MINIT MESYUARAT JAWATANKUASA KERJA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
MS ISO/IEC 27001:2013 KALI KE-20 (KHAS) SECARA ATAS TALIAN

Tarikh : 30 Mac 2021 (Selasa)

Masa : 9.00 pagi

Platform : Secara atas talian menerusi aplikasi *Zoom Meeting*

Kehadiran : Seperti di **Lampiran A**

Minit	Agenda	Tindakan/ Makluman
20.1	**Aluan Pengerusi** Pengerusi: (a) memulakan mesyuarat dengan mengalu-alukan kehadiran ahli ke Mesyuarat Jawatankuasa Kerja Sistem Pengurusan Keselamatan Maklumat Kali Ke-20 (Khas) secara atas talian melalui Aplikasi *Zoom Meeting.* (b) memaklumkan agenda mesyuarat pada kali ini adalah untuk mengesahkan perubahan/pindaan hasil semakan yang dilaksanakan ke atas: (i) Penyata Pemakaian (SoA) Semakan Mac 2021; (ii) Dokumen Rujukan Pelaksanaan ISMS Semakan Mac 2021; dan (iii) Laporan Penilaian Risiko ISMS Semakan Mac 2021.	**Makluman** **Makluman**
20.2	**Laporan Penyata Pemakaian (Statement of Applicability) & Dokumentasi ISMS** **20.2.1 Laporan Penyata Pemakaian (SoA) Semakan Mac 2021** (a) Mesyuarat mengambil maklum perubahan Penyata Pemakaian (SoA) sebagaimana dalam **Laporan Agenda 2.0** yang dibentang melibatkan perkara berikut:	**Makluman**

Minit	Agenda	Tindakan/ Makluman
	(i) Perubahan nama entiti ISMS iaitu Pusat Strategi dan Perhubungan Korporat (Nama lama: Pejabat Strategi Korporat dan Komunikasi) & Bahagian Governan dan Integriti, Pejabat Naib Canselor (Nama lama: Unit Integriti); (ii) Penambahan entiti baharu ISMS iaitu Pejabat Pengurusan Keselamatan dan Kesihatan Pekerjaaan selaku peneraju baharu bagi Pelan Kesinambungan Perkhidmatan UPM; dan (iii) Perubahan ke atas kaedah kawalan serta pengemaskinian dokumen rujukan ke atas kawalan sedia ada. (b) Mesyuarat bersetuju meluluskan perubahan SoA Semakan Mac 2021 dengan beberapa penambahbaikan sebagaimana yang dinyatakan pada **Lampiran B.** (c) Mesyuarat meminta supaya perubahan SoA ini dikuatkuasakan pemakaiannya bermula 30 Mac 2021 dan dihebahkan kepada semua peneraju/entiti yang terlibat dengan pelaksanaan ISMS UPM. (d) Mesyuarat meminta semua peneraju/entiti ISMS merujuk kepada dokumen terkini melalui eISO UPM semasa pelaksanaan Audit Dalaman ISMS tahun 2021. **20.2.2 Dokumen Rujukan Pelaksanaan ISMS Semakan Mac 2021** (a) Mesyuarat mengambil maklum perubahan Dokumen Rujukan Pelaksanaan ISMS semakan Mac 2021 adalah sebagaimana Laporan **Agenda 2.0** yang dibentang iaitu melibatkan: (i) Perubahan nama Bahagian Governan dan Integriti, Pejabat Naib Canselor (Nama lama: Unit Integriti); (ii) Senarai PTJ terlibat dengan pensijilan ISMS digugurkan dan informasi berkaitan dirujuk terus melalui paparan di Portal eISO UPM;	**Sekretariat Pusat Jaminan Kualiti** **Sekretariat Pusat Jaminan Kualiti** **Ketua Pasukan ISMS** **Makluman**

Minit	Agenda	Tindakan/ Makluman
	(iii) Format penulisan Pihak Berkepentingan dan Keperluan Mereka & Isu Dalaman dan Isu Luaran dipecahkan mengikut pasukan ISMS; dan (iv) Peranan dan tanggungjawab Jawatankuasa ISMS digugurkan dan informasi berkaitan dirujuk terus melalui paparan di Portal eISO UPM. (b) Mesyuarat meneliti dan bersetuju meluluskan perubahan Dokumen Rujukan Pelaksanaan ISMS Semakan Mac 2021 dengan beberapa penambahbaikan sebagaimana yang dinyatakan pada **Lampiran C.** Dokumen ini akan dikuatkuasakan pemakaiannya pada 30 Mac 2021 dan perlu dihebahkan kepada semua peneraju/entiti ISMS di UPM.	**Sekretariat Pusat Jaminan Kualiti**
20.3	**Laporan Penilaian Risiko (RA) & Pelan Pemulihan Risiko (RTP) ISMS** (a) Mesyuarat mengambil maklum mengenai Laporan Penilaian Risiko dan Pelan Pemulihan Risiko Keselamatan Maklumat Tahun 2021 (semakan Mac 2021) setiap pasukan ISMS hasil Bengkel Semakan Penilaian Risiko ISMS yang diadakan pada 9 hingga 10 Mac 2021 adalah sebagaimana laporan **Agenda 3.0** yang dibentang. (b) Mesyuarat mengambil maklum secara keseluruhan laporan menunjukkan terdapat sebanyak 1083 risiko dengan tahap rendah (L) dan 102 risiko dengan tahap sederhana (M) manakala tiada risiko dengan tahap Tinggi (H) dicatatkan hasil daripada penilaian ke atas 776 aset yang terlibat bagi semua pasukan. (c) Mesyuarat turut mengambil maklum Pasukan Pendaftaran Pelajar Baharu Prasiswazah (Kampus Serdang) dan Pasukan Pusat Data mencatatkan penurunan jumlah aset, Pasukan Penilaian Pengajaran Prasiswazah di Fakulti mencatatkan pertambahan jumlah aset manakala jumlah aset bagi Pasukan Pendaftaran Pelajar Baharu Prasiswazah (Kampus Bintulu) tidak berubah. (d) Mesyuarat mengambil perhatian terhadap tindakan kawalan dan pelan pemulihan risiko yang digunakan oleh setiap peneraju ISMS dalam memastikan keberkesanan pelaksanaan Sistem Pengurusan	**Makluman** **Makluman** **Makluman** **Makluman**

Minit	Agenda	Tindakan/ Makluman
	Keselamatan Maklumat di UPM sebagaimana laporan yang dibentangkan. (e) Mesyuarat bersetuju meluluskan Laporan Penilaian Risiko dan Pelan Pemulihan Risiko ISMS (Semakan Mac 2021) untuk digunakan sebagai rujukan terkini semua pasukan ISMS.	**Penyelaras Penilaian Risiko ISMS**
20.4	**Hal-hal Lain** **20.4.1 Penyerahan Fungsi Keselamatan ICT Sektor Awam kepada NACSA** (a) Mesyuarat dimaklumkan mengenai Surat Timbalan Ketua Pengarah ICT MAMPU kepada Ketua Eksekutif Agensi Keselamatan Siber Negara (AKSN/NACSA): Penyerahan Fungsi Keselamatan ICT Sektor Awam kepada NACSA bertarikh 19 Oktober 2020 yang menyatakan MAMPU tidak lagi menjalankan fungsi keselamatan siber sektor awam sebagaimana arahan-arahan yang telah dikeluarkan melalui 12 dasar/pekeliling/penerbitan berkaitan keselamatan ICT termasuklah khidmat perundingan, penguatkuasaan dan penyelenggaraan sistem-sistem aplikasi yang menyokong 12 dasar/pekeliling/penerbitan berkaitan keselamatan ICT sektor awam (termasuk Penilaian Risiko menggunakan Aplikasi MyRAM). (b) Rentetan daripada itu, mesyuarat bersetuju mengambil tindakan berikut: (i) Sebarang permohonan dan pertanyaan berkaitan fungsi keselamatan siber termasuk Sistem MyRAM perlu dimajukan terus kepada pihak NACSA; dan (ii) Menyemak dan membuat pindaan terhadap dokumen ISO/dokumen rujukan ISMS pasukan/Portal eISO UPM (sekiranya kandungan dokumen/portal ada menyatakan pihak MAMPU sebagai peneraju Aplikasi MyRAM).	**Makluman** **Penyelaras Penilaian Risiko ISMS** **Sekretariat Pusat Jaminan Kualiti & Semua Ketua Pasukan ISMS**

Minit	Agenda	Tindakan/ Makluman
	20.4.2 Semakan ke atas Integriti Data Pelajar dalam Sistem Maklumat Pelajar (eSMP) Mesyuarat mengambil maklum berhubung beberapa isu melibatkan integriti data eSMP seperti status pengajian pelajar serta status semester pengajian pelajar yang tidak tepat yang dihadapi oleh pihak UPM Kampus Bintulu. Justeru mesyuarat meminta supaya perkara ini diambil perhatian dan tindakan oleh pihak Pasukan Pendaftaran Pelajar Baharu Prasiswazah bagi memastikan proses pendaftaran pelajar prasiswazah dapat berjalan dengan lancar.	**Ketua Pasukan Pendaftaran Pelajar Baharu Prasiswazah (Kampus Serdang)**
20.5	**Penangguhan Mesyuarat** Mesyuarat ditangguhkan pada jam 1.00 tengahari dengan ucapan terima kasih daripada Pengerusi.	

LAMPIRAN A

SENARAI KEHADIRAN
MESYUARAT JAWATANKUASA KERJA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
MS ISO/IEC 27001:2013 KALI KE-20 (KHAS) SECARA ATAS TALIAN

HADIR

1. Ts. Krishnan Mariappan **- Pengerusi**
2. Puan Haslida Hassan (Penasihat Jawatankuasa Kerja ISMS)
3. Ts. Mohd Faizal Daud (Penasihat Jawatankuasa Kerja ISMS)
4. Encik Rosmi Othman (Penasihat Jawatankuasa Kerja ISMS)
5. Encik Shahriman Hashim (Ketua, Pasukan Pendaftaran Pelajar Baharu Prasiswazah Kampus Serdang)
6. Encik Noor Hakim Ahmad (Ketua, Pasukan Pendaftaran Pelajar Baharu Prasiswazah Kampus Bintulu)
7. Encik Sudirman Asmadi (Timbalan Ketua, Pasukan Pendaftaran Pelajar Baharu Prasiswazah Kampus Bintulu)
8. Ts. Shahril Iskandar Amir (Ketua, Pasukan Pusat Data)
9. Encik Ahmad Nizam Abdullah (Ketua, Pasukan Penilaian Pengajaran Prasiswazah di Fakulti)
10. Encik Wan Hafizi Wan Umar (Penyelaras Penilaian Risiko ISMS)
11. Puan Shamriza Shari **- Setiausaha**

TURUT HADIR

1. Encik Adidi Tamin (Pasukan Pendaftaran Pelajar Baharu Prasiswazah Kampus Serdang)

TIDAK HADIR (DENGAN KENYATAAN)

1. Dato' Haji Rosdi Wah (Penasihat Jawatankuasa Kerja ISMS)
2. Encik Nuruliman Ibrahim (Timbalan Ketua, Pasukan Pendaftaran Pelajar Baharu Prasiswazah Kampus Serdang)
3. Ts. Rostam Abu Bakar (Timbalan Ketua, Pasukan Pusat Data)
4. Puan Yasminani Mohamad (Timbalan Ketua, Pasukan Penilaian Pengajaran Prasiswazah di Fakulti)

	PENYATA PEMAKAIAN **(*STATEMENT OF APPLICABILITY)*** **SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

1.0 PENGENALAN

Dokumen Penyata Pemakaian (*Statement of Applicability (*SoA)) menggariskan objektif kawalan dan kawalan di Annex A dalam Standard MS ISO/IEC 27001:2013 selaras dengan keperluan Sistem Pengurusan Keselamatan Maklumat di Universiti Putra Malaysia.

2.0 TUJUAN

Dokumen ini bertujuan untuk menetapkan proses yang perlu dipatuhi dalam menyediakan SoA.

3.0 PROSES PENYATA PEMAKAIAN *(*SoA)

3.1 PENYEDIAAN SoA

Proses yang terlibat dalam penyediaan SoA merangkumi:

(a) Memahami keperluan SoA dalam Standard MS ISO/IEC 27001:2013.

