.7.30 BR004	2.0	24.6.2025	A	Jawatankuasa Kerja ISMS	Semua Pusat	-
												Laporan Penilaian Semula Bencana Perkhidmatan ICT	UM02-PT04-PK04-5.7.30 BR005	2.0	24.6.2025	A	Jawatankuasa Kerja ISMS	Semua Pusat	-
												Laporan Simulasi Pemulihan Bencana	UM02-PT04-PK04-5.7.30 BR006	2.0	24.6.2025	A	Jawatankuasa Kerja ISMS	Semua Pusat	-
	34B				Prosedur Penentuan Keutamaan Pemulihan Perkhidmatan ICT (PPKP)	UM02-PT04-PK04-5.7.30 MI001B	2.0	19.6.2025	A	Terhad	Jawatankuasa Kerja ISMS	Borang Analisis Impak Perniagaan (BIA)	UM02-PT04-PK04-5.7.30 BR007	3.0	24.6.2025	A	Jawatankuasa Kerja ISMS	Semua Pusat	-
35	35	5.31	Keperluan Perundangan dan Kontrak	5.7.31	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
36	36	5.32	Hak Harta Intelek	5.7.32	Prosedur Pengurusan Hak Harta Intelek	UM02-PT04-PK04-5.7.32 PR001	1.0	19.6.2025	A	Terhad	PPPD & PIDi	-	-	-	-	-	-	-	-
37	37	5.33	Perlindungan Rekod	5.7.33	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
38	38	5.34	Privasi dan Perlindungan Maklumat Peribadi	5.7.34	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
39	39	5.35	Semakan Bebas Keselamatan Maklumat	5.7.35	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
40	40	5.36	Piawaian untuk Keselamatan Maklumat	5.7.36	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
41	41	5.37	Prosedur Operasi Yang Di Dokumenkan	5.7.37	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
42	42	6.01	Tapisan Keselamatan	5.8.1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
43	43	6.02	Terma dan Syarat Pelantikan	5.8.2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
44	44	6.03	Program Kesedaran, Pendidikan dan Latihan Keselamatan Maklumat	5.8.3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

No	Ser#	Standard/ Annex		No. DIPICT	Dokumen						Borang							Catatan
					Nama Dokumen	No.Dokumen	No. Semakan	Tarikh Kuatkuasa	Status	Klasifikasi	Pemilik	Nama Borang	No. Borang	No. Semakan	Tarikh Kuatkuasa	Status	Pemilik	Pengguna	
45	45	6.04	Tindakan Disiplin	5.8.4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
46	46	6.05	Tanggungjawab selepas Pertukaran atau Penamatan Perkhidmatan	5.8.5	Prosedur Pertukaran Dan Penamatan Perkhidmatan	UM02-PT04-PK04-5.8.5 PR001	2.0	19.6.2025	A	Terhad	Unit Pentadbiran	Senarai Semak Pertukaran/Cuti Panjang/Tamat Perkhidmatan	UM02-PT04-PK04-5.8.5 BR001	2.0	24.6.2025	A	Unit Pentadbiran	Semua Pusat	-
47	47	6.06	Perjanjian Kerahsiaan atau Tanpa Mendedahkan	5.8.6	-	-	-	-	-	-	-	Surat Akujanji Kerahsiaan JTM	UM02-PT04-PK04-5.8.6 BR001	2.0	24.6.2025	A	Unit Pentadbiran	Semua Staf & Pelajar Latihan	-
					-	-	-	-	-	-	-	Borang Perjanjian Tanpa Pendedahan (NDA)	UM02-PT04-PK04-5.8.6 BR002	2.0	24.6.2025	A	Jawatankuasa Kerja ISMS	Semua Pusat	-
48	48	6.07	Bekerja Jarak Jauh	5.8.7	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
49	49	6.08	Pelaporan Insiden Keselamatan Maklumat	5.8.8	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
50	50	7.01	Perimeter Keselamatan Fizikal	5.9.1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
51	51	7.02	Kemasukan Fizikal	5.9.2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
52	52	7.03	Keselamatan Pejabat, Bilik dan Kemudahan ICT	5.9.3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
53	53	7.04	Pemantauan Keselamatan Fizikal	5.9.4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
54	54	7.05	Perlindungan daripada Ancaman Fizikal dan Persekitaran	5.9.5	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
55	55	7.06	Bekerja di Kawasan Selamat	5.9.6	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
56	56	7.07	Polisi Meja Bersih dan Skrin Bersih	5.9.7	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
57	57	7.08	Penempatan dan Perlindungan Aset ICT	5.9.8	Prosedur Pengurusan Perkhidmatan Pelayan	UM02-PT04-PK04-5.9.8 PR001	1.0	19.6.2025	A	Terhad	PID-SPPB-UPDPA	Borang Pendaftaran Pelayan	UM02-PT04-PK04-5.9.8 BR001	2.0	24.6.2025	A	PID-SPPB-UPDPA	PID-SPPB-UPDPA	-
												Borang Permohonan/ Penamatan Akaun Pengguna	UM02-PT04-PK04-5.9.8 BR002	2.0	24.6.2025	A	PID-SPPB-UPDPA	PID-SPPB-UPDPA	-
												Borang Ketersediaan Pelayan	UM02-PT04-PK04-5.9.8 BR003	2.0	24.6.2025	A	PID-SPPB-UPDPA	PID-SPPB-UPDPA	-
												Borang Senarai Semak Keselamatan Pelayan	UM02-PT04-PK04-5.9.8 BR004	2.0	24.6.2025	A	PID-SPPB-UPDPA	PID-SPPB-UPDPA	-
												Borang Tampalan Pelayan	UM02-PT04-PK04-5.9.8 BR005	2.0	24.6.2025	A	PID-SPPB-UPDPA	PID-SPPB-UPDPA	-
												Borang Permohonan Perkhidmatan Pengehosan Web	UM02-PT04-PK04-5.9.8 BR006	2.0	24.6.2025	A	PID-SPPB-UPDPA	PID-SPPB-UPDPA	-
												Buku Log Pita LTO	UM02-PT04-PK04-5.9.8 BR007	2.0	24.6.2025	A	PID-SPPB-UPDPA	PID-SPPB-UPDPA	-
												Borang Pengeluaran Pita Perpustakaan Media	UM02-PT04-PK04-5.9.8 BR008	2.0	24.6.2025	A	PID-SPPB-UPDPA	PID-SPPB-UPDPA	-
												Borang Permohonan Sandaran/ Pemulihan	UM02-PT04-PK04-5.9.8 BR009	2.0	24.6.2025	A	PID-SPPB-UPDPA	PID-SPPB-UPDPA	-
												Borang Pendaftaran Kemaskini Nama Domain di DNS	UM02-PT04-PK04-5.9.8 BR010	2.0	24.6.2025	A	PID-SPPB-UPDPA	PID-SPPB-UPDPA	-
58	58	7.09	Keselamatan Aset di Luar Premis	5.9.9	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
59	59	7.10	Media Storan	5.9.10	Prosedur Sanitasi Data	UM02-PT04-PK04-5.9.10 PR001	1.0	19.6.2025	A	Terhad	PID	Borang Permohonan Sanitasi Data	UM02-PT04-PK04-5.9.10 BR001	1.0	24.6.2025	A	Jawatankuasa Kerja ISMS	Semua Pusat	-
60	60	7.11	Utiliti Sokongan	5.9.11	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
61	61	7.12	Keselamatan Pengkabelan	5.9.12	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
62	62	7.13	Penyelenggaraan Peralatan	5.9.13	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
63	63	7.14	Pelupusan atau Penggunaan Semula Peralatan	5.9.14	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
64	64	8.01	Keselamatan Peranti Pengguna	5.10.1	Garis Panduan Penggunaan Peranti Mudah Alih Persendirian	UM02-PT04-PK04-5.10.1 GP001	2.0	3.2.2023	A	Terhad	PID	-	-	-	-	-	-	-	-
65	65	8.02	Hak Capaian Istimewa	5.10.2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
66	66	8.03	Sekatan Capaian Maklumat	5.10.3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
67	67	8.04	Capaian kepada Kod Sumber	5.10.4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