(b) Menyediakan kandungan SoA dengan mengambil kira aspek berikut:

(i) Menyenaraikan semua objektif kawalan dan kawalan di Annex A dalam Standard MS ISO/IEC 27001:2013;

(ii) Memberi jawapan **"Ya"** dengan justifikasi pemilihan kepada objektif kawalan dan kawalan selaras dengan **penemuan Pelan Pemulihan Risiko***;*

(iii) Memberi jawapan **"Ya"** kepada objektif kawalan dan kawalan **yang sedang dilaksanakan**;

(iv) Memberi jawapan **"Separa"** kepada kawalan yang **masih dalam pembangunan;**

(v) Menyenaraikan **nama prosedur / panduan / dokumen** yang dirujuk bagi menyokong pelaksanaan objektif kawalan dan kawalan tersebut; dan

(vi) Memberi jawapan **"Tidak"** kepada objektif kawalan dan kawalan yang **tidak dipilih** dengan alasan pengecualiannya.

(c) Membentangkan cadangan awal SoA dalam Mesyuarat Jawatankuasa Kerja ISMS.

3.2 PELAKSANAAN SoA

Pelaksanaan SoA hendaklah mengambil kira aspek berikut:

(a) Memaklumkan kepada semua pengguna ISMS berhubung penguatkuasaan dokumen SoA;

(b) Melaksanakan program kesedaran pematuhan semua peraturan Polisi ISMS selaras dengan keperluan SoA;

(c) Memantau tahap pematuhan pelaksanaan kawalan dalam SoA sekurang-kurangnya sekali dalam setahun; dan
(d) Melaporkan penemuan di para c) dalam Mesyuarat Jawatankuasa Kerja ISMS untuk pertimbangan dan kelulusan.

3.3 PENGEMASKINIAN SoA

SoA perlu dikemaskini dengan mengambilkira perkara berikut:

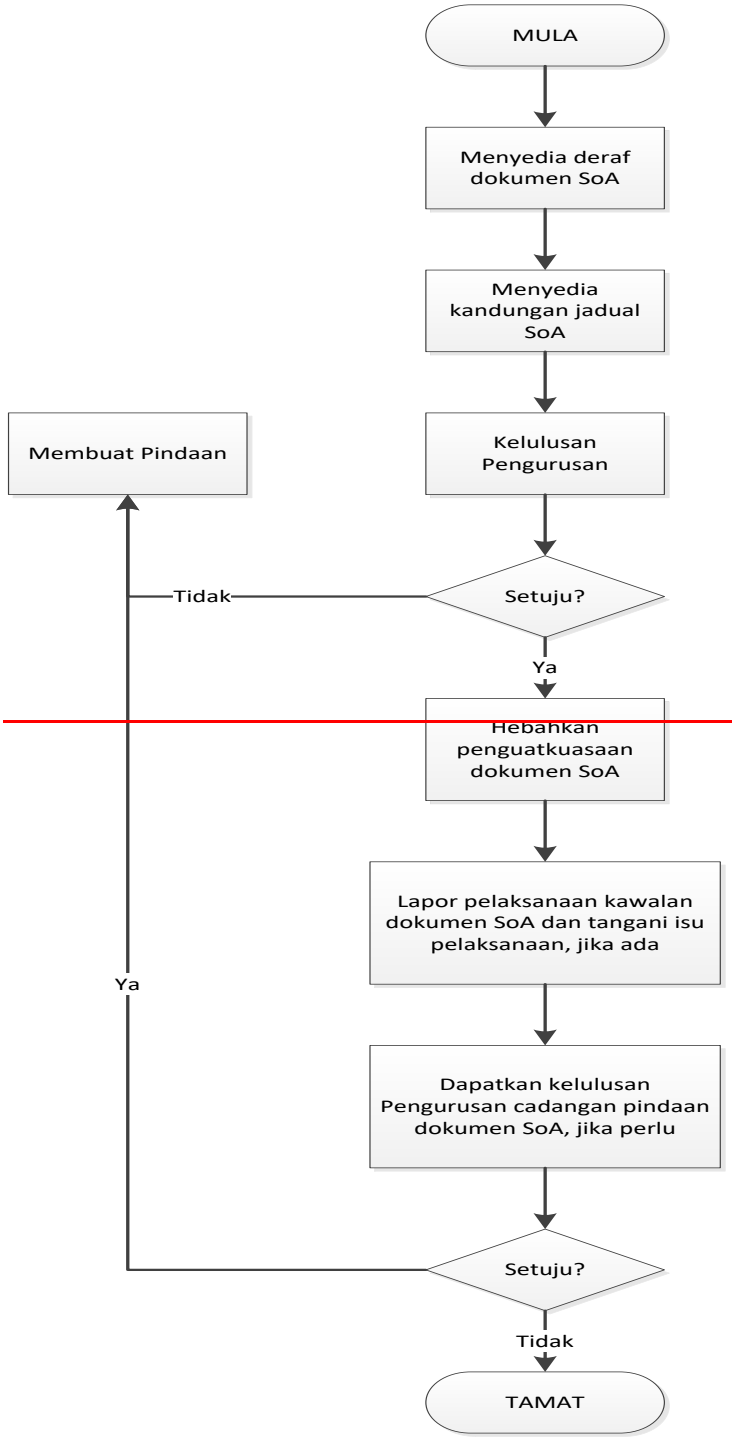
(a) Penemuan penilaian semula risiko;
(b) Perubahan justifikasi pemilihan kawalan;
(c) Perluasan skop ISMS;
(d) Penambahan atau pengecualian aset ISMS;
(e) Perubahan struktur organisasi;
(f) Penambahbaikan ke atas pelaksanaan ISMS;
(g) Pengemaskinian ke atas dokumen rujukan; dan
(h) Perubahan disebabkan oleh keperluan lain.

Sebarang pindaan kepada SoA hendaklah mematuhi perkara yang dinyatakan dalam para 3.1(c) di atas.

4.0 JADUAL PENYATAAN PEMAKAIAN *(SoA)*

SoA di **LAMPIRAN A** menyediakan ringkasan keputusan berkaitan pemulihan risiko (*risk treatment*). Sebarang objektif kawalan dan kawalan yang **tidak dipilih** diberikan alasan pengecualiannya bagi memastikan suatu kawalan tidak sengaja diabaikan.

~~5.0 CARTA ALIRAN~~



PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT

Lampiran A: SoA Pensijilan MS ISO/IEC 27001:2013 ISMS Universiti Putra Malaysia

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
A.5 DASAR KESELAMATAN MAKLUMAT	A.5.1	**Hala tuju pengurusan untuk keselamatan maklumat** Menyediakan hala tuju dan sokongan pengurusan untuk keselamatan maklumat menurut keperluan perniagaan serta undang-undang dan peraturan yang berkaitan.					
	A.5.1.1	**Dasar keselamatan maklumat** Satu set dasar untuk keselamatan maklumat hendaklah ditakrifkan, diluluskan oleh pengurusan, diterbitkan dan disampaikan kepada kakitangan dan pihak luaran yang berkaitan.	Pusat Jaminan Kualiti	YA	YA	Memastikan kawalan keselamatan maklumat dibangunkan dan disahkan oleh Pengurusan Atasan dan disampaikan kepada umum.	• Dasar ISMS UPM - diluluskan oleh Pengerusi Lembaga Pengarah Universiti ~~pada 10 Disember 2019~~ - dikomunikasi menerusi Portal eISO UPM • ~~Dokumen Rujukan Pelaksanaan Sistem Pengurusan Keselamatan Maklumat – DASAR ISMS~~
	A.5.1.2	**Kajian semula dasar untuk keselamatan maklumat** Dasar untuk keselamatan maklumat hendaklah dikaji semula pada sela masa yang dirancang atau jika berlaku perubahan yang ketara bagi memastikan kesesuaian, kecukupan dan keberkesanannya berterusan.	Pusat Jaminan Kualiti	YA	YA	Memastikan dasar sentiasa terkini berdasarkan skop dan pelaksanaan ISMS.	• Semakan berkala dilaksanakan semasa Mesyuarat Kajian Semula Pengurusan ISMS UPM

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
A.6 PERANCANGAN BAGI KESELAMATAN MAKLUMAT	A.6.1	**Perancangan dalaman** Menyediakan rangka kerja pengurusan untuk memulakan dan mengawal pelaksanaan dan operasi keselamatan dalam organisasi.					
	A.6.1.1	**Peranan dan tanggungjawab keselamatan maklumat** Semua tanggungjawab keselamatan maklumat hendaklah ditakrifkan dan diperuntukkan.	Pusat Jaminan Kualiti	YA	YA	Memastikan semua tanggungjawab keselamatan maklumat ditakrifkan dan diperuntukkan.	• ~~Dokumen Rujukan Pelaksanaan Sistem Pengurusan Keselamatan Maklumat - PERANAN DAN TANGGUNGJAWAB~~ • Peranan dan Tanggungjawab Jawatankuasa Keselamatan Maklumat UPM - menerusi Portal eISO UPM
	A.6.1.2	**Pengasingan tugas** Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubah suai, tanpa kebenaran atau dengan tidak sengaja mengubah, atau menyalahgunakan aset organisasi.	Peneraju ISMS & Pejabat Pendaftar	YA	YA	Memastikan tugas dan bidang tugas diasingkan untuk mengurangkan peluang bagi pengubahsuaian atau penyalahgunaan aset organisasi yang tidak dibenarkan atau yang tidak disengajakan.	• Senarai tugas Akademik/Bukan Akademik/Pelaksana ▪ Termasuk tugas pentadbiran. (Contoh: sebagai Dekan, Pengetua Kolej, Pengarah, Penolong Pengarah/Timbalan Pengarah) • Senarai tugas pada setiap pekerja UPM • Struktur organisasi PTJ

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.6.1.3	**Hubungan dengan pihak berkuasa** Hubungan yang baik dengan pihak berkuasa yang berkaitan hendaklah dikekalkan.	Peneraju ISMS	YA	YA	Memastikan hubungan dengan pihak berkuasa berkaitan dikekalkan.	• Akta Universiti dan Kolej Universiti 1971 ~~Pindaan 2012~~ • Akta Perubatan 1971 • Akta Perlesenan Tenaga Atom 1984 (Akta 304) • Seksyen 66 Akta Imigresen 1969/63 (Akta 155) • Perlembagaan Universiti Putra Malaysia (P.U.(A) 448/2010) • *Malaysian Medical Council*
	A.6.1.4	**Hubungan dengan kumpulan berkepentingan yang khusus** Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan persatuan/pertubuhan profesional yang lain hendaklah dikekalkan.	Peneraju ISMS	YA	YA	Memastikan hubungan dengan pihak kepentingan atau lain-lain forum keselamatan dan persatuan profesional dikekalkan.	• Pelan Kesinambungan Perkhidmatan (PKP) • Pelan Komunikasi Krisis • Prosedur Pelan Tindak Balas Insiden ICT (UPM/ISMS/SOK/P001) • Pelan Pemulihan Bencana ICT (Rujukan DRP ICT UPM) • Pengauditan OSHA • MyCert ~~– MAMPU~~ • Cybersecurity Malaysia

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.6.1.5	**Keselamatan maklumat dalam pengurusan projek** Keselamatan maklumat hendaklah ditangani dalam pengurusan projek, tanpa mengambil kira jenis projek.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan keselamatan maklumat dalam pengurusan projek yang terlibat dalam skop pensijilan dikawal.	• Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) • Garis Panduan Pelaksanaan Implementasi Aplikasi (OPR/IDEC/GP07/IMPLEMENTASI APLIKASI)
	A.6.2	**Peranti mudah alih dan telekerja** Memastikan keselamatan telekerja dan penggunaan peranti mudah alih.					
	A.6.2.1	**Dasar peranti mudah alih** Dasar dan langkah-langkah keselamatan sokongan hendaklah digunakan bagi menguruskan risiko yang timbul melalui penggunaan peranti mudah alih.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan polisi dan sokongan kepada pengukuran keselamatan diambil kira bagi mengurus risiko daripada penggunaan peranti mudah alih.	• GPKTMK 6.2.1 Peranti Mudah Alih • Garis Panduan Keselamatan Peralatan Mudah Alih (UPM/ISMS/SOK/ GP05/PERALATAN MUDAH ALIH)
	A.6.2.2	**Telekerja** Dasar dan langkah-langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan di tapak telekerja.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan kawalan capaian kepada sistem (teleworking) oleh pekerja yang dibenarkan sahaja.	• Garis Panduan Pemantauan Capaian ke Sistem (UPM/ISMS/OPR/GP06/ PEMANTAUAN CAPAIAN) ~~Perkara 4.0 Pemantauan Capaian~~ • GPKTMK 6.2.2 *Teleworking* • Arahan Kerja Perkhidmatan Sokongan ICT (OPR/IDEC/AK31/ PERKHIDMATAN

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
							SOKONGAN ICT) Perkara 3.2.1 Rangkaian ~~(4)~~
A.7 KESELAMATAN SUMBER MANUSIA	A.7.1	**Sebelum penjawatan** Memastikan kakitangan dan kontraktor memahami tanggungjawab mereka dan sesuai dengan peranan yang dipertimbangkan untuk mereka.					
	A.7.1.1	**Saringan** Semakan penentusahan latar belakang ke atas semua calon untuk penjawatan hendaklah dilakukan menurut undang-undang, peraturan dan etika yang berkaitan dan hendaklah bersesuaian dengan keperluan perniagaan, klasifikasi maklumat yang hendak diakses dan risiko yang dikenal pasti.	Pejabat Pendaftar	YA	YA	Memastikan semua calon melepasi tapisan keselamatan Kerajaan Malaysia bagi semua calon yang ditawarkan jawatan di UPM.	• Prosedur Pelantikan Staf Tetap Bagi Kumpulan Pengurusan dan Profesional (Bukan Akademik) dan Kumpulan Pelaksana (UPM/SOK/BUM/P001) • GPKTMK 7.0 (a) : Sebelum Perkhidmatan • Surat Tawaran Jawatan Tetap – keperluan tapisan keselamatan KERAJAAN MALAYSIA. Ini dilaksanakan secara dalam talian di http://evetting.cgso.gov.my/ dalam tempoh 30 hari mulai tarikh lapor diri Bukti permohonan tapisan keselamatan kerajaan Malaysia telah dibuat dikemukakan kepada Pejabat Pendaftar semasa melapor diri. • Rekod Kenyataan Perkhidmatan (RKP) bagi calon yang dilantik dari agensi luar

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
							• ~~Borang Butir-Butir Perkhidmatan Yang Lepas Dengan Badan-Badan Awam/Swasta (SOK/BUM/BR03/BUTIR)~~
	A.7.1.2	**Terma dan syarat penjawatan** Persetujuan berkontrak dengan kakitangan dan kontraktor hendaklah menyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat.	Pejabat Pendaftar & Pejabat Bursar	YA	YA	Memastikan kontrak perjanjian terhadap pekerja dan pembekal menyatakan tanggungjawab organisasi terhadap keselamatan maklumat.	• Prosedur Pendaftaran Syarikat dan Pekerja/Individu (UPM/OPR/BUR-BUY/P003) • ~~Garis Panduan Lapor Diri (~~ Surat Aku Janji ~~Pekerja UPM) (UPM/SOK/BUM/GP03/LAPOR DIRI)~~ • Borang Pengesahan Lapor Diri (SOK/BUM/BR03/ BORANGPENGESAHAN) • Borang Perakuan untuk ditandatangani Oleh penjawat Awam Berkenaan Dengan Akta Rahsia Rasmi 1972 (SOK/BUM/BR03/AKTA RAHSIA RASMI)
	A.7.2	**Dalam tempoh penjawatan** Memastikan kakitangan dan kontraktor mengetahui dan memenuhi tanggungjawab keselamatan maklumat mereka.					
	A.7.2.1	**Tanggungjawab pengurusan** Pengurusan hendaklah menghendaki semua	Pejabat Pendaftar & Pejabat Bursar	YA	YA	Memastikan polisi dan prosedur keselamatan maklumat yang telah ditetapkan oleh	• Perintah Am • Peraturan Kewangan • Prosedur Perolehan Universiti (UPM/SOK/KEW-BUY/P016)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
		kakitangan dan kontraktor supaya mengamalkan keselamatan maklumat menurut dasar dan prosedur organisasi yang ditetapkan.				organisasi diikuti oleh pekerja dan pembekal.	• ~~Garis Panduan Lapor Diri (~~Surat Aku Janji ~~Pekerja UPM) (UPM/SOK/BUM/GP03/LAPOR DIRI)~~ • Borang Perakuan untuk Ditandatangani oleh Penjawat Awam Berkenaan Akta Rahsia Rasmi 1972 (SOK/BUM/BR03/AKTA RAHSIA RASMI)
	A.7.2.2	**Kesedaran, pendidikan dan latihan tentang keselamatan maklumat** Semua kakitangan organisasi dan, jika berkaitan, kontraktor hendaklah diberikan kesedaran, pendidikan dan latihan sewajarnya dan menerima maklumat secara tetap tentang dasar dan prosedur organisasi, yang berkaitan dengan fungsi tugas mereka.	Peneraju ISMS (Pasukan pendaftaran Pelajar Baharu Prasiswazah – Kampus Serdang & Pasukan Pusat Data), Pejabat Pendaftar, Pejabat Bursar & Pusat Jaminan Kualiti	YA	YA	Memastikan pekerja, pelajar dan pembekal menerima latihan dan program kesedaran berkaitan dengan polisi organisasi yang berkaitan dengan fungsi kerja masing-masing.	• Prosedur Pengurusan Latihan Pekerja Universiti Putra Malaysia (UPM/SOK/LAT/P001) • GPKTMK Perkara ~~7.0 (b) ii~~ 7.2 (b) Dalam Perkhidmatan • Taklimat Keselamatan Maklumat bagi Pelaksanaan Minggu Perkasa Putra • ISMS – Latihan/Takwim di bawah Pusat Jaminan Kualiti • Surat Aku Janji Pihak Luar

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.7.2.3	**Proses tatatertib** Proses tatatertib yang formal hendaklah diadakan dan disampaikan kepada kakitangan bagi membolehkan tindakan diambil terhadap mereka yang melakukan pelanggaran keselamatan maklumat.	Pejabat Pendaftar & ~~Unit Integriti~~ Bahagian Governan dan Integriti, Pejabat Naib Canselor	YA	YA	Memastikan proses tindakan tatatertib dilaksanakan terhadap pekerja yang telah melanggar peraturan keselamatan maklumat.	• Akta 605 - Akta Badan-badan Berkanun (Tatatertib dan Surcaj) 2000 • Akta Rahsia Rasmi 1972 • Kaedah-Kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian F • Prosedur Pengurusan Mesyuarat Tatatertib Staf (UPM/OPR/PNC-UI/P001)
	A.7.3	**Penamatan dan pertukaran penjawatan** Melindungi kepentingan organisasi sebagai sebahagian daripada proses pertukaran atau penamatan penjawatan.					
	A.7.3.1	**Penamatan atau pertukaran tanggungjawab penjawatan** Tanggungjawab dan tugas keselamatan maklumat yang masih sah selepas penamatan atau pertukaran penjawatan hendaklah ditakrifkan, disampaikan kepada kakitangan dan kontraktor dan dikuatkuasakan.	Pejabat Pendaftar & Pejabat Bursar	YA	YA	Memastikan tanggungjawab keselamatan maklumat terhadap pekerja atau pembekal yang telah tamat perkhidmatan atau berlaku perubahan pekerja hendaklah dikenal pasti dan dikuatkuasakan.	• Perintah –perintah Am Persekutuan Bab A : Peraturan-Peraturan Pegawai Awam (Pelantikan, Kenaikan Pangkat Dan Penamatan Perkhidmatan) ~~2005~~ 2012 • GPKTMK Perkara 7.0 (C) Bertukar Atau Tamat Perkhidmatan • ~~Surat Pelantikan Jawatan Pegawai Kanan dikeluarkan oleh Pejabat Naib Canselor~~ • Borang Nota Serah Tugas (SOK/BUM/BR03/SERAH TUGAS)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
							• Dokumen Perjanjian dengan Pembekal/Kontraktor/Pihak Ketiga
A.8 PENGURUSAN ASET	A.8.1	**Tanggungjawab terhadap aset** Mengenal pasti aset organisasi dan mentakrifkan tanggungjawab perlindungan yang sewajarnya.					
	A.8.1.1	**Inventori aset** Maklumat, lain-lain aset yang dikaitkan dengan maklumat, dan fasiliti pemprosesan maklumat hendaklah dikenal pasti dan inventori aset ini hendaklah disediakan dan disenggarakan.	Peneraju ISMS & Pejabat Bursar	YA	YA	Memastikan aset yang terlibat dengan fasiliti pemprosesan maklumat dikenalpasti dan inventori aset tersebut disedia dan diselenggara.	• ~~•~~ Kaedah-kaedah ~~UPM~~ Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014 Bahagian D – ~~Pengurusan Aset Teknologi Maklumat dan Komunikasi~~ • GPKTMK 3.0 Perkara 8.0 : Pengurusan Aset • Prosedur Pengurusan Aset Alih (UPM/SOK/KEW-AST/P012)
	A.8.1.2	**Pemilikan aset** Aset yang disenggara dalam inventori hendaklah mempunyai pemilik.	Peneraju ISMS & Pejabat Bursar	YA	YA	Memastikan setiap aset yang diselanggara mempunyai pemilik.	• Kaedah-kaedah Universiti Putra Malaysia ~~UPM~~ (Teknologi Maklumat dan Komunikasi) 2014, Bahagian D – ~~Pengurusan Aset Teknologi Maklumat dan Komunikasi~~ • GPKTMK 3.0 Perkara 8.0 : Pengurusan Aset • Prosedur Pengurusan Aset Alih (UPM/SOK/KEW-AST/P012)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.8.1.3	**Penggunaan aset yang dibenarkan** Peraturan penggunaan yang dibenarkan bagi maklumat dan aset yang dikaitkan dengan maklumat dan kemudahan pemprosesan maklumat hendaklah dikenal pasti, didokumenkan dan dilaksanakan.	Peneraju ISMS & Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan peraturan untuk kebolehgunaan maklumat dan aset yang berkaitan dengan kemudahan pemprosesan maklumat dan maklumat itu dikenal pasti, didokumen dan dilaksanakan.	• ~~•~~ Kaedah-Kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian F – ~~Pengurusan Data dan Maklumat~~ • GPKTMK 3.0 Perkara 8.2 Pengelasan dan Pengendalian Maklumat
	A.8.1.4	**Pemulangan aset** Semua kakitangan dan pengguna pihak luar hendaklah memulangkan semua aset organisasi yang berada dalam pemilikannya apabila ditamatkan penjawatan, kontrak atau perjanjian mereka.	Peneraju ISMS, Pejabat Pendaftar & Pejabat Bursar	YA	YA	Memastikan aset organisasi dipulangkan selepas tamat perkhidmatan.	• Perintah –perintah Am Persekutuan Bab A : Peraturan-Peraturan Pegawai Awam (Pelantikan, Kenaikan Pangkat Dan Penamatan Perkhidmatan) ~~2005~~ 2012 • Prosedur Pengurusan Aset Alih (UPM/SOK/KEW-AST/P012) • Pekerja : Borang Nota Serah Tugas (SOK/BUM/BR03/SERAH TUGAS) • Dokumen Kontrak Perolehan Pembekal/Pihak Ketiga • Surat Pertukaran (pekerja tidak lagi boleh mengakses sistem di PTJ lama)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.8.2	**Pengelasan maklumat** Memastikan maklumat mendapat tahap perlindungan yang sesuai menurut kepentingannya kepada organisasi.					
	A.8.2.1	**Pengelasan maklumat** Maklumat hendaklah dikelaskan berdasarkan keperluan undang-undang, nilai, tahap kritikal dan sensitiviti terhadap pendedahan atau pengubahsuaian yang tidak dibenarkan.	Peneraju ISMS & Pejabat Pendaftar	YA	YA	Memastikan maklumat dikelaskan untuk mengelak daripada pendedahan atau pengubahsuaian yang tidak dibenarkan.	• Arahan Keselamatan Kerajaan Malaysia • Akta Arkib Negara 2003 (Akta 629) • GPKTMK 3.0 Perkara 8.2 Pengkelasan dan Pengendalian Maklumat • Garis Panduan Pengendalian Maklumat (UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT)
	A.8.2.2	**Pelabelan maklumat** Set prosedur yang sesuai untuk pelabelan maklumat hendaklah dibangunkan dan dilaksanakan menurut skim pengelasan maklumat yang diterima pakai oleh organisasi.	Peneraju ISMS & Pejabat Pendaftar	YA	YA	Memastikan prosedur untuk pelabelan maklumat dibangunkan mengikut skema klasifikasi maklumat oleh organisasi.	• Arahan Keselamatan Kerajaan Malaysia • Akta Arkib Negara 2003 (Akta 629): (m/s : 28) Bahagian V: Pentadbiran Arkib-Pemprosesan dan pemeliharaan arkib awam. • GPKTMK 3.0 Perkara 8.2 Pengkelasan dan Pengendalian Maklumat • Garis Panduan Pengendalian Maklumat (UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.8.2.3	**Pengendalian aset** Prosedur pengendalian aset hendaklah dibangunkan dan dilaksanakan menurut skim pengelasan maklumat yang diterima pakai oleh organisasi.	Peneraju ISMS	YA	YA	Memastikan prosedur pengendalian aset dibangun dan dilaksanakan mengikut skema klasifikasi maklumat oleh organisasi.	• Kaedah-kaedah ~~UPM~~ Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian D – ~~Pengurusan Aset Teknologi Maklumat dan Komunikasi~~ • GPKTMK 3.0 Perkara 8.0 Pengurusan Aset • Prosedur Pengurusan Aset Alih (UPM/SOK/KEW-AST/P012) • Garis Panduan Pengendalian Maklumat (UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT)
	A.8.3	**Pengendalian media** Mencegah pendedahan, pengubahsuaian, penyingkiran, atau pemusnahan tanpa kebenaran terhadap maklumat yang disimpan dalam media.					
	A.8.3.1	**Pengurusan media boleh alih** Prosedur hendaklah dilaksanakan bagi pengurusan media boleh alih menurut skim pengelasan maklumat yang diterima pakai oleh organisasi.	Peneraju ISMS	YA	YA	Memastikan prosedur bersesuaian dibangunkan mengikut klasifikasi yang digunakan oleh organisasi.	• Tatacara Pengurusan Aset Alih Kerajaan : pelupusan • GPKTMK 3.0 Perkara 8.3 : Pengendalian media • Garis Panduan Pengendalian Maklumat (UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.8.3.2	**Pelupusan media** Media hendaklah dilupuskan dengan selamat melalui prosedur formal apabila tidak diperlukan lagi.	Peneraju ISMS	YA	YA	Media yang tidak lagi diperlukan perlu dilupuskan menggunakan prosedur yang dibangunkan.	• Tatacara Pengurusan Aset Alih Kerajaan : pelupusan • GPKTMK 3.0 Perkara 8.3 : Pengendalian media • Arahan Kerja Pelupusan Pita *Backup* (UPM/ISMS/OPR/AK07) • Garis Panduan Pelupusan Aset Alih (UPM/SOK/KEW/GP020/AST)
	A.8.3.3	**Pemindahan media fizikal** Media yang mengandungi maklumat hendaklah dilindungi daripada akses tanpa izin, penyalahgunaan atau kerosakan semasa pengangkutan.	Peneraju ISMS	YA	YA	Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa perpindahan.	• GPKTMK 3.0 Perkara 8.3 – Pengendalian Media • Garis Panduan Pengendalian Maklumat (UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
A.9 KAWALAN AKSES	A.9.1	**Kawalan akses bagi keperluan perniagaan** Mengehadkan akses kepada maklumat dan kemudahan pemprosesan maklumat.					
	A.9.1.1	**Dasar kawalan akses** Dasar kawalan akses hendaklah diwujudkan, didokumenkan dan dikaji semula berdasarkan keperluan perniagaan dan keperluan keselamatan maklumat.	Peneraju ISMS	YA	YA	Dasar kawalan capaian hendaklah diwujud , didokumen dan dikaji semula berdasarkan keperluan keselamatan perniagaan dan maklumat.	• Arahan Keselamatan : Keselamatan Fizikal • GPKTMK 3.0 Perkara 9.1 : Dasar Kawalan Akses • Garis Panduan Kawalan Akses Ke Pusat Data (UPM/ISMS/OPR/GP03/KAWALAN AKSES) • Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/GP06/ PEMANTAUAN CAPAIAN)
	A.9.1.2	**Akses kepada rangkaian dan perkhidmatan rangkaian** Pengguna hanya hendaklah diberikan akses kepada rangkaian dan perkhidmatan rangkaian yang dibenarkan secara khusus.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan pengguna mempunyai akses kepada perkhidmatan rangkaian yang telah dikhususkan kepada mereka.	• GPKTMK 3.0 Perkara 13.2 : Kawalan Akses Rangkaian • Garis Panduan Pengurusan Pengagihan Rangkaian (UPM/ISMS/OPR/GP13/AGIHAN RANGKAIAN)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.9.2	**Pengurusan akses pengguna** Memastikan akses oleh pengguna yang dibenarkan dan menghalang akses tanpa izin kepada sistem dan perkhidmatan.					
	A.9.2.1	**Pendaftaran dan pembatalan pengguna** Proses formal pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan pemberian hak akses.	Peneraju ISMS	YA	YA	Memastikan proses pendaftaran dan pembatalan pengguna dilaksanakan untuk membolehkan pemberian hak akses.	• GPKTMK 3.0 Perkara 9.2 : Pengurusan Capaian Pengguna • Prosedur Kawalan dan Pemantauan Capaian ke Sistem di Pusat Data (UPM/ISMS/OPR/P003) • Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE/AK01) • Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/ GP06/PEMANTAUAN CAPAIAN) • Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI) • Garis Panduan Pengurusan Identiti Pengguna (ID) Sistem Maklumat Pelajar (PU/PS/GP010/SMP-ID) • Garis Panduan Pengurusan Identiti Pengguna Id eKlinik (OPR/PKU/GP13/EKLINIK-ID) • Buku Panduan Perkhidmatan Perubatan Pusat Kesihatan Universiti