No	Ser#	Standard/ Annex		No. DIPICT	Dokumen						Borang							Catatan
					Nama Dokumen	No.Dokumen	No. Semakan	Tarikh Kuatkuasa	Status	Klasifikasi	Pemilik	Nama Borang	No. Borang	No. Semakan	Tarikh Kuatkuasa	Status	Pemilik	Pengguna	
68	68	8.05	Pengesahan Selamat (Secure Authentication)	5.10.5	Prosedur Kawalan Keselamatan Akaun dan Log-On	UM02-PT04-PK04-5.10.5 PR001	2.0	19.6.2025	A	Terhad	PIDi-SKS	-	-	-	-	-	-	-	-
69	69	8.06	Pengurusan Kapasiti (Capacity Management)	5.10.6	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
70	70	8.07	Perlindungan Terhadap Perisian Hasad (Malware)	5.10.7	Prosedur Instalasi dan Konfigurasi Komputer	UM02-PT04-PK04-5.10.7 PR001	2.0	19.6.2025	A	Terhad	PID-UPK	Senarai Semak Intalasi dan Pengukuhan Keselamatan Komputer	UM02-PT04-PK04-5.10.7 BR001	2.0	24.6.2025	A	PID-SPPB-UK	Semua Pusat	-
71	71	8.08	Pengurusan Kerentanan Teknikal	5.10.8	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
72	72	8.09	Pengurusan Konfigurasi	5.10.9	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
73	73	8.10	Penghapusan Maklumat	5.10.10	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
74	74	8.11	Penopengan Data	5.10.11	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
75	75	8.12	Pencegahan Kebocoran Data	5.10.12	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
76	76	8.13	Sandaran Maklumat	5.10.13	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
77	77	8.14	Lewahan Kemudahan Pemprosesan Maklumat	5.10.14	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
78	78	8.15	Penjanaan Log	5.10.15	Prosedur Pengurusan Log	UM02-PT04-PK04-5.10.15 PR001	1.0	19.6.2025	A	Terhad	PIDi-SKS	-	-	-	-	-	-	-	-
79	79	8.16	Aktiviti Pemantauan	5.10.16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
80	80	8.17	Penyeragaman Jam	5.10.17	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
81	81	8.18	Penggunaan Program Utiliti yang Mempunyai Hak Istimewa	5.10.18	-	-	-	-	-	-	-	Borang Senarai Akses Program Utiliti dan Alat/Perisian Percuma/Sumber Terbuka	UM02-PT04-PK04-5.10.18 BR001	2.0	24.6.2025	A	Jawatankuasa Kerja ISMS	Semua Pusat	-
82	82	8.19	Pemasangan Perisian pada Operasi	5.10.19	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
83	83	8.20	Keselamatan Rangkaian	5.10.20	Prosedur Pengurusan Perkhidmatan Rangkaian	UM02-PT04-PK04-5.10.20 PR001	1.0	19.6.2025	A	Terhad	PID-SRDP-UR	Borang Permohonan Capaian Port	UM02-PT04-PK04-5.10.20 BR001	2.0	24.6.2025	A	PID-SRPD-UR	Semua Pusat	-
												Borang Permohonan Perkhidmatan UM-VPN	UM02-PT04-PK04-5.10.20 BR002	2.0	24.6.2025	A	PID-SRPD-UR	Semua Pusat	-
												Senarai Semak Pengukuhan Wireless Controller	UM02-PT04-PK04-5.10.20 BR003	2.0	24.6.2025	A	PID-SRPD-UR	Semua Pusat	-
												Senarai Semak Pengukuhan Firewall	UM02-PT04-PK04-5.10.20 BR004	2.0	24.6.2025	A	PID-SRPD-UR	Semua Pusat	-
												Senarai Semak Pengukuhan Switch	UM02-PT04-PK04-5.10.20 BR005	2.1	24.11.2025	A	PID-SRPD-UR	Semua Pusat	-
84	84	8.21	Keselamatan Perkhidmatan Rangkaian	5.10.21	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
85	85	8.22	Pengasingan Rangkaian	5.10.22	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
86	86	8.23	Penapisan Web	5.10.23	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
87	87	8.24	Penggunaan Kriptografi	5.10.24	-	-	-	-	-	-	-	Borang Senarai Aplikasi Yang Menggunakan Kawalan Kriptografi	UM02-PT04-PK04-5.10.24 BR001	2.0	24.6.2025	A	Jawatankuasa Kerja ISMS	Semua Pusat	-
88	88	8.25	Kitaran Hayat Pembangunan Selamat	5.10.25	Prosedur Pembangunan dan Penyelenggaraan Sistem Aplikasi	UM02-PT04-PK04-5.10.25 PR001	2.0	10.10.2025	A	Terhad	PPPD-SDKP, PPPD-SDTP, PIDi-STB	Borang Matriks Kawalan Capaian	UM02-PT04-PK04-5.10.25 BR001	2.0	24.6.2025	A	PPPD-SDKP, PPPD-SDTP, PIDi-STB	PPPD-SDKP, PPPD-	-
												Senarai Semak Jaminan Kualiti Sistem	UM02-PT04-PK04-5.10.25 BR002	2.1	10.10.2025	A	PPPD-SDKP, PPPD-SDTP, PIDi-STB	PPPD-SDKP, PPPD-	-
												Borang Pengujian Unit Sistem Aplikasi	UM02-PT04-PK04-5.10.25 BR003	2.0	24.6.2025	A	PPPD-SDKP, PPPD-SDTP, PIDi-STB	PPPD-SDKP, PPPD-	-
89	89	8.26	Keperluan Keselamatan Aplikasi	5.10.26	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
90	90	8.27	Prinsip Reka Bentuk dan Kejuruteraan Sistem yang Selamat	5.10.27	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
91	91	8.28	Pengekodan Selamat	5.10.28	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
92	92	8.29	Pengujian Keselamatan Semasa Pembangunan dan Penerimaan	5.10.29	Prosedur Pengujian Sistem Aplikasi	UM02-PT04-PK04-5.10.29 PR001	2.0	1.6.2025	A	Terhad	PPPD-UPS	Borang Penerimaan Pengujian Pengguna (UAT)	UM02-PT04-PK04-5.10.29 BR001	2.0	24.6.2025	A	PPPD-UPS	PPPD-SDKP, PPPD-	-

No	Ser#	Standard/ Annex		No. DIPICT	Dokumen						Borang							Catatan
					Nama Dokumen	No.Dokumen	No. Semakan	Tarikh Kuatkuasa	Status	Klasifikasi	Pemilik	Nama Borang	No. Borang	No. Semakan	Tarikh Kuatkuasa	Status	Pemilik	Pengguna	
												Borang Pengesahan Penerimaan Sistem/Modul	UM02-PT04-PK04-5.10.29 BR002	2.0	24.6.2025	A	PPPD-UPS	PPPD-SDKP, PPPD-	-
												Borang Pengujian Sistem Aplikasi	UM02-PT04-PK04-5.10.29 BR003	2.0	24.6.2025	A	PPPD-UPS	PPPD-SDKP, PPPD-	-
93	93	8.30	Pembangunan Sistem secara Luaran	5.10.30	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
94	94	8.31	Pengasingan Persekitaran Pembangunan, Pengujian	5.10.31	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
95	95	8.32	Pengurusan Perubahan	5.10.32	Prosedur Kawalan Dokumen ICT	UM02-PT04-PK04-5.10.32 PR001	2.0	19.8.2025	A	Terhad	Jawatankuasa Kerja ISMS	Borang Permohonan Pindaan Perkhidmatan/Infrastruktur ICT	UM02-PT04-PK04-5.10.32 BR001	2.0	24.6.2025	A	Jawatankuasa Kerja ISMS	PID dan PPPD	-
												Borang Permohonan Pendaftaran/ Pindaan Dokumen ICT	UM02-PT04-PK04-5.10.32 BR002	2.0	24.6.2025	A	Jawatankuasa Kerja ISMS	Semua Pusat	-
96	96	8.33	Data Pengujian	5.10.33	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
97	97	8.34	Perlindungan Sistem Maklumat Semasa Ujian Audit	5.10.34	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
98	98	Tidak berkenaan		6.3.1	Arahan Kerja Pengurusan Insiden Keselamatan Maklumat	UM02-PT04-PK04-AK001					PIDi	-	-	-	-	-	-	-	Dokumen Kualiti di bawah SPK
99	99			6.3.2	Arahan Kerja Pengurusan Kelulusan Teknikal Projek ICT	UM02-PT04-PK04-AK002					SGD	-	-	-	-	-	-	-	Dokumen Kualiti di bawah SPK
100	100			6.3.3	Arahan Kerja Pengurusan Permohonan Kelulusan Perolehan/ Pembangunan dan Naiktaraf/ Perubahan Sistem Aplikasi	UM02-PT04-PK04-AK003					PPPD	-	-	-	-	-	-	-	Dokumen Kualiti di bawah SPK
101	101				Arahan Kerja Pentadbiran Profil Keselamatan Pengguna Sistem Aplikasi	UM02-PT04-PK04-AK012						-	-	-	-	-	-	-	Dokumen Kualiti di bawah SPK
102	102				Arahan Kerja Penerimaan Sistem dan Penyelenggaraan Sistem yang Dibangunkan oleh Pihak Ketiga	UM02-PT04-PK04-AK013					PPPD	-	-	-	-	-	-	-	Dokumen Kualiti di bawah SPK
103	103			6.3.4	Arahan Kerja Pengurusan Permohonan Perkhidmatan VPN	UM02-PT04-PK04-AK007					PID	-	-	-	-	-	-	-	Dokumen Kualiti di bawah SPK
104	104				Arahan Kerja Pengurusan Permohonan Capaian Port	UM02-PT04-PK04-AK008					PID	-	-	-	-	-	-	-	Dokumen Kualiti di bawah SPK
105	105				Pemasangan & Penyelenggaraan Peralatan Rangkaian Utama, Titik Data & Fiber Optik	UM02-PT04-PK04-AK009					PID	-	-	-	-	-	-	-	Dokumen Kualiti di bawah SPK
106	106			6.3.5	Arahan Kerja Pengurusan Perkhidmatan Webhosting	UM02-PT04-PK04-AK004					PID	-	-	-	-	-	-	-	Dokumen Kualiti di bawah SPK
107	107				Arahan Kerja Penempatan Pelayan di Pusat Data Jabatan Teknologi Maklumat	UM02-PT04-PK04-AK005					PID	-	-	-	-	-	-	-	Dokumen Kualiti di bawah SPK
108	108				Arahan Kerja Pendaftaran Nama Domain di Domain Name System (DNS) Universiti Malaya	UM02-PT04-PK04-AK006					PID	-	-	-	-	-	-	-	Dokumen Kualiti di bawah SPK
109	109			6.3.6	Garis Panduan Pelaksanaan Pemilikan Komputer Melalui Kaedah Buy Your Own Device (BYOD)	UM02-PT04-PK04-6.3.6 GP001	4.1	14.1.2026	A	Terhad	PID	-	-	-	-	-	-	-	-
110	110			6.3.7	Arahan Kerja Pengurusan Perisian (Off-the-Shelf)	UM02-PT04-PK04-AK010					PID	-	-	-	-	-	-	-	Dokumen Kualiti di bawah SPK
111	111			6.3.8	Arahan Kerja Pengurusan Permohonan Perkhidmatan Multimedia	UM02-PT04-PK04-AK011					PIDi	-	-	-	-	-	-	-	Dokumen Kualiti di bawah SPK