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.9.2.2	**Peruntukan akses pengguna** Proses formal peruntukan akses pengguna hendaklah dilaksanakan dalam pemberian atau pembatalan hak akses kepada semua jenis pengguna untuk semua sistem dan perkhidmatan.	Peneraju ISMS	YA	YA	Memastikan penetapan dan pembatalan hak akses untuk semua jenis pengguna dilaksanakan.	• GPKTMK 3.0 Perkara 9.2 : Pengurusan Capaian Pengguna • Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/GP06/ PEMANTAUAN CAPAIAN) • Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI) • Garis Panduan Pengurusan Identiti Pengguna (ID) Sistem Maklumat Pelajar (PU/PS/GP010/SMP-ID) • Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE/AK01) • Garis Panduan Pengurusan Identiti Pengguna Id eKlinik (OPR/PKU/GP13/EKLINIK-ID) • Buku Panduan Perkhidmatan Perubatan Pusat Kesihatan Universiti
	A.9.2.3	**Pengurusan hak akses istimewa** Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan dan dikawal.	Peneraju ISMS	YA	YA	Memastikan kebenaran hak akses dihadkan dan dikawal.	• GPKTMK 3.0 Perkara 9.2 : Pengurusan Capaian Pengguna • Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/GP06/ PEMANTAUAN CAPAIAN)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
							• Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI) • Garis Panduan Pengurusan Identiti Pengguna (ID) Sistem Maklumat Pelajar (PU/PS/GP010/SMP-ID) • Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE/AK01) • Garis Panduan Pengurusan Identiti Pengguna Id eKlinik (OPR/PKU/GP13/EKLINIK-ID) • Buku Panduan Perkhidmatan Perubatan Pusat Kesihatan Universiti
	A.9.2.4	**Pengurusan maklumat pengesahan rahsia pengguna** Peruntukan maklumat pengesahan rahsia hendaklah dikawal melalui proses pengurusan formal.	Peneraju ISMS, Pejabat Pendaftar & Bahagian Kemasukan dan Bahagian Urus Tadbir Akademik	YA	YA	Memastikan pengesahan maklumat rahsia sentiasa dikawal.	• GPKTMK 3.0 Perkara 10.0 : Kawalan Kriptografi • Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE/AK01) • Garis Panduan Pengurusan UPM-ID (UPM/ISMS/OPR/GP16/UPM-ID) • Kelulusan Ketua Bahagian Pengurusan Sumber Manusia bagi permohonan baru/ kemaskini bagi perolehan ID eIHRAMS. ~~Penamatan ID bagi pekerja yang bertukar/berhenti/tiada peranan~~

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
							~~dilaksanakan dalam tempoh 14 hari bekerja.~~ • Garis Panduan Pengurusan UPM-ID (UPM/ISMS/OPR/GP16/UPM-ID)) - Perkara 2.0.8 Nyahaktif Akaun UPM-ID
	A.9.2.5	**Kajian semula hak akses pengguna** Pemilik aset hendaklah mengkaji semula hak akses pengguna pada sela masa tetap.	Peneraju ISMS, Pejabat Bursar & Pejabat Pendaftar	YA	YA	Memastikan hak capaian pengguna disemak semula.	• Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE/AK01) • Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR /GP06/PEMANTAUAN CAPAIAN) • Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI) • Garis Panduan Pengurusan Identiti Pengguna (ID) Sistem Maklumat Pelajar (PU/PS/GP010/SMP-ID) • Garis Panduan Pengurusan Identiti Pengguna Id eKlinik (OPR/PKU/GP13/EKLINIK-ID) • Semakan semula ID pengguna eIHRAMS dilaksanakan setahun sekali • Buku Panduan Perkhidmatan Perubatan Pusat Kesihatan Universiti

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.9.2.6	**Penyingkiran atau pelarasan hak akses** Hak akses semua kakitangan dan pengguna pihak luar kepada maklumat dan kemudahan pemprosesan maklumat hendaklah disingkirkan apabila ditamatkan penjawatan, kontrak atau perjanjian, atau diselaraskan apabila terdapat perubahan.	Peneraju ISMS	YA	YA	Memastikan hak akses kepada maklumat dan kemudahan dikeluarkan selepas tamat perkhidmatan atau apabila berlaku perubahan.	• GPKTMK 3.0 Perkara 9.2 : Pengurusan Capaian Pengguna • Prosedur Kawalan dan Pemantauan Capaian ke Sistem di Pusat Data (UPM/ISMS/OPR/P003) • Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE/AK01) • Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/GP06/ PEMANTAUAN CAPAIAN) • Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI) • Garis Panduan Pengurusan Identiti Pengguna (ID) Sistem Maklumat Pelajar (PU/PS/GP010/SMP-ID)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.9.3	**Tanggungjawab pengguna** Memastikan pengguna bertanggungjawab melindungi maklumat pengesahan mereka.					
	A.9.3.1	**Penggunaan maklumat pengesahan rahsia** Pengguna dikehendaki mematuhi amalan organisasi dalam menggunakan maklumat pengesahan rahsia.	Peneraju ISMS (Pasukan Pusat Data & Pasukan Penilaian Pengajaran Prasiswazah di Fakulti)	YA	YA	Memastikan pengguna mengikut semua amalan yang telah ditetapkan dalam pengesahan maklumat.	• GPKTMK 3.0 Perkara 10.0 : Kawalan Kriptografi • Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI) • Garis Panduan Pengurusan UPM-ID (UPM/ISMS/OPR/GP16/UPM-ID) • Surat Aku Janji
	A.9.4	**Kawalan akses sistem dan aplikasi** Menghalang akses tanpa izin kepada sistem dan aplikasi.					
	A.9.4.1	**Sekatan akses maklumat** Akses kepada maklumat dan fungsi sistem aplikasi hendaklah dihadkan menurut dasar kawalan akses.	Peneraju ISMS	YA	YA	Memastikan akses kepada maklumat dan sistem aplikasi dihadkan mengikut prosedur kawalan akses.	• GPKTMK 3.0 Perkara 9.1 : Dasar Kawalan Capaian • Prosedur Kawalan dan Pemantauan Capaian ke Sistem di Pusat Data (UPM/ISMS/OPR/P003) • Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE/AK01) • Garis Panduan Kawalan Akses Ke Pusat Data (UPM/ISMS/OPR/GP03/KAWALAN AKSES)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
							• Garis Panduan Pemantauan Capaian Ke Sistem UPM/ISMS/OPR/GP06/PEMANTAUAN CAPAIAN) • Garis Panduan Pengendalian Maklumat (UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT) • Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI) • Garis Panduan Pengurusan Identiti Pengguna (ID) Sistem Maklumat Pelajar (PU/PS/GP010/SMP-ID) • Garis Panduan Pengurusan Identiti Pengguna Id eKlinik (OPR/PKU/GP13/EKLINIK-ID)
	A.9.4.2	**Prosedur log masuk yang selamat** Jika dikehendaki oleh dasar kawalan akses, akses kepada sistem dan aplikasi hendaklah dikawal oleh prosedur log masuk yang selamat.	Pusat Pembangunan Maklumat dan Komunikasi & Pusat Pembangunan Akademik	YA	YA	Memastikan akses kepada sistem dan aplikasi dikawal menggunakan prosedur bersesuaian.	• GPKTMK 3.0 Perkara 9.0 : Kawalan Akses • Prosedur Kawalan dan Pemantauan Capaian ke Sistem di Pusat Data (UPM/ISMS/OPR/P003) • Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE/AK01)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
							• Garis Panduan Pengurusan UPM-ID (UPM/ISMS/OPR/GP16/UPM-ID)
	A.9.4.3	**Sistem pengurusan kata laluan** Sistem pengurusan katalaluan hendaklah interaktif dan memastikan kata laluan yang berkualiti.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan sistem pengurusan kata laluan adalah interaktif dan kata laluan berkualiti.	• GPKTMK 3.0 9.2 : Pengurusan Capaian Pengguna • Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI) • Garis Panduan Pengurusan Identiti Pengguna (ID) Sistem Maklumt Pelajar (PU/PS/GP010/SMP-ID) • Garis Panduan Pengurusan UPM-ID (UPM/ISMS/OPR/GP16/ UPM-ID)
	A.9.4.4	**Penggunaan program utiliti yang mempunyai hak istimewa** Penggunaan program utiliti yang mungkin mampu melepasi kawalan sistem dan aplikasi hendaklah disekat dan dikawal dengan ketat.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan utiliti program yang boleh mengganggu sistem aplikasi perlu dihad dan dikawal.	• GPTMK 12.2 :Perisian Berbahaya • Prosedur Kawalan dan Pemantauan Capaian ke Sistem di Pusat Data (UPM/ISMS/OPR/P003) • Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/GP06/PEMANTAUAN CAPAIAN)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.9.4.5	**Kawalan akses kepada kod sumber program** Akses kepada kod sumber program hendaklah dihadkan.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan akses kepada program kod sumber perlu dihadkan.	• GPKTMK 9.4 : Keselamatan Fail Sistem • Garis Panduan Perlaksanaan Pengaturcaraan Sistem Aplikasi (OPR/iDEC/GP06/Pengaturcaraan Aplikasi)
A.10 KRIPTOGRAFI	A.10.1	**Kawalan kriptografi** Memastikan penggunaan kriptografi yang betul dan berkesan bagi melindungi kerahsiaan, kesahihan dan/atau integriti maklumat.					
	A.10.1.1	**Dasar penggunaan kawalan kriptografi** Dasar penggunaan kawalan kriptografi bagi melindungi maklumat hendaklah dibangunkan dan dilaksanakan.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan polisi penggunaan kawalan kriptografi untuk perlindungan maklumat dibangun dan dilaksanakan.	• Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi ~~2014~~) 2014, Bahagian G , ~~Bahagian Kawalan Keselamatan TMK~~ Klausa 21(a) • GPKTMK 10.0 : ~~Kawalan~~ Kriptografi • Garis Panduan Pengendalian Maklumat (UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT) Perkara 5.2.1.1

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.10.1.2	**Pengurusan kekunci** Dasar penggunaan, perlindungan dan tempoh hayat kekunci kriptografi hendaklah dibangunkan dan dilaksanakan sepanjang kitar hayatnya.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan polisi penggunaan, perlindungan dan jangka hayat kunci kriptografi dibangun dan dilaksanakan.	• Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan komunikasi ~~2014~~) 2014, Bahagian G , ~~Bahagian Kawalan Keselamatan TMK~~ Klausa 21(c) • GPKTMK 10.0 (c) : Pengurusan *Public Key Infrastructure* (PKI) • Garis Panduan Pengendalian Maklumat (UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT) Perkara 5.2.1.2
A.11 KESELAMATAN FIZIKAL DAN PERSEKITARAN	A.11.1	**Kawasan selamat** Menghalang akses fizikal tanpa kebenaran, kerosakan dan gangguan terhadap maklumat dan kemudahan pemprosesan maklumat organisasi.					
	A.11.1.1	**Perimeter keselamatan fizikal** Perimeter keselamatan hendaklah ditakrifkan dan digunakan bagi melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat yang sensitif atau kritikal.	Peneraju ISMS	YA	YA	Memastikan perimeter keselamatan ditentukan dan digunakan untuk melindungi kawasan yang mengandungi maklumat yang sensitif atau kritikal.	• Arahan Keselamatan : Keselamatan Fizikal • ~~Dokumen Rujukan Pelaksanaan Sistem Pengurusan Keselamatan Maklumat - Lokasi Skop Pensijilan ISMS UPM~~ • Lokasi Skop Pensijilan ISMS UPM - menerusi Portal eISO UPM • GPKTMK 11.1 (a) : Keselamatan Fizikal Kawasan • GPKTMK 11.1(c) – Kawasan Larangan

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.11.1.2	**Kawalan kemasukan fizikal** Kawasan selamat hendaklah dilindungi oleh kawalan kemasukan yang sesuai bagi memastikan kakitangan yang diberi kebenaran sahaja dibenarkan masuk.	Peneraju ISMS	YA	YA	Memastikan kawalan bersesuaian dilaksanakan bagi memastikan hanya pengguna yang diberi hak akses sahaja dibenarkan masuk ke dalam kawasan terkawal.	• Arahan Keselamatan : Keselamatan Fizikal • GPKTMK 11.1(b) Kawalan Masuk Fizikal • ~~Dokumen Rujukan Pelaksanaan Sistem Pengurusan Keselamatan Maklumat - Lokasi Skop Pensijilan ISMS UPM~~ • Lokasi Skop Pensijilan ISMS UPM - menerusi Portal eISO UPM • Prosedur Kawalan Akses (UPM/OPR/BKU/P001) • Prosedur Pengoperasian Pengurusan Pusat Data (UPM/ISMS/OPR/P001) - ~~Perkara 6.2~~ Kawalan Akses ke Pusat Data • Garis Panduan Kawalan Akses ke Pusat Data (UPM/ISMS/OPR/GP03/KAWALAN AKSES)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.11.1.3	**Keselamatan pejabat, bilik dan kemudahan** Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah direka bentuk dan dilaksanakan.	Peneraju ISMS	YA	YA	Memastikan keselamatan fizikal direka dan digunakan.	• Arahan Keselamatan : Keselamatan Fizikal • GPKTMK 11.1 (d) – Keselamatan Pejabat, Bilik dan Kemudahan • ~~Dokumen Rujukan Pelaksanaan Sistem Pengurusan Keselamatan Maklumat - Lokasi Skop Pensijilan ISMS UPM~~ • Lokasi Skop Pensijilan ISMS UPM - menerusi Portal eISO UPM
	A.11.1.4	**Perlindungan daripada ancaman luar dan persekitaran** Perlindungan fizikal daripada bencana alam, serangan hasad atau kemalangan hendaklah direka bentuk dan dilaksanakan.	Peneraju ISMS	YA	YA	Memastikan perlindungan fizikal dibangun dan digunakan.	• Akta Keselamatan dan Kesihatan Pekerjaan 1994 (AKTA 514) • Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi ~~2014~~) 2014, ~~Bhgn~~ Bahagian D, Klausa 9 (b) • GPKTMK 3.0 Perkara 11.1 (e) : Kawalan Persekitaran
	A.11.1.5	**Bekerja di kawasan selamat** Prosedur bekerja di kawasan selamat	Peneraju ISMS	YA	YA	Memastikan prosedur bagi memastikan keselamatan tempat kerja dibangun dan dilaksanakan.	• Akta Keselamatan dan Kesihatan Pekerjaan 1994 (AKTA 514) • GPKTMK 3.0 Perkara 11.1 (f) : Bekerja dalam Kawasan Keselamatan

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
		hendaklah direka bentuk dan dilaksanakan.					
	A.11.1.6	**Kawasan penyerahan dan pemunggahan** Akses keluar masuk seperti kawasan penyerahan dan pemunggahan serta akses lain yang membolehkan mereka yang tidak dibenarkan melaluinya untuk memasuki premis hendaklah dikawal, dan jika boleh, diasingkan daripada kemudahan pemprosesan maklumat bagi mengelakkan akses tanpa kebenaran.	~~Pasukan Pusat Data~~ Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan kawasan penghantaran dan pemunggahan perlu dikawal, jika perlu diasingkan daripada fasiliti pemprosesan maklumat bagi mengelakkan akses yang tidak dibenarkan.	• Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi ~~2014~~) 2014, ~~Bhgn~~ Bahagian D, Klausa 9 (b) • GPKTMK Perkara 11.1 (g) : Kawasan Penghantaran dan Pemunggahan

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.11.2	**Peralatan** Untuk mengelakkan kehilangan, kerosakan, kecurian atau penjejasan aset dan gangguan terhadap operasi organisasi.					
	A.11.2.1	**Penempatan dan perlindungan peralatan** Peralatan hendaklah ditentukan penempatannya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran, dan peluang akses tanpa kebenaran.	Peneraju ISMS	YA	YA	Memastikan peralatan diletakkan ditempat yang dilindungi untuk mengurangkan risiko bahaya dan peluang akses yang tidak dibenarkan.	• Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi ~~2014~~) 2014, ~~Bhgn~~ Bahagian D, Klausa 9 (b) • GPKTMK Perkara 11.3 : Keselamatan Peralatan
	A.11.2.2	**Utiliti sokongan** Peralatan hendaklah dilindungi daripada kegagalan bekalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan.	Peneraju ISMS	YA	YA	Memastikan peralatan dilindungi daripada kegagalan bekalan kuasa dan gangguan yang disebabkan oleh kegagalan utiliti sokongan.	• GPKTMK 3.0 Perkara 11.1 (h) : Perkhidmatan Sokongan • Prosedur Penyelenggaraan Berkala (UPM/SOK/PYG/P002) • Garis Panduan Penyelenggaraan Operasi Pusat Data (UPM/ISMS/OPR/GP01/ PENYELENGGARAAN OPERASI)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.11.2.3	**Keselamatan kabel** Kabel bekalan kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan kabel bekalan kuasa dan telekomunikasi dilindungi daripada pemintasan, gangguan atau kerosakan.	• GPKTMK 3.0 Perkara 11.1 (i) : Keselamatan Kabel • ~~Garis Panduan Pengurusan Sistem Pengkabelan (UPM/ISMS/OPR /GP12/PEMASANGAN KABEL)~~
	A.11.2.4	**Penyenggaraan peralatan** Peralatan hendaklah disenggara dengan betul bagi memastikan ketersediaan dan integriti yang berterusan.	Peneraju ISMS	YA	YA	Memastikan peralatan diselenggara.	• Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan komunikasi ~~2014~~) 2014, ~~Bhgn~~ Bahagian D, Klausa 10 • GPKTMK 3.0 Perkara 11.3 (e) : Penyelenggaraan Peralatan • Prosedur Perkhidmatan ICT (UPM/OPR/IDEC/P002) • Prosedur Penyelenggaraan ICT (UPM/OPR/IDEC/P003) • Perjanjian Kontrak Perkhidmatan Penyelenggaraan • Manual Pelaksanaan Program Jaminan Kualiti (QAP) Dalam Perkhidmatan Radiologi Perkara 4.2

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.11.2.5	**Pengalihan aset** Peralatan, maklumat atau perisian tidak boleh dibawa keluar dari premis tanpa mendapat kebenaran terlebih dahulu.	Peneraju ISMS & Pejabat Bursar	YA	YA	Memastikan peralatan, maklumat atau perisian tidak di bawa keluar dari lokasi tanpa kebenaran.	• GPKTMK Perkara 11.3 (f) : Peralatan di Luar Premis • Prosedur Pengurusan Aset Alih (UPM/SOK/KEW-AST/P012) • ~~Prosedur Perkhidmatan ICT (UPM/OPR/IDEC/P002)~~
	A.11.2.6	**Keselamatan peralatan dan aset di luar premis** Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis organisasi.	Peneraju ISMS & Pejabat Bursar	YA	YA	Memastikan keselamatan dan risiko setiap aset yang berada dilokasi luar diambil kira.	• GPKTMK Perkara 11.3 (f) : Peralatan Di Luar Premis Prosedur Pengurusan Aset Alih (UPM/SOK/KEW-AST/P012) • ~~Prosedur Perkhidmatan ICT (UPM/OPR/IDEC/P002)~~
	A.11.2.7	**Pelupusan yang selamat atau penggunaan semula peralatan** Semua bahagian peralatan yang mengandungi media penyimpanan hendaklah disahkan bagi memastikan sebarang data yang sensitif dan perisian berlesen telah dikeluarkan atau berjaya ditulis ganti sebelum	Peneraju ISMS	YA	YA	Memastikan aset yang terlibat dengan storan media perlu disemak dan data sensitif di buang sebelum diguna semula atau dimusnahkan.	• Pekeliling Perbendaharaan Bil 5/2007 : Bab E : Pelupusan (m/s : 36) • Pekeliling Bendahari Bil 1 2008 : Bahagian E Pelupusan • GPKTMK 11.3 (g) : Pelupusan Peralatan • Prosedur Pengurusan Aset Alih (UPM/SOK/KEW-AST/P012)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
		dilupuskan atau diguna semula.					
	A.11.2.8	**Peralatan pengguna tanpa jagaan** Pengguna hendaklah memastikan peralatan yang dibiarkan tanpa jagaan mempunyai perlindungan sewajarnya.	Peneraju ISMS	YA	YA	Memastikan peralatan yang ditinggalkan di kawal dengan dengan sempurna.	• GPKTMK Perkara 11.3 (h) : Peralatan Ditinggalkan Pengguna
	A.11.2.9	**Dasar meja bersih dan skrin kosong** Dasar meja bersih untuk pengendalian kertas dan media penyimpanan boleh alih serta dasar skrin kosong untuk kemudahan pemprosesan maklumat hendaklah digunakan.	Peneraju ISMS	YA	YA	Memastikan polisi *clear desk* dan *clear screen* diguna pakai.	• GPKTMK Perkara 11.3 (i) : Panduan *Clear Desk* dan *Clear Screen* • Buku Panduan Perkhidmatan Perubatan Pusat Kesihatan Universiti