LAMPIRAN B: SENARAI JAWATANKUASA ICT UM

Lampiran B1 : Terma Rujukan Jawatankuasa Pengurusan ICT (JKPICT)

Lampiran B2 : Terma Rujukan Jawatankuasa Pengguna ICT (JPICT)

Lampiran B3 : Terma Rujukan Jawatankuasa Teknikal ICT (JTICT)

Lampiran B4 : Terma Rujukan Jawatankuasa Penilaian Sistem Aplikasi (JPSA)

Lampiran B5 : Terma Rujukan Jawatankuasa Pembangunan Projek ICT (JAPPICT)

Lampiran B6 : Terma Rujukan Jawankuasa Kerja Sistem Pengurusan Keselamatan Maklumat (JK ISMS)

LAMPIRAN B1: TERMA RUJUKAN JAWATANKUASA PENGURUSAN ICT (JKPICT)

UNIVERSITI MALAYA

Terma Rujukan Jawatankuasa

Nama Jawatankuasa	:	Jawatankuasa Pengurusan ICT, Universiti Malaya.
Pengenalan	:	Jawatankuasa Pengurusan ICT (JKPICT) adalah salah satu dari tiga buah Jawatankuasa di bawah tadbir urus ICT Universiti Malaya (UM). Ia merupakan jawatankuasa tertinggi yang menentukan hala tuju perkhidmatan ICT di UM untuk menyokong visi dan misi Universiti Malaya. JKPICT menjalankan fungsi yang sama dengan Jawatankuasa Pengurusan Universiti (JKPU) UM dengan fokus membawa agenda ICT.
Punca Kuasa	:	Naib Canselor melantik ahli JKPICT
Keanggotaan	:	Pengerusi: Naib Canselor UM Setiausaha: Pengarah Eksekutif, Jabatan Teknologi Maklumat (JTM) Ahli: 1. Timbalan Naib Canselor (Akademik & Antarabangsa) 2. Timbalan Naib Canselor (Penyelidikan & Inovasi) 3. Timbalan Naib Canselor (Hal Ehwal Pelajar) 4. Timbalan Naib Canselor (Pembangunan) 5. Pendaftar/Wakil Tetap 6. Bendahari/Wakil Tetap 7. Ketua Pegawai Digital (CDO), UM 8. Pengarah Pusat Perubatan Universiti Malaya 9. Pengarah Eksekutif Jabatan Kesarjanaan Digital dan Maklumat Semesta (Perpustakaan) 10. Ketua Bahagian Perundangan 11. Pegawai Keselamatan ICT (ICTSO); dan 12. Dua (2) orang Ketua PTj akademik atau Timbalan, masing-masing mewakili aliran Sains dan Sastera Jemputan: Pegawai Kanan dari Universiti Malaya jika perlu Urusetia: Seksyen Governan Digital, JTM
Tempoh Keanggotaan	:	Tempoh jawatan adalah selama dua (2) tahun atau seperti tempoh pelantikan sebagai Pengurusan Tertinggi Universiti.
Bidang Kuasa Jawatankuasa	:	1. Menetapkan hala tuju dan strategi untuk pembangunan dan pelaksanaan inisiatif ICT UM dengan mengambil kira keperluan dan falsafah ICT Universiti secara

keseluruhannya;

2. Meluluskan Pelan Tindakan ICT UM;
3. Memperaku dokumen polisi yang berkaitan ICT untuk kelulusan Lembaga Pengarah Universiti (LPU);
4. Memutuskan perkara-perkara dasar yang berkaitan ICT di UM;
5. Melapor penetapan dan pelaksanaan dasar ICT serta status pembangunan ICT di kampus kepada Jawatankuasa Pengurusan dari masa ke semasa.

Mesyuarat : Jawatankuasa hendaklah bermesyuarat sekurang-kurangnya dua (2) kali setahun.

Notis Mesyuarat :

1. Notis bagi sesuatu mesyuarat hendaklah disampaikan secara bertulis atau secara elektronik oleh Setiausaha kepada ahli-ahli Jawatankuasa selewat-lewatnya tujuh (7) hari sebelum tarikh yang ditetapkan bagi mesyuarat itu atau mengikut keperluan.
2. Notis bagi sesuatu mesyuarat hendaklah menyatakan tempat, tarikh dan masa yang ditetapkan bagi mesyuarat itu.

Agenda :

1. Agenda bagi sesuatu mesyuarat serta kertas-kertas yang berkaitan hendaklah disampaikan kepada ahli-ahli Jawatankuasa sekurang-kurangnya tujuh (7) hari sebelum tarikh yang ditetapkan bagi mesyuarat itu atau mengikut keperluan.
2. Seseorang ahli Jawatankuasa yang hendak memasukkan sesuatu perkara dalam agenda mesyuarat hendaklah memberitahu Setiausaha sekurang-kurangnya tiga (3) hari sebelum mesyuarat diadakan.

Kuorum : Kuorum mesyuarat adalah separuh daripada jumlah ahli keseluruhan.

Perjalanan Mesyuarat :

1. Pengerusi, jika ia hadir, hendaklah mempengerusikan semua Mesyuarat Jawatankuasa.
2. Jika Pengerusi tidak hadir pada sesuatu mesyuarat Jawatankuasa atau sebahagian darinya, maka selama ia tidak hadir itu mesyuarat hendaklah dipengerusikan oleh mana-mana ahli jawatankuasa yang diarahkan oleh Pengerusi.
3. Perjalanan sesuatu mesyuarat Jawatankuasa hendaklah mengikut agenda mesyuarat yang telah diedarkan terlebih dahulu. Dengan syarat bahawa Jawatankuasa boleh, jika difikirkannya patut, meminda susunan perkara-perkara yang telah dimasukkan dalam agenda.

4. Apa-apa perkara yang tidak ada dalam agenda bagi sesuatu mesyuarat boleh, jika difikirkan patut oleh Jawatankuasa, ditimbang dan diputuskan oleh Jawatankuasa pada mesyuarat itu di bawah "Hal-hal lain".

5. Jika sesuatu mesyuarat ditamatkan sebelum menyelesaikan kesemua perkara dalam agenda bagi mesyuarat itu, maka perkara yang belum selesai itu bolehlah diselesaikan dalam agenda bagi mesyuarat yang berikutnya.

   Dengan syarat bahawa jika dipersetujui oleh semua ahli yang hadir, sesuatu mesyuarat boleh ditangguhkan untuk disambung semula pada tarikh dan masa yang ditetapkan oleh Jawatankuasa.

6. Sesuatu usul yang pada pendapat Setiausaha memerlukan keputusan segera boleh dikemukakan untuk keputusan jawatankuasa menerusi surat edaran kepada ahli-ahli Jawatankuasa dan dalam hal demikian tiap-tiap ahli hendaklah diberi masa sekurang-kurangnya tiga (3) hari untuk menyatakan pendapatnya atas usul itu.

7. Sesuatu usul yang dikemukakan secara edaran hendaklah diputuskan mengikut persetujuan sebulat suara semua ahli yang memberi jawapan kepada Setiausaha dalam masa yang diberikan menurut sub perenggan (1): Dengan syarat bahawa bilangan ahli yang memberi jawapan itu hendaklah tidak kurang daripada bilangan yang diperlukan untuk mengadakan kuorum.

8. Jika pada akhir masa yang diberikan menurut sub perenggan (1) itu didapati bahawa:

   (1) Terdapat sekurang-kurangnya dua (2) orang ahli yang memberi jawapan menyatakan mereka tidak bersetuju dengan usul yang dikemukakan secara edaran itu, maka usul itu hendaklah dibentangkan dalam suatu mesyuarat yang berikutnya.

   (2) Bagi seseorang ahli yang tidak memberi jawapan dalam masa yang ditetapkan, jawapan tersebut akan dinyatakan sebagai bersetuju dengan usul yang dikemukakan secara edaran itu.

9. Tiap-tiap keputusan yang dibuat secara edaran hendaklah dilaporkan kepada Jawatankuasa dalam mesyuarat yang berikutnya untuk makluman.

Minit dan Laporan : 1. Minit-minit bagi sesuatu mesyuarat Jawatankuasa hendaklah diedarkan dan laporan kepada ahli-ahli Jawatankuasa dalam masa sepuluh (10) hari bekerja selepas mesyuarat itu diadakan.

2. Cadangan-cadangan bagi meminda sesuatu minit hendaklah disampaikan kepada Setiausaha dalam masa

sepuluh (10) hari bekerja selepas minit itu diedarkan kepada ahli-ahli. Jika tiada apa-apa cadangan diterima oleh Setiausaha dalam tempoh itu, maka minit itu sebagaimana yang disediakan oleh Setiausaha hendaklah dianggap betul dan tindakan- tindakan berasaskan kepadanya boleh diambil.

3. Minit-minit bagi sesuatu mesyuarat atau mesyuarat khas hendaklah disahkan dalam mesyuarat yang berikutnya.

   Tertakluk kepada sub perenggan (1), minit-minit mesyuarat yang disahkan hendaklah disifatkan sebagai rekod yang lengkap mengenai keputusan-keputusan yang dibuat oleh Jawatankuasa.

   Jika ada apa-apa keraguan mengenai tafsiran sesuatu minit mesyuarat Jawatankuasa maka perkara itu hendaklah diputuskan dengan merujuk kepada apa-apa kertas Jawatankuasa yang telah dibentangkan dalam mesyuarat itu. Jika keraguan itu tidak dapat dijelaskan dengan cara demikian Jawatankuasa hendaklah memutuskan perkara itu sebagaimana yang difikirkan patut oleh Jawatankuasa.

Meminda Peraturan Tatacara Mesyuarat : Pindaan kepada tatacara mesyuarat ini boleh diluluskan menerusi ketetapan Jawatankuasa yang dibuat dalam sesuatu mesyuarat Jawatankuasa dengan persetujuan sekurang- kurangnya dua pertiga daripada jumlah ahli Jawatankuasa.

Dengan syarat bahawa sesuatu pindaan kepada tatacara mesyuarat ini tidak boleh dikuatkuasa sehingga pindaan itu dibawa untuk kelulusan Pihak Berkuasa yang berkaitan.

Diluluskan oleh:

YBHG. PROFESOR DATO' SERI IR. DR.
NOOR AZUAN ABU OSMAN
Naib Canselor
Universiti Malaya

Tarikh: 1 OKTOBER 2024

LAMPIRAN B2: TERMA RUJUKAN JAWATANKUASA PENGGUNA ICT (JPICT)

UNIVERSITI MALAYA

Terma Rujukan Jawatankuasa

Nama Jawatankuasa	:	Jawatankuasa Pengguna ICT (JPICT)
Pengenalan	:	JPICT adalah salah satu dari tiga buah Jawatankuasa di bawah tadbir urus ICT Universiti Malaya (UM). JPICT membincangkan hal-hal berkaitan kepenggunaan ICT (Community Engagement) di UM dan menyuarakan keperluan ICT kepada Jawatankuasa Pengurusan ICT (JKPICT).
Punca Kuasa	:	Naib Canselor melantik ahli JPICT
Keanggotaan	:	**Pengerusi** Timbalan Naib Canselor (Pembangunan) **Timbalan Pengerusi** Ketua Pegawai Digital (CDO) **Setiausaha Tetap:** Pengarah Eksekutif JTM **Ahli:** 1. Dekan Fakulti Komputer Sains & Teknologi Maklumat (FSKTM) 2. Pengarah Eksekutif Jabatan Kesarjanaan Digital dan Maklumat Semesta (Perpustakaan) 3. Dua (2) orang staf akademik mewakili aliran sains 4. Dua (2) orang staf akademik mewakili aliran sastera 5. Satu (1) orang Pengetua Kolej Kediaman 6. Satu (1) staf Bahagian Hal Ehwal Pelajar 7. Dua (2) orang staf bukan akademik 8. Dua (2) orang wakil pelajar Ijazah Dasar (wakil Kesatuan Mahasiswa Universiti Malaya) 9. Dua (2) orang wakil pelajar Ijazah Tinggi **Jemputan:** Pengarah-pengarah Pusat JTM (Tetap) dan Ahli Jemputan Universiti Malaya jika perlu **Urusetia:** Seksyen Governan Digital, JTM

Tempoh Keanggotaan	:	Tempoh jawatan adalah dua (2) tahun untuk Pengerusi dan ahli-ahli yang lain kecuali wakil pelajar, di mana pelantikan adalah secara tahunan.
Bidang Kuasa Jawatankuasa	:	1. Melaporkan isu-isu ICT kepada Jawatankuasa Pengurusan ICT 2. Mengumpul maklum balas berkaitan dengan kemudahan ICT di PTj 3. Mencadangkan penambahbaikan kemudahan ICT Universiti Malaya 4. Melaksanakan tanggungjawab lain yang diarahkan oleh Jawatankuasa Pemandu ICT.
Mesyuarat	:	Jawatankuasa hendaklah bermesyuarat sekurang-kurangnya tiga (3) kali setahun.
Notis Mesyuarat	:	1. Notis bagi sesuatu mesyuarat hendaklah disampaikan secara bertulis atau secara elektronik oleh Setiausaha kepada ahli-ahli Jawatankuasa selewat-lewatnya tujuh (7) hari sebelum tarikh yang ditetapkan bagi mesyuarat itu atau mengikut keperluan. 2. Notis bagi sesuatu mesyuarat hendaklah menyatakan tempat, tarikh dan masa yang ditetapkan bagi mesyuarat tersebut. 3. Seseorang ahli Jawatankuasa yang hendak memasukkan sesuatu perkara dalam agenda mesyuarat hendaklah memberitahu Setiausaha sekurang-kurangnya tiga (3) hari sebelum mesyuarat diadakan.
Agenda	:	1. Agenda bagi sesuatu mesyuarat serta kertas-kertas yang berkaitan hendaklah disampaikan kepada ahli-ahli Jawatankuasa sekurang-kurangnya tujuh (7) hari sebelum tarikh yang ditetapkan bagi mesyuarat itu atau mengikut keperluan. 2. Seseorang ahli Jawatankuasa yang hendak memasukkan sesuatu perkara dalam agenda mesyuarat hendaklah memberitahu Setiausaha sekurang-kurangnya tiga (3) hari sebelum mesyuarat diadakan.
Kuorum	:	Kuorum mesyuarat adalah separuh daripada jumlah ahli keseluruhan.

Perjalanan Mesyuarat :

1. Pengerusi, jika ia hadir, hendaklah mempengerusikan semua Mesyuarat Jawatankuasa.
2. Jika Pengerusi tidak hadir pada sesuatu mesyuarat Jawatankuasa atau sebahagian darinya, maka selama ia tidak hadir, mesyuarat hendaklah dipengerusikan oleh Timbalan Pengerusi atau mana-mana ahli jawatankuasa yang diarahkan oleh Pengerusi.
3. Perjalanan sesuatu mesyuarat Jawatankuasa hendaklah mengikut agenda mesyuarat yang telah diedarkan terlebih dahulu. Dengan syarat bahawa Jawatankuasa boleh, jika difikirkannya patut, meminda susunan perkara-perkara yang telah dimasukkan dalam agenda.
4. Apa-apa perkara yang tidak ada dalam agenda bagi sesuatu mesyuarat boleh, jika difikirkan patut oleh Jawatankuasa, ditimbang dan diputuskan oleh Jawatankuasa pada mesyuarat itu di bawah "Hal-hal lain".
5. Jika sesuatu mesyuarat ditamatkan sebelum menyelesaikan kesemua perkara dalam agenda bagi mesyuarat itu, maka perkara yang belum selesai itu bolehlah diselesaikan dalam agenda bagi mesyuarat yang berikutnya.

   Dengan syarat bahawa jika dipersetujui oleh semua ahli yang hadir, sesuatu mesyuarat boleh ditangguhkan untuk disambung semula pada tarikh dan masa yang ditetapkan oleh Jawatankuasa.
6. Sesuatu usul yang pada pendapat Setiausaha memerlukan keputusan segera boleh dikemukakan untuk keputusan jawatankuasa menerusi surat edaran kepada ahli-ahli Jawatankuasa dan dalam hal demikian tiap-tiap ahli hendaklah diberi masa sekurang-kurangnya tiga (3) hari untuk menyatakan pendapatnya atas usul itu.
7. Sesuatu usul yang dikemukakan secara edaran hendaklah diputuskan mengikut persetujuan sebulat suara semua ahli yang memberi jawapan kepada Setiausaha dalam masa yang diberikan menurut sub perenggan (a): Dengan syarat bahawa bilangan ahli yang memberi jawapan itu hendaklah tidak kurang daripada bilangan yang diperlukan untuk mengadakan kuorum.

8. Jika pada akhir masa yang diberikan menurut sub perenggan (a) itu didapati bahawa:

   (1) Terdapat sekurang-kurangnya dua (2) orang ahli yang memberi jawapan menyatakan mereka tidak bersetuju dengan usul yang dikemukakan secara edaran itu, maka usul itu hendaklah dibentangkan dalam suatu mesyuarat yang berikutnya.

   (2) Bagi seseorang ahli yang tidak memberi jawapan dalam masa yang ditetapkan, jawapan tersebut akan dinyatakan sebagai bersetuju dengan usul yang dikemukakan secara edaran itu.

9. Tiap-tiap keputusan yang dibuat secara edaran hendaklah dilaporkan kepada Jawatankuasa dalam mesyuarat yang berikutnya untuk makluman.

Minit dan Laporan :

1. Minit-minit bagi sesuatu mesyuarat Jawatankuasa hendaklah diedarkan dan laporan kepada ahli-ahli Jawatankuasa dalam masa sepuluh (10) hari bekerja selepas mesyuarat itu diadakan.

2. Cadangan-cadangan bagi meminda sesuatu minit hendaklah disampaikan kepada Setiausaha dalam masa sepuluh (10) hari bekerja selepas minit itu diedarkan kepada ahli-ahli. Jika tiada apa-apa cadangan diterima oleh Setiausaha dalam tempoh itu, maka minit itu sebagaimana yang disediakan oleh Setiausaha hendaklah dianggap betul dan tindakan-tindakan berasaskan kepadanya boleh diambil.

3. Minit-minit bagi sesuatu mesyuarat atau mesyuarat khas hendaklah disahkan dalam mesyuarat yang berikutnya.

4. Tertakluk kepada subperenggan (a), minit-minit mesyuarat yang disahkan hendaklah disifatkan sebagai rekod yang lengkap mengenai keputusan-keputusan yang dibuat oleh Jawatankuasa.

Meminda Peraturan Tatacara Mesyuarat :

Pindaan kepada tatacara mesyuarat ini boleh diluluskan menerusi ketetapan Jawatankuasa yang dibuat dalam sesuatu mesyuarat Jawatankuasa, dengan persetujuan sekurang-kurangnya dua pertiga daripada jumlah ahli Jawatankuasa.

Dengan syarat bahawa sesuatu pindaan kepada tatacara mesyuarat ini tidak boleh dikuatkuasa sehingga pindaan itu dibawa untuk kelulusan Pihak Berkuasa yang berkaitan.