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
A.12 KESELAMATAN OPERASI	A.12.1	**Prosedur dan tanggungjawab operasi** Memastikan operasi kemudahan pemprosesan maklumat yang betul dan selamat.					
	A.12.1.1	**Prosedur operasi yang didokumenkan** Prosedur operasi hendaklah didokumenkan dan disediakan untuk semua pengguna yang memerlukannya.	Pusat Jaminan Kualiti	YA	YA	Memastikan prosedur operasi didokumen dan disediakan kepada yang memerlukan.	• Prosedur Pengurusan Dokumen ISO (UPM/PGR/P001) • Sistem Pengurusan ISO UPM (e-ISO) - http://reg.upm.edu.my/eISO
	A.12.1.2	**Pengurusan perubahan** Perubahan dalam organisasi, proses perniagaan, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal.	Pusat Jaminan Kualiti & Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan perubahan kepada organisasi, proses bisnes dan fasiliti pemprosesan maklumat dikawal.	• Bidang kuasa Pihak Berkuasa Universiti di bawah Seksyen 16 Perlembagaan UPM termasuklah: (a) Bidang kuasa Lembaga Pengarah Universiti (b) Bidang kuasa Senat Universiti (c) Bidang kuasa Jawatankuasa Tetap Kewangan (d) Bidang kuasa Jawatankuasa Pengurusan Universiti • Bidang kuasa Mesyuarat Kajian Semula Pengurusan • Bidang kuasa Jawatankuasa Kualiti

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
							• Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) • Prosedur Perkhidmatan ICT (UPM/OPR/IDEC/P002)
	A.12.1.3	**Pengurusan kapasiti** Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan kapasiti masa hadapan bagi memastikan prestasi sistem yang dikehendaki dicapai.	Peneraju ISMS	YA	YA	Memastikan penggunaan sumber dipantau dan unjuran dibuat untuk keperluan masa depan untuk memastikan keperluan prestasi sistem.	• GPKTMK 12.1 (d): Pengurusan Kapasiti • Prosedur Penyelenggaran ICT (UPM/OPR/IDEC/P003) • Arahan Kerja Konfigurasi Server (UPM/ISMS/OPR/AK11)
	A.12.1.4	**Pengasingan persekitaran pembangunan, pengujian dan operasi** Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko akses tanpa izin atau perubahan	~~Peneraju ISMS~~ Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan pembangunan, pengujian dan operasi persekitaran diasingkan untuk mengurangkan risiko kepada akses yang tidak dibenarkan.	• ~~GPKTMK 14.0 : Perolehan, pembangunan dan penyelenggaraan sistem maklumat~~ • GPKTMK 14.3 (a) : Prosedur Kawalan Persekitaran Selamat • Garis Panduan Penyediaan Server Di Pusat Data (UPM/ISMS/OPR/GP02/PENYEDIAAN SERVER) 7.2.2

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
		kepada persekitaran operasi.					
	A.12.2	**Perlindungan daripada perisian hasad** Memastikan maklumat dan kemudahan pemprosesan maklumat dilindungi daripada perisian hasad.					
	A.12.2.1	**Kawalan daripada perisian hasad** Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan daripada perisian hasad hendaklah dilaksanakan, digabungkan dengan kesedaran pengguna yang sewajarnya.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan kawalan ke atas perisian hasad (*malware)* dibangunkan.	• GPKTMK 12.2 (a) : Perlindungan daripada Perisian Berbahaya
	A.12.3	**Sandaran** Melindungi kehilangan data.					
	A.12.3.1	**Sandaran maklumat** Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan salinan pendua dilaksanakan dan diuji secara berkala.	• GPKTMK Perkara 12.3 (a) : *Backup* • Garis Panduan Pengurusan *Backup* Pangkalan Data dan Aplikasi (UPM/ISMS/OPR/GP14/BACKUP)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
		tetap menurut dasar sandaran yang dipersetujui.					
	A.12.4	**Pengelogan dan pemantauan** Merekodkan kejadian dan menghasilkan bukti.					
	A.12.4.1	**Pengelogan kejadian** Log kejadian yang merekodkan aktiviti pengguna, pengecualian, ralat dan kejadian keselamatan maklumat hendaklah dihasilkan, disimpan dan dikaji semula secara tetap.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan *event log* dijana, disimpan dan dikaji secara berkala.	• GPKTMK 12.4: *Logging* dan Pemantauan
	A.12.4.2	**Perlindungan maklumat log** Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada ubahan dan akses tanpa izin.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan kemudahan dan maklumat dilindungi daripada akses yang tidak dibenarkan.	• GPKTMK 12.4 (b): Perlindungan Maklumat Log • Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/GP06/Pemantauan Capaian)
	A.12.4.3	**Log pentadbir dan pengendali** Aktiviti pentadbir sistem dan pengendali sistem	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan aktiviti pentadbir sistem direkod, dikawal dan di pantau berkala.	• GPKTMK 12.4 (c): Pentadbir dan Operator Log

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
		hendaklah direkodkan dan log tersebut hendaklah dilindungi dan dikaji semula secara tetap.					• Prosedur Kawalan dan Pemantauan Capaian ke Sistem di Pusat Data (UPM/ISMS/OPR/P003) • Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI) • Garis Panduan Perlindungan Maklumat Log (UPM/ISMS/OPR/GP08/MAKLUMAT LOG)
	A.12.4.4	**Penyegerakkan jam** Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah disegerakkan mengikut satu sumber rujukan masa.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan masa bagi semua pemprosesan maklumat diselaraskan dengan satu sumber rujukan masa.	• GPKTMK12.4 (d): Pelarasan Masa • *Network Time Protocol* (time.upm.edu.my)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.12.5	**Kawalan perisian yang beroperasi** Memastikan kewibawaan sistem yang beroperasi.					
	A.12.5.1	**Pemasangan perisian pada sistem yang beroperasi** Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem yang beroperasi.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan kawalan pemasangan perisian ke atas sistem pengoperasian.	• GPKTMK 12.5: Kawalan Ke atas Perisian Pengoperasian • Prosedur Perkhidmatan ICT (UPM/OPR/IDEC/P002) • ~~*Manual installation*~~ Panduan Instalasi
	A.12.6	**Pengurusan kerentanan teknikal** Mencegah eksploitasi kerentanan teknikal.					
	A.12.6.1	**Pengurusan kerentanan teknikal** Maklumat tentang kerentanan teknikal sistem maklumat yang digunakan hendaklah diperoleh pada masa yang tepat, pendedahan organisasi terhadap kerentanan tersebut hendaklah dinilai dan langkah-langkah yang	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan maklumat berkaitan kelemahan terhadap sistem dinilai dan diukur.	• GPKTMK 12.6: Pengurusan Kerentanan Teknikal • ~~Garis Panduan Penilaian Risiko Aset (UPM/ISMS/SOK/GP02/RISK ASSESSMENT)~~ • Garis Panduan Penilaian Tahap Keselamatan (UPM/ISMS/OPR/ /GP09/TAHAP KESELAMATAN) • Panduan Penilaian Risiko Aset Sistem Pengurusan Keselamatan Maklumat

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
		sesuai hendaklah diambil untuk menangani risiko yang berkaitan.					
	A.12.6.2	**Sekatan ke atas pemasangan perisian** Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan peraturan kawalan instalasi perisian dibangun dan dilaksanakan.	• GPKTMK 12.6 (b): Menghadkan Instalasi Perisian • ~~*Manual installation*~~ Panduan Instalasi
	A.12.7	**Pertimbangan tentang audit sistem maklumat** Meminimumkan kesan aktiviti audit ke atas sistem yang beroperasi.					
	A.12.7.1	**Kawalan audit sistem maklumat** Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas proses perniagaan.	Pusat Jaminan Kualiti & Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan keperluan audit dan aktiviti yang melibatkan pengesahan terhadap sistem operasi ~~perlu dirancang dan bersetuju untuk mengurangkan gangguan kepada proses bisnes~~ dirancang dengan teliti dan dipersetujui untuk meminimumkan gangguan (disruption)	• GPKTMK 12.7: Kawalan Audit Sistem Maklumat • Audit Dalaman ISMS

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
						pada proses sesebuah organisasi.	
A.13 KESELAMATAN KOMUNIKASI	A.13.1	**Pengurusan keselamatan rangkaian** Memastikan perlindungan maklumat dalam rangkaian dan dalam kemudahan sokongan pemprosesan maklumat dalam rangkaian.					
	A.13.1.1	**Kawalan rangkaian** Rangkaian hendaklah diurus dan dikawal bagi melindungi maklumat dalam sistem dan aplikasi.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan rangkaian perlu urus dan dikawal.	• GPKTMK 13.1 : Pengurusan Keselamatan Rangkaian • GPKTMK 13.2 : Kawalan Akses Rangkaian • Garis Panduan Pengurusan Pengagihan Rangkaian (UPM/ISMS/OPR/ /GP13/AGIHAN RANGKAIAN) • Garis Panduan Pengurusan UPM-ID (UPM/ISMS/OPR/GP16/UPM-ID)
	A.13.1.2	**Keselamatan perkhidmatan rangkaian** Mekanisme keselamatan, tahap perkhidmatan dan keperluan pengurusan bagi semua perkhidmatan rangkaian hendaklah dikenal pasti dan	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Tidak melibatkan *Internet service provider*. Hanya menggunakan intranet (UPMNET).	• GPKTMK 13.1 Pengurusan Keselamatan Rangkaian • ~~KPI iDEC – (Perkhidmatan rangkaian – ketersediaan rangkaian & jaminan jalur lebar)~~ • Kontrak ~~sambungan~~ Perkhidmatan ~~WAN~~ Internet antara UPM dengan *Network Service Provider* (NSP)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
		dimasukkan dalam perjanjian perkhidmatan rangkaian, sama ada perkhidmatan ini disediakan secara dalaman atau oleh khidmat luaran.					• Kontrak perkhidmatan *Firewall* dan WAF dengan pembekal
	A.13.1.3	**Pengasingan dalam rangkaian** Kelompok perkhidmatan maklumat, pengguna dan sistem maklumat hendaklah diasingkan dalam rangkaian.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan pengasingan rangkaian dilaksanakan.	• Garis Panduan Pengurusan Pengagihan Rangkaian (UPM/ISMS/OPR /GP13/AGIHAN RANGKAIAN)
	A.13.2	**Pemindahan maklumat** Memelihara keselamatan maklumat yang dipindahkan dalam sesebuah organisasi dan dengan mana-mana entiti luaran.					
	A.13.2.1	**Dasar dan prosedur pemindahan maklumat** Dasar, prosedur dan kawalan pemindahan formal hendaklah disediakan bagi melindungi pemindahan maklumat	Peneraju ISMS	YA	YA	Memastikan polisi dan kawalan terhadap pemindahan maklumat perlu disediakan.	• GPKTMK 13.3 : Pengurusan Pertukaran Maklumat • Prosedur Pertukaran Maklumat (UPM/ISMS/SOK/P002) • Garis Panduan Pengendalian Maklumat (UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
		melalui penggunaan semua jenis kemudahan komunikasi.					
	A.13.2.2	**Perjanjian tentang pemindahan maklumat** Perjanjian hendaklah menangani aspek keselamatan dalam pemindahan maklumat perniagaan antara organisasi dengan pihak luaran.	Peneraju ISMS & Pejabat Bursar	YA	YA	Memastikan kontrak perjanjian memenuhi keperluan keselamatan penghantaran maklumat diantara pembekal dan organisasi.	• GPKTMK 13.3(a) : Pertukaran Maklumat • Peraturan Kewangan • Prosedur Pertukaran Maklumat (UPM/ISMS/SOK/P002)
	A.13.2.3	**Pesanan elektronik** Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya.	Pusat Pembangunan Maklumat dan Komunikasi, Pejabat Pendaftar & Pusat Strategi dan Perhubungan Korporat	YA	YA	Memastikan kawalan terhadap pesanan elektronik dibangunkan.	• Akta Rahsia Rasmi 1972 • Kaedah-Kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian F • GPKTMK Perkara 13.3 (b): Pengurusan Mel Elektronik • Garis Panduan E-mel UPM • Panduan Amalan Komunikasi Berkesan • Surat Aku Janji ~~Pekerja~~