Diluluskan oleh:

YBHG. PROFESOR DATO' SERI IR. DR.
NOOR AZUAN ABU OSMAN
Naib Canselor
Universiti Malaya

Tarikh: 29 APR 2025

LAMPIRAN B3: TERMA RUJUKAN JAWATANKUASA TEKNIKAL ICT (JTICT)

UNIVERSITI MALAYA

Terma Rujukan Jawatankuasa

Nama Jawatankuasa	:	Jawatankuasa Teknikal ICT (JTICT), Universiti Malaya
Pengenalan	:	JTICT adalah salah satu dari tiga buah Jawatankuasa di bawah tadbir urus ICT Universiti Malaya (UM). JTICT menilai secara teknikal dan kos permohonan projek-projek ICT di UM untuk menyokong visi dan misi UM.
Punca Kuasa	:	Naib Canselor melantik ahli JTICT
Keanggotaan	:	**Pengerusi:** Timbalan Naib Canselor (Pembangunan) **Timbalan Pengerusi:** Ketua Pegawai Digital (CDO) **Ahli:** 1. Pendaftar/Wakil Tetap 2. Bendahari/Wakil Tetap 3. Pengarah Eksekutif, Jabatan Teknologi Maklumat (JTM) 4. Pengarah Eksekutif, Jabatan Kesarjanaan Digital dan Maklumat Semesta (Perpustakaan) 5. Pengarah, Jabatan Teknologi Maklumat (JTM), Pusat Perubatan Universiti Malaya (PPUM) 6. Pengarah, Pusat Pengurusan Data dan Maklumat (PPDM) 7. Wakil Tetap Staf Akademik Bidang Kepakaran Rangkaian *(Networking)*, Fakulti Sains Komputer & Teknologi Maklumat (FSKTM) 8. Wakil Tetap Staf Akademik Bidang Kepakaran Keselamatan (*Security*), Fakulti Sains Komputer & Teknologi Maklumat (FSKTM) 9. Wakil Tetap Staf Akademik Bidang Kepakaran Kepintaran Buatan (*Artificial Intelligence*), Fakulti Sains Komputer & Teknologi Maklumat (FSKTM) 10. Wakil Tetap Staf Akademik Bidang Kepakaran Sistem Maklumat (*Information System*), Fakulti Sains Komputer & Teknologi Maklumat (FSKTM)

Jemputan:
Pengarah-Pengarah Pusat JTM (Tetap) dan
Ahli jemputan Universiti Malaya jika perlu

Urusetia:
Seksyen Governan Digital, JTM

Bidang Kuasa Jawatankuasa :

1. Menilai dan melulus semua permohonan perolehan projek ICT UM berdasarkan peraturan-peraturan semasa yang berkuatkuasa.
2. Mengesyorkan kelulusan teknikal projek ICT kepada JPICT KPT.
3. Memantau kemajuan pembangunan dan pelaksanaan projek ICT UM yang diluluskan oleh JPICT KPT/JTISA dan melapor kepada JPICT KPT.
4. Mengenal pasti masalah dan isu semasa dalam pembangunan atau pelaksanaan projek ICT Universiti serta mengesyorkan cadangan penyelesaian kepada JPICT KPT.
5. Menyelaras dan menyeragamkan pembangunan ICT UM agar selari dengan Pelan Anjakan Digital.
6. Meluluskan projek dan pembelian berkaitan ICT sebelum urusan perolehan dilaksanakan.

Kuasa Melulus Jawatankuasa :

Bil.	Kategori Permohonan	Kuasa Melulus
1.	Perolehan ICT nilai di bawah RM2 ribu	Pengerusi
2.	Perolehan ICT nilai di bawah RM50 ribu	Kelulusan Secara Edaran
3.	Perolehan ICT nilai melebihi RM50 ribu	JTICT

Mesyuarat : Jawatankuasa hendaklah bersidang sekurang-kurangnya dua (2) kali dalam tempoh satu (1) bulan. Pengerusi Jawatankuasa boleh memanggil mesyuarat pada bila-bila masa sekiranya perlu.

Notis Mesyuarat :

1. Notis bagi sesuatu mesyuarat hendaklah disampaikan secara bertulis atau secara elektronik oleh Setiausaha kepada ahli-ahli Jawatankuasa selewat-lewatnya tujuh (7) hari sebelum tarikh yang ditetapkan bagi mesyuarat itu atau mengikut keperluan.
2. Notis bagi sesuatu mesyuarat hendaklah menyatakan tempat, tarikh dan masa yang ditetapkan bagi mesyuarat tersebut.
3. Seseorang ahli Jawatankuasa yang hendak memasukkan sesuatu perkara dalam agenda mesyuarat hendaklah memberitahu Setiausaha sekurang-kurangnya tiga (3) hari sebelum mesyuarat diadakan.

Kuorum : Mesyuarat perlu dihadiri sekurang-kurangnya 1/3 daripada ahli jawatankuasa yang dilantik, termasuk Pengerusi.

Perjalanan Mesyuarat :

1. Pengerusi, jika ia hadir, hendaklah mempengerusikan semua Mesyuarat Jawatankuasa.
2. Jika Pengerusi tidak hadir pada sesuatu mesyuarat Jawatankuasa atau sebahagian darinya, maka selama ia tidak hadir, mesyuarat hendaklah dipengerusikan oleh Timbalan Pengerusi atau mana-mana ahli jawatankuasa yang diarahkan oleh Pengerusi.
3. Perjalanan sesuatu mesyuarat Jawatankuasa hendaklah mengikut agenda mesyuarat yang telah diedarkan terlebih dahulu. Dengan syarat bahawa Jawatankuasa boleh, jika difikirkannya patut, meminda susunan perkara-perkara yang telah dimasukkan dalam agenda.
4. Apa-apa perkara yang tidak ada dalam agenda bagi sesuatu mesyuarat boleh, jika difikirkan patut oleh Jawatankuasa, ditimbang dan diputuskan oleh Jawatankuasa pada mesyuarat itu di bawah "Hal-hal lain".
5. Jika sesuatu mesyuarat ditamatkan sebelum menyelesaikan kesemua perkara dalam agenda bagi mesyuarat itu, maka perkara yang belum selesai itu bolehlah diselesaikan dalam agenda bagi mesyuarat yang berikutnya.

   Dengan syarat bahawa jika dipersetujui oleh semua ahli yang hadir, sesuatu mesyuarat boleh ditangguhkan untuk disambung semula pada tarikh dan masa yang ditetapkan oleh Jawatankuasa.
6. Sesuatu usul yang pada pendapat Setiausaha memerlukan keputusan segera boleh dikemukakan untuk keputusan jawatankuasa menerusi surat edaran kepada ahli-ahli Jawatankuasa dan dalam hal demikian tiap-tiap ahli hendaklah diberi masa sekurang-kurangnya tiga (3) hari untuk menyatakan pendapatnya atas usul itu.
7. Sesuatu usul yang dikemukakan secara edaran hendaklah diputuskan mengikut persetujuan sebulat suara semua ahli yang memberi jawapan kepada Setiausaha dalam masa yang diberikan menurut sub perenggan (a): Dengan syarat bahawa bilangan ahli yang memberi jawapan itu hendaklah tidak kurang daripada bilangan yang diperlukan untuk mengadakan kuorum.
8. Jika pada akhir masa yang diberikan menurut sub perenggan (a) itu didapati bahawa:

   (1) Terdapat sekurang-kurangnya dua (2) orang ahli yang memberi jawapan menyatakan mereka tidak bersetuju dengan usul yang dikemukakan secara edaran itu, maka usul itu hendaklah dibentangkan dalam suatu mesyuarat yang berikutnya.

(2) Bagi seseorang ahli yang tidak memberi jawapan dalam masa yang ditetapkan, jawapan tersebut akan dinyatakan sebagai bersetuju dengan usul yang dikemukakan secara edaran itu.

9. Tiap-tiap keputusan yang dibuat secara edaran hendaklah dilaporkan kepada Jawatankuasa dalam mesyuarat yang berikutnya untuk makluman.

Minit dan Laporan :

1. Minit-minit Jawatankuasa hendaklah diedarkan dan laporkan kepada ahli-ahli Jawatankuasa dalam masa sepuluh (10) hari bekerja selepas mesyuarat diadakan.
2. Cadangan-cadangan bagi meminda sesuatu minit hendaklah disampaikan kepada Setiausaha dalam masa sepuluh (10) hari bekerja selepas minit itu diedarkan kepada ahli-ahli. Jika tiada apa-apa cadangan diterima oleh Setiausaha dalam tempoh itu, maka minit itu sebagaimana yang disediakan oleh Setiausaha hendaklah dianggap betul dan tindakan- tindakan berasaskan kepadanya boleh diambil.
3. Minit-minit bagi sesuatu mesyuarat atau mesyuarat khas hendaklah disahkan dalam mesyuarat yang berikutnya.
4. Jika ada apa-apa keraguan mengenai tafsiran sesuatu minit mesyuarat Jawatankuasa maka perkara itu hendaklah diputuskan dengan merujuk kepada apa- apa kertas Jawatankuasa yang telah dibentangkan dalam mesyuarat itu. Jika keraguan itu tidak dapat dijelaskan dengan cara demikian Jawatankuasa hendaklah memutuskan perkara itu sebagaimana yang difikirkan patut oleh Jawatankuasa.

Meminda Peraturan Tatacara Mesyuarat :

Pindaan kepada tatacara mesyuarat ini boleh diluluskan menerusi ketetapan Jawatankuasa yang dibuat dalam sesuatu mesyuarat Jawatankuasa dengan persetujuan sekurang-kurangnya dua pertiga daripada jumlah ahli Jawatankuasa.

Dengan syarat bahawa sesuatu pindaan kepada tatacara mesyuarat ini tidak boleh dikuatkuasa sehingga pindaan itu dibawa untuk kelulusan Pihak Berkuasa yang berkaitan.