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.13.2.4	**Perjanjian kerahsiaan atau ketakdedahan** Keperluan untuk perjanjian kerahsiaan atau ketakdedahan yang menggambarkan keperluan organisasi terhadap perlindungan maklumat hendaklah dikenal pasti, dikaji semula dan didokumenkan secara tetap.	Pejabat Pendaftar & Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan NDA bagi keperluan melindungi maklumat perlu dikenal pasti, di pantau dan didokumenkan.	• Akta Rahsia Rasmi 1972 • Akta Arkib Negara 2003 (Akta 629) • GPKTMK Perkara 15.1 : Pihak Ketiga • Borang Permohonan Data (OPR/PEND/BR01/DATA). Bahagian D:Perakuan Pemohon dan Pengesahan Ketua PTJ/Ketua Jabatan untuk Sokongan • *Non Discloser Aggreement* (NDA) • Surat Aku Janji ~~Pekerja~~ • Surat Aku Janji Pihak Luar
A.14 PEMEROLEHAN, PEMBANGUNAN DAN PENYENGGARAAN SISTEM	A.14.1	**Keperluan keselamatan sistem maklumat** Memastikan keselamatan maklumat dijadikan bahagian penting dalam sistem maklumat sepanjang kitar hayat. Ini juga termasuk keperluan untuk sistem maklumat yang menyediakan perkhidmatan melalui rangkaian awam.					
	A.14.1.1	**Analisis dan spesifikasi keperluan keselamatan maklumat** Keperluan berkaitan keselamatan maklumat hendaklah disertakan dalam keperluan untuk	Peneraju ~~Proses~~ ISMS	YA	YA	Memastikan keperluan keselamatan maklumat perlu dimasukkan ke dalam sistem baharu atau sistem sedia ada.	• Prosedur Perolehan Universiti (UPM/SOK/KEW-BUY/P016) • Garis Panduan Perlaksanaan Pengaturcaraan Sistem Aplikasi (OPR/iDEC/GP06/Pengaturcaraan Aplikasi)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
		sistem maklumat baharu atau penambahbaikan pada sistem maklumat sedia ada.					
	A.14.1.2	**Melindungi perkhidmatan aplikasi dalam rangkaian awam** Maklumat yang terlibat dalam perkhidmatan aplikasi yang disebarkan melalui rangkaian awam hendaklah dilindungi daripada aktiviti pemalsuan, pertikaian kontrak serta pendedahan dan pengubahsuaian yang tidak dibenarkan.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan kawalan terhadap rangkaian awam perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan atau pengubahsuaian yang tidak dibenarkan.	• GPTMK 3.0 Perkara 13.1 : Pengurusan Keselamatan Rangkaian • Garis Panduan Keselamatan Peralatan Mudah Alih (UPM/ISMS/SOK/GP05/PERALATAN MUDAH ALIH) 2.0 Panduan 1(viii) • Perlaksanaan *Network Authentication* UPM https://authenticate.upm.edu.my/
	A.14.1.3	**Melindungi transaksi perkhidmatan aplikasi** Maklumat yang terlibat dalam transaksi perkhidmatan aplikasi hendaklah dilindungi bagi mengelakkan	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan maklumat yang terlibat dalam transaksi perkhidmatan aplikasi dilindungi untuk menghalang penghantaran yang tidak lengkap, tersalah laluan ,	• GPTMK 14.1 (c) – Melindungi Transaksi Perkhidmatan Aplikasi • Perlaksanaan *Secure Socket Layer-SSL* di Sistem Aplikasi

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
		penghantaran tidak sempurna, salah hala, pindaan mesej tanpa kebenaran, pendedahan tanpa kebenaran, duplikasi atau ulang tayang mesej tanpa kebenaran.				pengubahan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan , duplikasi mesej yang tidak dibenarkan atau ulangan.	
	A.14.2	**Keselamatan dalam proses pembangunan dan sokongan** Memastikan keselamatan maklumat direka bentuk dan dilaksanakan dalam kitar hayat pembangunan sistem maklumat.					
	A.14.2.1	**Dasar pembangunan selamat** Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan polisi keselamatan pembangunan sistem dan aplikasi dibangun dan diguna pakai.	• GPKTMK Perkara 14.1 : Keselamatan dalam Pembangunan Sistem dan Aplikasi • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) • Garis Panduan Perlaksanaan Pengaturcaraan Sistem Aplikasi (OPR/iDEC/GP06/Pengaturcaraan Aplikasi)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.14.2.2	**Prosedur kawalan perubahan sistem** Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan prosedur kawalan perubahan formal.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan perubahan kepada proses pembangunan perlu dikawal menggunakan prosedur kawalan perubahan.	• GPKTMK Perkara 14.2 (a) : Prosedur Kawalan Perubahan • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001)
	A.14.2.3	**Kajian semula teknikal bagi aplikasi selepas perubahan platform operasi** Apabila platform operasi berubah, aplikasi penting perniagaan hendaklah dikaji semula dan diuji bagi memastikan tiada impak yang menjejaskan ke atas operasi atau keselamatan organisasi.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan perubahan ke atas aplikasi perlu di semak dan diuji untuk memastikan tiada kesan buruk terhadap organisasi atau keselamatan.	• GPKTMK Perkara 14.2 (a) : Prosedur Kawalan Perubahan • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.14.2.4	**Sekatan ke atas perubahan dalam pakej perisian** Pengubahsuaian ke atas pakej perisian adalah tidak digalakkan, terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal dengan ketat.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan sebarang perubahan atau pengubahsuaian pakej aplikasi perlu dikawal.	• GPKTMK Perkara 14.2 (a) : Prosedur Kawalan Perubahan • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001)
	A.14.2.5	**Prinsip kejuruteraan sistem yang selamat** Prinsip kejuruteraan bagi sistem yang selamat hendaklah diwujudkan, didokumenkan, disenggara dan digunakan untuk sebarang usaha pelaksanaan sistem maklumat.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan prinsip persekitaran pembangunan selamat diamalkan dalam setiap projek pembangunan sistem aplikasi.	• GPKTMK 14.3 : Persekitaran Pembangunan Selamat • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) • Garis Panduan Perlaksanaan Pengaturcaraan Sistem Aplikasi (OPR/iDEC/GP06/Pengaturcaraan Aplikasi)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.14.2.6	**Persekitaran pembangunan selamat** Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan persekitaran pembangunan selamat diamalkan dalam setiap proses pembangunan sistem aplikasi.	• GPKTMK 3.0 Perkara 14.3 : Persekitaran Pembangunan Selamat • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) • Garis Panduan Perlaksanaan Pengaturcaraan Sistem Aplikasi (OPR/iDEC/GP06/Pengaturcaraan Aplikasi)
	A.14.2.7	**Pembangunan oleh khidmat luaran** Organisasi hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dijalankan oleh khidmat luaran.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan aktiviti pembangunan oleh pihak luar perlu diselia dan dipantau.	• GPKTMK 14.3 (C) : Pembangunan Sistem Aplikasi oleh Pihak Ketiga • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) • Prosedur Perolehan Universiti (UPM/SOK/KEW-BUY/P016) • Dokumen Kontrak

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.14.2.8	**Pengujian keselamatan sistem** Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan ujian keselamatan perlu dilaksanakan semasa pembangunan aplikasi.	• Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) • Garis Panduan Penilaian Tahap Keselamatan (UPM/ISMS/OPR /GP09/TAHAP KESELAMATAN)
	A.14.2.9	**Pengujian penerimaan sistem** Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan ujian penerimaan perlu dilaksanakan bagi sistem baru atau naik taraf.	• Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) • Garis Panduan Pelaksanaan Pengujian Sistem Aplikasi (OPR/iDEC/GP05/Pengujian Aplikasi)
	A.14.3	**Data ujian** Memastikan perlindungan bagi data yang digunakan untuk pengujian.					

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.14.3.1	**Perlindungan data ujian** Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan data pengujian dipilih, dilindungi dan dikawal.	• GPKTMK Perkara 14.3 (b. iii) : Pengujian Pembangunan atau Penaiktarafan Sistem • Arahan Kerja Perkhidmatan Sokongan ICT (OPR/IDEC/AK31/ Perkhidmatan Sokongan ICT) - 3.3.2 Pengurusan dan Implimentasi
A.15 HUBUNGAN PEMBEKAL	A.15.1	**Keselamatan maklumat dalam hubungan pembekal** Memastikan perlindungan aset organisasi yang boleh diakses oleh pembekal.					
	A.15.1.1	**Dasar keselamatan maklumat untuk hubungan pembekal** Keperluan keselamatan maklumat untuk mengurangkan risiko yang dikaitkan dengan akses pembekal kepada aset organisasi hendaklah dipersetujui dengan pembekal dan didokumenkan.	Peneraju ISMS	YA	YA	Memastikan keperluan keselamatan maklumat didokumenkan dan dipersetujui oleh pihak pembekal.	• Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi ~~2014~~) 2014, ~~Bhgn~~ Bahagian F, Klausa 16 (c) • GPKTMK Perkara 15.1 : Pihak Ketiga • Prosedur Perolehan Universiti (UPM/SOK/KEW-BUY/P016) • Surat Aku Janji Pihak Luar • Kontrak Bekalan/Perkhidmatan

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.15.1.2	**Menangani keselamatan dalam perjanjian pembekal** Semua keperluan keselamatan maklumat yang berkaitan hendaklah diwujudkan dan dipersetujui dengan setiap pembekal yang boleh mengakses, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur IT untuk maklumat organisasi.	Peneraju ISMS	YA	YA	Memastikan keperluan keselamatan maklumat dibangunkan dan dipersetujui oleh pihak pembekal.	• Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi ~~2014~~) 2014, ~~Bhgn~~ Bahagian F, Klausa 16 (c) • GPKTMK Perkara 15.1 : Pihak Ketiga • Prosedur Perolehan Universiti (UPM/SOK/KEW-BUY/P016) • Dokumen Perjanjian antara UPM dan Pihak Pembekal • Surat Aku Janji Pihak Luar • Kontrak Bekalan/Perkhidmatan