Diluluskan oleh:

YBHG. PROFESOR DATO' SERI IR. DR.
NOOR AZUAN ABU OSMAN

Naib Canselor
Universiti Malaya

Tarikh: 30 APR 2025

LAMPIRAN B4: TERMA RUJUKAN JAWATANKUASA PENILAIAN SISTEM APLIKASI (JPSA)

UNIVERSITI MALAYA

Terma Rujukan Jawatankuasa

Nama Jawatankuasa	:	Jawatankuasa Penilaian Sistem Aplikasi (JPSA), Universiti Malaya
Pengenalan	:	Jawatankuasa Penilaian Sistem Aplikasi (JPSA) adalah salah satu dari Jawatankuasa di bawah tadbir urus ICT Universiti Malaya. JPSA adalah merupakan Jawatankuasa yang bertanggungjawab dalam membuat penilaian bagi semua permohonan pembangunan/perolehan baharu, penaiktarafan dan perubahan sistem aplikasi sedia ada. Hanya projek yang mendapat sokongan JPSA layak dikemukakan untuk kelulusan teknikal daripada Jawatankuasa Teknikal ICT (JTICT) Universiti Malaya.
Punca Kuasa	:	Naib Canselor melantik ahli JPSA
Keanggotaan		**Pengerusi:** Timbalan Naib Canselor (Pembangunan) **Timbalan Pengerusi:** Ketua Pegawai Digital (CDO) **Ahli :** 1. Pendaftar/Wakil Tetap 2. Pengarah Eksekutif, Jabatan Teknologi Maklumat (JTM) 3. Dekan/Wakil tetap, Fakulti Sains Komputer & Teknologi Maklumat (FSKTM) 4. Seorang (1) staf akademik bertaraf Profesor, masing masing mewakili aliran Sains dan Sains Sosial 5. Seorang (1) Wakil Tetap Persatuan Kakitangan Akademik UM (PKAUM) 6. Pengarah, Pusat Penyelesaian dan Pembangunan Digital, JTM 7. Pengarah, Pusat Pengurusan Data dan Maklumat (PPDM) 8. Pengarah, Jabatan Teknologi Maklumat (JTM), Pusat Perubatan Universiti Malaya (PPUM) **Jemputan:** Pengarah-pengarah Pusat JTM (Tetap) dan Ahli jemputan di Universiti Malaya jika perlu

Urusetia:
Seksyen Governan Digital JTM

Bidang Kuasa Jawatankuasa :

1. Menilai secara keseluruhan impak permohonan pembangunan/perolehan baharu, penaiktarafan dan perubahan sistem aplikasi sedia ada termasuk dari aspek keperluan integrasi antara platform, infrastruktur pelayan atau perkakasan, kos pembangunan sebenar meliputi masa, tenaga kerja dan kewangan.
2. Menilai pembangunan/perolehan baharu, penaiktarafan dan perubahan sistem aplikasi sedia ada, antaranya, bagi memastikan tidak berlaku duplikasi/percanggahan projek yang dikemukakan dengan sistem sedia ada dan ia adalah selari dengan pelan strategik ICT dan/ atau Universiti.
3. Menyokong permohonan pembangunan/ perolehan baharu, penaiktarafan dan perubahan sistem aplikasi sedia ada setelah membuat penilaian sewajarnya.
4. Mempertimbang dan meluluskan pentauliahan serta penyahtauliahan sistem aplikasi di dalam Universiti Malaya.

Kuasa Melulus Jawatankuasa :

Bil	Kategori Permohonan	Kuasa Melulus
1.	Pembangunan/perolehan baharu berkaitan sistem aplikasi yang dimohon oleh PTj atau projek dalaman PTM (sama ada melibatkan kos atau tidak)	JPSA
2.	Penaiktarafan/perubahan aplikasi sedia ada yang dimohon oleh PTj (sama ada melibatkan kos atau tidak)	JPSA
3.	Penaiktarafan/perubahan kepada sistem aplikasi sedia ada yang merupakan projek dalaman PTM (sama ada melibatkan kos atau tidak)	Pengerusi JPSA
4.	Perubahan berskala kecil kepada sistem aplikasi sedia ada yang dimohon oleh PTj.	Ketua Seksyen Aplikasi

Mesyuarat : Jawatankuasa hendaklah bermesyuarat sekurang kurangnya empat (4) kali setahun. Pengerusi Jawatankuasa boleh memanggil mesyuarat pada bila-bila masa jika ada keperluan.

Notis Mesyuarat	:	1. Notis bagi sesuatu mesyuarat hendaklah disampaikan secara bertulis atau secara elektronik oleh Setiausaha kepada ahli-ahli Jawatankuasa selewat-lewatnya tujuh (7) hari sebelum tarikh yang ditetapkan bagi mesyuarat itu atau mengikut keperluan. 2. Notis bagi sesuatu mesyuarat hendaklah menyatakan tempat, tarikh dan masa yang ditetapkan bagi mesyuarat itu.
Agenda	:	1. Agenda bagi sesuatu mesyuarat serta kertas-kertas yang berkaitan hendaklah disampaikan kepada ahli-ahli Jawatankuasa sekurang-kurangnya tujuh (7) hari sebelum tarikh yang ditetapkan bagi mesyuarat itu atau mengikut keperluan. 2. Seseorang ahli Jawatankuasa yang hendak memasukkan sesuatu perkara dalam agenda mesyuarat hendaklah memberitahu Setiausaha sekurang-kurangnya tiga (3) hari sebelum mesyuarat diadakan.
Kuorum	:	Mesyuarat perlu dihadiri sekurang-kurangnya 1/3 daripada ahli jawatankuasa yang dilantik, termasuk Pengerusi.
Perjalanan Mesyuarat	:	1. Pengerusi, jika ia hadir, hendaklah mempengerusikan semua Mesyuarat Jawatankuasa. 2. Jika Pengerusi tidak hadir pada sesuatu mesyuarat Jawatankuasa atau sebahagian darinya, maka selama ia tidak hadir, mesyuarat hendaklah dipengerusikan oleh Timbalan Pengerusi atau mana-mana ahli jawatankuasa yang diarahkan oleh Pengerusi. 3. Perjalanan sesuatu mesyuarat Jawatankuasa hendaklah mengikut agenda mesyuarat yang telah diedarkan terlebih dahulu. Dengan syarat bahawa Jawatankuasa boleh, jika difikirkannya patut, meminda susunan perkara-perkara yang telah dimasukkan dalam agenda. 4. Apa-apa perkara yang tidak ada dalam agenda bagi sesuatu mesyuarat boleh, jika difikirkan patut oleh Jawatankuasa, ditimbang dan diputuskan oleh Jawatankuasa pada mesyuarat itu di bawah "Hal-hal lain". 5. Jika sesuatu mesyuarat ditamatkan sebelum menyelesaikan kesemua perkara dalam agenda bagi mesyuarat itu, maka perkara yang belum selesai itu bolehlah diselesaikan dalam agenda bagi mesyuarat yang berikutnya.

Dengan syarat bahawa jika dipersetujui oleh semua ahli yang hadir, sesuatu mesyuarat boleh ditangguhkan untuk disambung semula pada tarikh dan masa yang ditetapkan oleh Jawatankuasa.

6. Sesuatu usul yang pada pendapat Setiausaha memerlukan keputusan segera boleh dikemukakan untuk keputusan jawatankuasa menerusi surat edaran kepada ahli-ahli Jawatankuasa dan dalam hal demikian tiap-tiap ahli hendaklah diberi masa sekurang-kurangnya tiga (3) hari untuk menyatakan pendapatnya atas usul itu.

7. Sesuatu usul yang dikemukakan secara edaran hendaklah diputuskan mengikut persetujuan sebulat suara semua ahli yang memberi jawapan kepada Setiausaha dalam masa yang diberikan menurut sub perenggan (a): Dengan syarat bahawa bilangan ahli yang memberi jawapan itu hendaklah tidak kurang daripada bilangan yang diperlukan untuk mengadakan kuorum.

8. Jika pada akhir masa yang diberikan menurut sub perenggan (a) itu didapati bahawa:

   (1) Terdapat sekurang-kurangnya dua (2) orang ahli yang memberi jawapan menyatakan mereka tidak bersetuju dengan usul yang dikemukakan secara edaran itu, maka usul itu hendaklah dibentangkan dalam suatu mesyuarat yang berikutnya.

   (2) Bagi seseorang ahli yang tidak memberi jawapan dalam masa yang ditetapkan, jawapan tersebut akan dinyatakan sebagai bersetuju dengan usul yang dikemukakan secara edaran itu.

9. Tiap-tiap keputusan yang dibuat secara edaran hendaklah dilaporkan kepada Jawatankuasa dalam mesyuarat yang berikutnya untuk makluman.

Minit dan Laporan :

1. Minit-minit bagi sesuatu mesyuarat Jawatankuasa hendaklah diedarkan dan laporan kepada ahli-ahli Jawatankuasa dalam masa sepuluh (10) hari bekerja selepas mesyuarat itu diadakan.

2. Cadangan-cadangan bagi meminda sesuatu minit hendaklah disampaikan kepada Setiausaha dalam masa sepuluh (10) hari bekerja selepas minit itu diedarkan kepada ahli-ahli. Jika tiada apa-apa cadangan diterima oleh Setiausaha dalam tempoh itu, maka minit itu sebagaimana yang disediakan oleh Setiausaha hendaklah dianggap betul dan tindakan- tindakan berasaskan kepadanya boleh diambil.

3. Minit-minit bagi sesuatu mesyuarat atau mesyuarat khas hendaklah disahkan dalam mesyuarat yang berikutnya.

   Tertakluk kepada subperenggan (a), minit-minit mesyuarat yang disahkan hendaklah disifatkan sebagai rekod yang lengkap mengenai keputusan-keputusan yang dibuat oleh Jawatankuasa.

4. Jika ada apa-apa keraguan mengenai tafsiran sesuatu minit mesyuarat Jawatankuasa maka perkara itu hendaklah diputuskan dengan merujuk kepada apa-apa kertas Jawatankuasa yang telah dibentangkan dalam mesyuarat itu. Jika keraguan itu tidak dapat dijelaskan dengan cara demikian Jawatankuasa hendaklah memutuskan perkara itu sebagaimana yang difikirkan patut oleh Jawatankuasa.

Meminda Peraturan Tatacara Mesyuarat : Pindaan kepada tatacara mesyuarat ini boleh diluluskan menerusi ketetapan Jawatankuasa yang dibuat dalam sesuatu mesyuarat Jawatankuasa dengan persetujuan sekurang-kurangnya dua pertiga daripada jumlah ahli Jawatankuasa.

Dengan syarat bahawa sesuatu pindaan kepada tatacara mesyuarat ini tidak boleh dikuatkuasa sehingga pindaan itu dibawa untuk kelulusan Pihak Berkuasa yang berkaitan.

Diluluskan oleh:

YBHG. PROFESOR DATO' SERI IR. DR.
NOOR AZUAN ABU OSMAN
Naib Canselor
Universiti Malaya

Tarikh: 29 APR 2025

LAMPIRAN B5: TERMA RUJUKAN JAWATANKUASA PEMBANGUNAN PROJEK ICT (JAPPICT)

UNIVERSITI MALAYA

Terma Rujukan Jawatankuasa

Nama Jawatankuasa	:	Jawatankuasa Pembangunan Projek ICT (JAPPICT)
Pengenalan	:	JAPPICT adalah satu Jawatankuasa di bawah seliaan Ketua Pegawai Digital (CDO). JAPPICT bertanggungjawab memperakukan kebolehlaksanaan dan memantau pelaksanaan projek ICT di bawah JTM, memastikan setiap projek dilaksanakan secara menyeluruh, selaras dengan prosedur yang ditetapkan, menggunakan sumber secara optimum, serta disiapkan mengikut jangka masa yang ditetapkan.
Punca Kuasa	:	Ketua Pegawai Digital (CDO) melantik ahli JAPICT.
Keanggotaan	:	**Pengerusi:** Ketua Pegawai Digital (CDO) **Ahli:** 1. Pengarah Eksekutif JTM 2. Pengarah Pusat JTM 3. Ketua Pengurus Projek **Urus Setia:** Seksyen Governan Digital, JTM **Jemputan:** Pegawai dari JTM jika perlu.
Tempoh Keanggotaan	:	Tempoh jawatan adalah selama dua (2) tahun atau seperti yang dinyatakan dalam surat pelantikan.
Bidang Kuasa Jawatankuasa	:	1. Memperakukan kebolehlaksanaan projek berdasarkan dokumen permohonan yang dikemukakan. 2. Mengesyorkan kertas kerja permohonan pelaksanaan projek ICT untuk kelulusan pengurusan yang lebih tinggi. 3. Mengenalpasti keperluan, isu dan masalah yang timbul serta memberikan cadangan penyelesaian. 4. Memantau perkembangan status pelaksanaan dan kewangan projek ICT.
Mesyuarat	:	Jawatankuasa hendaklah bermesyuarat sekurang-kurangnya empat (4) kali setahun. Pengerusi Jawatankuasa

boleh memanggil mesyuarat pada bila-bila masa jika ada keperluan.

Notis Mesyuarat :

1. Notis bagi sesuatu mesyuarat hendaklah disampaikan secara bertulis atau secara elektronik oleh Urus Setia kepada ahli-ahli Jawatankuasa selewat-lewatnya tujuh (7) hari sebelum tarikh yang ditetapkan bagi mesyuarat itu atau mengikut keperluan.
2. Notis bagi sesuatu mesyuarat hendaklah menyatakan tempat, tarikh dan masa yang ditetapkan bagi mesyuarat tersebut.
3. Seseorang ahli Jawatankuasa yang hendak memasukkan sesuatu perkara dalam agenda mesyuarat hendaklah memberitahu Urus Setia sekurang-kurangnya tiga (3) hari sebelum mesyuarat diadakan.

Agenda :

1. Agenda bagi sesuatu mesyuarat serta kertas-kertas yang berkaitan hendaklah disampaikan kepada ahli- ahli Jawatankuasa sekurang-kurangnya tujuh (7) hari sebelum tarikh yang ditetapkan bagi mesyuarat itu atau mengikut keperluan.
2. Seseorang ahli Jawatankuasa yang hendak memasukkan sesuatu perkara dalam agenda mesyuarat hendaklah memberitahu Urus Setia sekurang-kurangnya tiga (3) hari sebelum mesyuarat diadakan.

Kuorum : Mesyuarat perlu dihadiri tidak kurang dari separuh (1/2) keahlian jawatankuasa yang dilantik, termasuk Pengerusi.

Perjalanan Mesyuarat :

1. Pengerusi, jika ia hadir, hendaklah mempengerusikan semua Mesyuarat Jawatankuasa.
2. Jika Pengerusi tidak hadir pada sesuatu mesyuarat Jawatankuasa atau sebahagian darinya, maka selama ia tidak hadir, mesyuarat hendaklah dipengerusikan oleh mana-mana ahli jawatankuasa yang diarahkan oleh Pengerusi.
3. Perjalanan sesuatu mesyuarat Jawatankuasa hendaklah mengikut agenda mesyuarat yang telah diedarkan terlebih dahulu. Dengan syarat bahawa Jawatankuasa boleh, jika difikirkannya patut, meminda susunan perkara-perkara yang telah dimasukkan dalam agenda.
4. Apa-apa perkara yang tidak ada dalam agenda bagi sesuatu mesyuarat boleh, jika difikirkan patut oleh Jawatankuasa, ditimbang dan diputuskan oleh Jawatankuasa pada mesyuarat itu di bawah "Hal-hal lain".
5. Jika sesuatu mesyuarat ditamatkan sebelum menyelesaikan kesemua perkara dalam agenda bagi mesyuarat itu, maka perkara yang belum selesai itu bolehlah diselesaikan dalam agenda bagi mesyuarat yang berikutnya:
   Dengan syarat bahawa jika dipersetujui oleh semua ahli yang hadir, sesuatu mesyuarat boleh ditangguhkan

untuk disambung semula pada tarikh dan masa yang ditetapkan oleh Jawatankuasa.

6. Sesuatu usul yang pada pendapat Urus Setia memerlukan keputusan segera boleh dikemukakan untuk keputusan jawatankuasa menerusi surat edaran kepada ahli-ahli Jawatankuasa dan dalam hal demikian tiap-tiap ahli hendaklah diberi masa sekurang-kurangnya tiga (3) hari untuk menyatakan pendapatnya atas usul itu.
7. Sesuatu usul yang dikemukakan secara edaran hendaklah diputuskan mengikut persetujuan sebulat suara semua ahli yang memberi jawapan kepada Setiausaha dalam masa yang diberikan menurut sub perenggan 6: Dengan syarat bahawa bilangan ahli yang memberi jawapan itu hendaklah tidak kurang daripada bilangan yang diperlukan untuk mengadakan kuorum.
8. Jika pada akhir masa yang diberikan menurut sub perenggan 7 itu didapati bahawa:
   (1) Terdapat sekurang-kurangnya dua (2) orang ahli yang memberi jawapan menyatakan mereka tidak bersetuju dengan usul yang dikemukakan secara edaran itu, maka usul itu hendaklah dibentangkan dalam suatu mesyuarat yang berikutnya.
   (2) Bagi seseorang ahli yang tidak memberi jawapan dalam masa yang ditetapkan, jawapan tersebut akan dinyatakan sebagai bersetuju dengan usul yang dikemukakan secara edaran itu.
9. Tiap-tiap keputusan yang dibuat secara edaran hendaklah dilaporkan kepada Jawatankuasa dalam mesyuarat yang berikutnya untuk makluman.

Minit dan Laporan :

1. Minit-minit bagi sesuatu mesyuarat Jawatankuasa hendaklah diedarkan dan laporan kepada ahli-ahli Jawatankuasa dalam masa sepuluh (10) hari bekerja selepas mesyuarat itu diadakan.
2. Cadangan-cadangan bagi meminda sesuatu minit hendaklah disampaikan kepada Urus Setia dalam masa sepuluh (10) hari bekerja selepas minit itu diedarkan kepada ahli-ahli. Jika tiada apa-apa cadangan diterima oleh Urus Setia dalam tempoh itu, maka minit itu sebagaimana yang disediakan oleh Urus Setia hendaklah dianggap betul dan tindakan-tindakan berasaskan kepadanya boleh diambil.
3. Minit-minit bagi sesuatu mesyuarat atau mesyuarat khas hendaklah disahkan dalam mesyuarat yang berikutnya.
4. Jika ada apa-apa keraguan mengenai tafsiran sesuatu minit mesyuarat Jawatankuasa maka perkara itu hendaklah diputuskan dengan merujuk kepada apa-apa kertas Jawatankuasa yang telah dibentangkan dalam mesyuarat itu. Jika keraguan itu tidak dapat dijelaskan dengan cara demikian Jawatankuasa hendaklah memutuskan perkara itu sebagaimana yang difikirkan patut oleh Jawatankuasa.

Meminda Peraturan Tatacara Mesyuarat	:	Pindaan kepada tatacara mesyuarat ini boleh diluluskan menerusi ketetapan Jawatankuasa yang dibuat dalam sesuatu mesyuarat Jawatankuasa dengan persetujuan sekurang-kurangnya dua pertiga daripada jumlah ahli Jawatankuasa. Dengan syarat bahawa sesuatu pindaan kepada tatacara mesyuarat ini tidak boleh dikuatkuasa sehingga pindaan itu dibawa untuk kelulusan Pihak Berkuasa yang berkaitan.

Diluluskan oleh:

PROFESOR TS. DR. NOR BADRUL ANUAR BIN JUMA'AT
Ketua Pegawai Digital
Universiti Malaya

Tarikh: 09 Disember 2024

LAMPIRAN B6: TERMA RUJUKAN JAWANKUASA KERJA SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (JK ISMS)

UNIVERSITI MALAYA

Terma Rujukan Jawatankuasa

Nama Jawatankuasa	:	Jawankuasa Kerja Sistem Pengurusan Keselamatan Maklumat (JK ISMS)
Pengenalan	:	Jawatankuasa Kerja Sistem Pengurusan Keselamatan Maklumat (JK ISMS) ialah entiti tunggal yang bertanggungjawab untuk merancang, melaksana, memantau dan bertindak ke atas semua bidang pengurusan keselamatan maklumat di JTM di bawah seliaan Pengarah Eksekutif ICT. Jawatankuasa ini terdiri di kalangan warga JTM yang dilantik tertakluk kepada terma rujukan dan berperanan untuk menggerak, membangun, melaksana dan menyelenggara ISMS.
Punca Kuasa	:	Pengarah Eksekutif JTM melantik ahli jawatankuasa.
Keanggotaan	:	**Pengerusi:** Pegawai Keselamatan ICT (ICTSO) **Ahli:** 1. Wakil Pengurusan Keselamatan Maklumat (ISMR) 2. Pengarah Pusat, JTM 3. Pengawal Dokumen ISMS 4. Pegawai Teknologi Maklumat, JTM **Urus Setia:** Pegawai Seksyen Governan Digital, JTM
Tempoh Keanggotaan	:	Tempoh jawatan adalah selama dua (2) tahun.
Bidang Kuasa Jawatankuasa	:	1. Memantau dan memastikan pelaksanaan ISMS selaras dengan standard ISO/IEC 27001. 2. Membangun, menyelenggara dan melaksanakan penambahbaikan terhadap dokumen-dokumen ISMS, pengurusan dokumentasi dan rekod ISMS, proses dan perkhidmatan.

3. Mengatur dan memantau aktivti tahunan ISMS dan memastikan ia dijalankan mengikut perancangan.
4. Membangunkan metodologi penilaian risiko dan proses *risk treatment plan* serta mengemukakan kepada pihak pengurusan untuk kelulusan.
5. Memantau keberkesanan pelaksanaan ISMS berdasarkan pengukuran pencapaian objektif keselamatan serta kawalan, hasil audit, insiden keselamatan dan maklum balas pihak berkepentingan.
6. Melaksanakan keputusan dan tindakan hasil Mesyuarat Kajian Semula Pengurusan ISMS (MKSP ISMS).
7. Mencadangkan dan/atau melaksanakan peluasan skop ISMS.
8. Berperanan sebagai Pegawai Risiko yang bertanggungjawab bagi perkara berikut:
    a. Mengenal pasti, menilai, mengurus dan memantau risiko bagi bahagian/seksyen.
    b. Merancang, memantau dan memastikan pelan mitigasi yang telah dirancang dapat dilaksanakan dalam tempoh yang ditetapkan.
    c. Memastikan penilaian risiko bahagian/seksyen dikemas kini secara berkala atau jika ada keperluan.

Mesyuarat : Jawatankuasa hendaklah bermesyuarat sekurang-kurangnya **tiga (3) kali setahun**. Pengerusi Jawatankuasa boleh memanggil mesyuarat pada bila-bila masa jika ada keperluan.

Notis Mesyuarat :
1. Notis bagi sesuatu mesyuarat hendaklah disampaikan secara bertulis atau secara elektronik oleh Urusetia kepada ahli-ahli Jawatankuasa selewat-lewatnya tujuh (7) hari sebelum tarikh yang ditetapkan bagi mesyuarat itu atau mengikut keperluan.
2. Notis bagi sesuatu mesyuarat hendaklah menyatakan tempat, tarikh dan masa yang ditetapkan bagi mesyuarat tersebut.

Agenda :
1. Agenda bagi sesuatu mesyuarat serta kertas-kertas yang berkaitan hendaklah disampaikan kepada ahli-ahli Jawatankuasa sekurang-kurangnya tujuh (7) hari sebelum tarikh yang ditetapkan bagi mesyuarat itu atau mengikut

keperluan.

2. Seseorang ahli Jawatankuasa yang hendak memasukkan sesuatu perkara dalam agenda mesyuarat hendaklah memberitahu Urusetia sekurang-kurangnya tiga (3) hari sebelum mesyuarat diadakan.

Kuorum : Mesyuarat perlu dihadiri tidak kurang dari **separuh (1/2) keahlian** jawatankuasa yang dilantik, termasuk Pengerusi.

Perjalanan Mesyuarat :

1. Pengerusi, jika ia hadir, hendaklah mempengerusikan Mesyuarat Jawatankuasa sehingga selesai.
2. Jika Pengerusi tidak hadir pada sesuatu mesyuarat Jawatankuasa atau sebahagian darinya, maka selama ia tidak hadir, mesyuarat hendaklah dipengerusikan oleh mana-mana ahli jawatankuasa yang diarahkan oleh Pengerusi.
3. Perjalanan sesuatu mesyuarat Jawatankuasa hendaklah mengikut agenda mesyuarat yang telah diedarkan terlebih dahulu. Dengan syarat bahawa Jawatankuasa boleh, jika difikirkannya patut, meminda susunan perkara-perkara yang telah dimasukkan dalam agenda.
4. Apa-apa perkara yang tidak ada dalam agenda bagi sesuatu mesyuarat boleh, jika difikirkan patut oleh Jawatankuasa, ditimbang dan diputuskan oleh Jawatankuasa pada mesyuarat itu di bawah "Hal-hal lain".
5. Jika sesuatu mesyuarat ditamatkan sebelum menyelesaikan kesemua perkara dalam agenda bagi mesyuarat itu, maka perkara yang belum selesai itu bolehlah diselesaikan dalam agenda bagi mesyuarat yang berikutnya.

   Dengan syarat bahawa jika dipersetujui oleh semua ahli yang hadir, sesuatu mesyuarat boleh ditangguhkan untuk disambung semula pada tarikh dan masa yang ditetapkan oleh Jawatankuasa.
6. Sesuatu usul yang pada pendapat urus setia memerlukan keputusan segera boleh dikemukakan untuk keputusan jawatankuasa menerusi surat edaran kepada ahli-ahli Jawatankuasa dan dalam hal demikian tiap-tiap ahli hendaklah diberi masa sekurang-kurangnya tiga (3) hari untuk menyatakan pendapatnya atas usul itu.

7. Sesuatu usul yang dikemukakan secara edaran hendaklah diputuskan mengikut persetujuan sebulat suara semua ahli yang memberi jawapan kepada urus setia dalam masa yang diberikan menurut sub perenggan 6. Dengan syarat bahawa bilangan ahli yang memberi jawapan itu hendaklah tidak kurang daripada bilangan yang diperlukan untuk mengadakan kuorum.

8. Jika pada akhir masa yang diberikan menurut sub perenggan 7 itu didapati bahawa:

   (1) Terdapat sekurang-kurangnya dua (2) orang ahli yang memberi jawapan menyatakan mereka tidak bersetuju dengan usul yang dikemukakan secara edaran itu, maka usul itu hendaklah dibentangkan dalam suatu mesyuarat yang berikutnya.

   (2) Bagi seseorang ahli yang tidak memberi jawapan dalam masa yang ditetapkan, jawapan tersebut akan dinyatakan sebagai bersetuju dengan usul yang dikemukakan secara edaran itu.

9. Tiap-tiap keputusan yang dibuat secara edaran hendaklah dilaporkan kepada Jawatankuasa dalam mesyuarat yang berikutnya untuk makluman.

Minit dan Laporan :

1. Minit-minit bagi sesuatu mesyuarat Jawatankuasa hendaklah diedarkan dan laporan kepada ahli-ahli Jawatankuasa dalam masa sepuluh (10) hari bekerja selepas mesyuarat itu diadakan.

2. Cadangan-cadangan bagi meminda sesuatu minit hendaklah disampaikan kepada Urusetia dalam masa sepuluh (10) hari bekerja selepas minit itu diedarkan kepada ahli-ahli. Jika tiada apa-apa cadangan diterima oleh Urusetia dalam tempoh itu, maka minit itu sebagaimana yang disediakan oleh Urusetia hendaklah dianggap betul dan tindakan-tindakan berasaskan kepadanya boleh diambil.

3. Minit-minit bagi sesuatu mesyuarat atau mesyuarat khas hendaklah disahkan dalam mesyuarat yang berikutnya.

4. Jika ada apa-apa keraguan mengenai tafsiran sesuatu minit mesyuarat Jawatankuasa maka perkara itu hendaklah diputuskan dengan merujuk kepada apa-apa kertas Jawatankuasa yang telah dibentangkan dalam mesyuarat itu. Jika keraguan itu tidak dapat dijelaskan dengan cara demikian Jawatankuasa hendaklah memutuskan perkara itu sebagaimana yang difikirkan patut oleh Jawatankuasa.

Meminda Peraturan Tatacara Mesyuarat : Pindaan kepada tatacara mesyuarat ini boleh diluluskan menerusi ketetapan Jawatankuasa yang dibuat dalam sesuatu mesyuarat Jawatankuasa dengan persetujuan sekurang-kurangnya dua pertiga (2/3) daripada jumlah ahli Jawatankuasa.

Dengan syarat bahawa sesuatu pindaan kepada tatacara mesyuarat ini tidak boleh dikuatkuasa sehingga pindaan itu dibawa untuk kelulusan Pihak Berkuasa yang berkaitan.

Diluluskan oleh:

MARINA BINTI MANSOR
Digitally signed by MARINA BINTI MANSOR
Date: 2025.08.18 08:35:45 +08'00'

MARINA BINTI MANSOR
Yang Menjalankan Fungsi Pengarah Eksekutif
Jabatan Teknologi Maklumat
Universiti Malaya