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.15.1.3	**Rantaian bekalan teknologi maklumat dan komunikasi** Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk menangani risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk.	Pejabat Bursar & Pejabat Penasihat Undang-Undang	YA	YA	Memastikan dokumen perjanjian antara pihak pembekal memenuhi keperluan keselamatan maklumat.	• GPKTMK Perkara 15.1 : Pihak Ketiga • Prosedur Perolehan Universiti (UPM/SOK/KEW-BUY/P016) • Senarai Semak Surat Cara Undang-undang (Perjanjian/Persefahaman)
	A.15.2	**Pengurusan penyampaian perkhidmatan pembekal** Mengekalkan tahap keselamatan maklumat dan penyampaian perkhidmatan yang dipersetujui selaras dengan perjanjian pembekal.					
	A.15.2.1	**Memantau dan mengkaji semula perkhidmatan pembekal** Organisasi hendaklah memantau, mengkaji semula dan mengaudit penyampaian perkhidmatan pembekal secara tetap.	Pejabat Bursar	YA	YA	Memastikan pemantauan, semakan terhadap penerimaan perkhidmatan pembekal dijalankan secara berkala.	• GPKTMK Perkara 15.2 : Pengurusan Penyampaian Perkhidmatan Pihak Ketiga • Arahan Kerja Penilaian Prestasi Syarikat (UPM/SOK/KEW/AK002/BUY)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.15.2.2	**Menguruskan perubahan kepada perkhidmatan pembekal** Perubahan kepada perolehan perkhidmatan daripada pembekal, termasuk mengekalkan dan menambah baik dasar keselamatan maklumat sedia ada, prosedur dan kawalan, hendaklah diuruskan, dengan mengambil kira kegentingan maklumat, sistem dan proses perniagaan yang terlibat dan pentaksiran semula risiko.	Pejabat Bursar & Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan polisi, prosedur dan kawalan bagi mengurus perubahan penyediaan perkhidmatan dilaksanakan.	• GPKTMK Perkara 15.2 : Pengurusan Penyampaian Perkhidmatan Pihak Ketiga • Prosedur Perolehan Universiti (UPM/SOK/KEW-BUY/P016)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
A.16 PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT	A.16.1	**Pengurusan insiden keselamatan maklumat dan penambahbaikan** Memastikan pendekatan yang konsisten dan berkesan dalam pengurusan insiden keselamatan maklumat, termasuk komunikasi tentang kejadian dan kelemahan keselamatan.					
	A.16.1.1	**Tanggungjawab dan prosedur** Tanggungjawab pengurusan dan prosedur hendaklah diwujudkan bagi memastikan tindak balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan prosedur dan tanggungjawan pengurusan dibangunkan untuk memastikan tindak balas yang cepat dan berkesan terhadap insiden keselamatan.	• Pelan Pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT) • Garis Panduan Pengendalian Insiden ICT (UPM/ISMS/OPR/GP18/ PENGENDALIAN INSIDEN)
	A.16.1.2	**Pelaporan kejadian keselamatan maklumat** Kejadian keselamatan maklumat hendaklah dilaporkan melalui saluran pengurusan yang bersesuaian dengan secepat mungkin.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan insiden keselamatan dilapor dengan cepat melalui saluran pengurusan yang betul.	• Pelan Pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT) • Garis Panduan Pengendalian Insiden ICT (UPM/ISMS/OPR/GP18/ PENGENDALIAN INSIDEN)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.16.1.3	**Pelaporan kelemahan keselamatan maklumat** Kakitangan dan kontraktor yang menggunakan sistem dan perkhidmatan maklumat organisasi adalah dikehendaki mencatatkan dan melaporkan sebarang kelemahan keselamatan maklumat yang diperhatikan atau disyaki dalam sistem atau perkhidmatan.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan pekerja dan pembekal melaporkan kelemahan keselamatan yang terdapat pada sistem atau perkhidmatan.	• Pelan pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT) • Prosedur Perkhidmatan ICT (UPM/OPR/IDEC/P002) • Garis Panduan Pengendalian Insiden ICT (UPM/ISMS/OPR/GP18/ PENGENDALIAN INSIDEN)
	A.16.1.4	**Penilaian dan keputusan tentang kejadian keselamatan maklumat** Kejadian keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan insiden keselamatan dinilai dan diputuskan sekiranya diklasifikasikan sebagai insiden keselamatan maklumat.	• Pelan pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT) • Prosedur Perkhidmatan ICT (UPM/OPR/IDEC/P002) • Garis Panduan Pengendalian Insiden ICT (UPM/ISMS/OPR/GP18/ PENGENDALIAN INSIDEN)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.16.1.5	**Tindak balas terhadap insiden keselamatan maklumat** Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan pengurusan insiden keselamatan mengikut prosedur.	• Pelan pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT) • Prosedur Perkhidmatan ICT (UPM/OPR/IDEC/P002) • Garis Panduan Pengendalian Insiden ICT (UPM/ISMS/OPR/GP18/ PENGENDALIAN INSIDEN)
	A.16.1.6	**Mempelajari daripada insiden keselamatan maklumat** Pengetahuan yang diperoleh daripada analisis dan penyelesaian insiden keselamatan maklumat hendaklah digunakan bagi mengurangkan kemungkinan berlakunya insiden atau impak insiden mendatang.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan analisis dan penyelesaian terhadap insiden keselamatan berlaku boleh digunakan untuk mengurangkan kemungkinan atau kesan pada masa akan datang.	• Pelan Pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT) • Garis Panduan Pengendalian Insiden ICT (UPM/ISMS/OPR/GP18/ PENGENDALIAN INSIDEN)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.16.1.7	**Pengumpulan bahan bukti** Organisasi hendaklah mentakrifkan dan menggunakan prosedur untuk mengenal pasti, mengumpul, memperoleh dan memelihara maklumat yang boleh digunakan sebagai bahan bukti.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan pengenalpastian, pengumpulan dan pemuliharaan maklumat perlu dilaksanakan sebagai bukti tindakan.	• GPKTMK 12.4: *Logging* dan Pemantauan • Pelan pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT) • Garis Panduan Pengendalian Insiden ICT (UPM/ISMS/OPR/GP18/ PENGENDALIAN INSIDEN)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
A.17 ASPEK KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERNIAGAAN	A.17.1	**Kesinambungan keselamatan maklumat** Kesinambungan keselamatan maklumat hendaklah diterapkan dalam sistem pengurusan kesinambungan perniagaan organisasi.					
	A.17.1.1	**Perancangan kesinambungan keselamatan maklumat** Organisasi hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam keadaan yang menjejaskan, contohnya, semasa krisis atau bencana.	~~Pejabat Strategi Korporat dan Komunikasi~~ Pejabat Pengurusan Keselamatan dan Kesihatan Pekerjaan & Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan keperluan kesinambungan pengurusan keselamatan maklumat.	• GPKTMK 17.0 – Pengurusan Kesinambungan Perkhidmatan • Pelan Kesinambungan Perkhidmatan • Pelan Pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT)
	A.17.1.2	**Pelaksanaan kesinambungan keselamatan maklumat** Organisasi hendaklah mewujudkan, mendokumenkan, melaksanakan dan menyenggarakan proses,	~~Pejabat Strategi Korporat dan Komunikasi~~ Pejabat Pengurusan Keselamatan dan Kesihatan Pekerjaan &	YA	YA	Memastikan prosedur dan kawalan bagi kesinambungan perkhidmatan dibangun dan didokumenkan.	• GPKTMK 17.0 – Pengurusan Kesinambungan Perkhidmatan • Pelan Kesinambungan Perkhidmatan • Pelan Pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
		prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan.	Pusat Pembangunan Maklumat dan Komunikasi				
	A.17.1.3	**Menentusahkan, mengkaji semula dan menilai kesinambungan keselamatan maklumat** Organisasi hendaklah menentusahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa tetap bagi memastikan ianya sahih dan berkesan semasa keadaan yang menjejaskan.	~~Pejabat Strategi Korporat dan Komunikasi~~ Pejabat Pengurusan Keselamatan dan Kesihatan Pekerjaan & Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan maklumat kawalan kesinambungan keselamatan disahkan dan dilaksanakan secara berkala untuk memastikan ia berkesan sekiranya berlaku bencana.	• GPKTMK 17.0 – Pengurusan Kesinambungan Perkhidmatan • Pelan Kesinambungan Perkhidmatan • Pelan Pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT) • Laporan Pengujian Simulasi DRP ICT UPM

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.17.2	**Lewahan** Memastikan ketersediaan kemudahan pemprosesan maklumat.					
	A.17.2.1	**Ketersediaan kemudahan pemprosesan maklumat** Kemudahan pemprosesan maklumat hendaklah dilaksanakan dengan lewahan yang mencukupi bagi memenuhi keperluan ketersediaan.	Peneraju ISMS & Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan fasiliti pemprosesan dibangunkan bagi memenuhi keperluan ketersediaan maklumat.	• Pelan Kesinambungan Perkhidmatan • Pelan Pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT)
A.18 PEMATUHAN	A.18.1	**Pematuhan kepada keperluan undang-undang dan kontrak** Mengelakkan pelanggaran obligasi undang-undang, statutori, kawal selia atau kontrak yang berkaitan dengan keselamatan maklumat dan sebarang keperluan keselamatan.					
	A.18.1.1	**Pengenalpastian keperluan undang-undang dan kontrak yang terpakai** Semua keperluan perundangan, statutori, kawal selia, kontrak yang	Pejabat Penasihat Undang-undang	YA	YA	Memastikan keperluan perundangan dikenal pasti dan didokumenkan serta dikemaskini.	• GPKTMK Perkara 18.1 (d) : Keperluan Perundangan • ~~Ringkasan~~ Senarai Undang-undang sedia ada melalui Portal eISO

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
		berkaitan dan pendekatan organisasi bagi memenuhi keperluan ini hendaklah dikenal pasti dengan jelas, didokumenkan dan dikemas kini bagi setiap sistem maklumat dan organisasi.					
	A.18.1.2	**Hak harta intelek** Prosedur yang sesuai hendaklah dilaksanakan bagi memastikan keperluan pematuhan perundangan, kawal selia dan kontrak yang berkaitan dengan hak harta intelek dan penggunaan produk perisian proprietari.	Peneraju ISMS & Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan prosedur bersesuaian dibangunkan untuk memastikan pematuhan kepada undang-undang.	• Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan komunikasi ~~2014~~) 2014, Bahagian D, Klausa 12 ~~Perkara 12 : Perlindungan Hak Cipta dan Pelesenan~~ • Jawatankuasa Teknologi Maklumat dan Komunikasi UPM • Kontrak Bekalan/Perkhidmatan
	A.18.1.3	**Perlindungan rekod** Rekod perlu dilindungi daripada kehilangan, kemusnahan, pemalsuan, akses tanpa izin dan pengeluaran tanpa kebenaran, mengikut	Peneraju ISMS	YA	YA	Memastikan rekod perlu di lindungi daripada kehilangan, kemusnahan, pemalsuan, akses tanpa kebenaran, peraturan, kontra atau keperluan bisnes.	• Akta Arkib Negara 2003 (Akta 629) • GPKTMK Perkara 8.3 (c) : Keselamatan Dokumen • Prosedur Pengurusan Dokumen ISO (UPM/PGR/P001)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
		keperluan undang-undang, kawal selia, kontrak dan perniagaan.					• Garis Panduan Pengurusan Keselamatan Perlindungan Dokumen Rasmi Universiti Putra Malaysia • Panduan Pengurusan Fail dan Rekod Universiti
	A.18.1.4	**Privasi dan perlindungan maklumat peribadi** Privasi dan perlindungan maklumat peribadi hendaklah dipastikan seperti yang dikehendaki dalam undang-undang dan peraturan yang relevan jika berkenaan.	Peneraju ISMS & Pejabat Pendaftar	YA	YA	Memastikan perlindungan terhadap maklumat peribadi memenuhi keperluan perundangan berkaitan.	• GPKTMK Perkara 13.3 : Pengurusan Pertukaran Maklumat • Prosedur Pengurusan Dokumen ISO (UPM/PGR/P001) • Prosedur Pertukaran Maklumat (UPM/ISMS/SOK/P002) • Borang Pergerakan Fail Pejabat Pendaftar (Fail Peribadi)
	A.18.1.5	**Peraturan kawalan kriptografi** Kawalan kriptografi hendaklah digunakan bagi mematuhi semua perjanjian, undang-undang dan peraturan yang relevan.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan kawalan kriptografi digunakan dengan mematuhi semua perjanjian berkenaan, undang-undang dan peraturan.	• Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi ~~2014~~) 2014, Bahagian G, Klausa 21 ~~Perkara 21 : Kawalan Kriptografi~~ • GPKTMK Perkara 10.0 : Kawalan Kriptografi

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
							• Garis Panduan Pengendalian Maklumat (UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT)
	A.18.2	**Kajian semula keselamatan maklumat** Memastikan keselamatan maklumat dilaksanakan dan dikendalikan menurut dasar dan prosedur organisasi.					
	A.18.2.1	**Kajian semula keselamatan maklumat secara berkecuali** Pendekatan organisasi dalam menguruskan keselamatan maklumat dan pelaksanaannya (iaitu, objektif kawalan, kawalan, dasar, proses dan prosedur untuk keselamatan maklumat) hendaklah dikaji semula secara berkecuali pada sela masa yang dirancang atau apabila berlaku perubahan yang ketara.	Pusat Jaminan Kualiti	YA	YA	Memastikan pengurusan keselamatan maklumat dikaji semula secara berkala atau apabila perubahan ketara berlaku.	• Mesyuarat Kajian Semula Pengurusan UPM • Mesyuarat Jawatankuasa Kualiti UPM • Mesyuarat Jawatankuasa Kerja ISMS

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.18.2.2	**Pematuhan dasar dan standard keselamatan** Pengurus hendaklah mengkaji semula secara tetap pematuhan pemprosesan maklumat dan prosedur dalam bidang tanggungjawabnya terhadap dasar keselamatan yang bersesuaian, standard dan sebarang keperluan keselamatan yang lain.	Pusat Jaminan Kualiti	YA	YA	Memastikan pematuhan ke atas proses dan prosedur disemak semula dengan dasar-dasar keselamatan yang sesuai, standard dan sebarang keperluan keselamatan yang lain.	• Prosedur Pengurusan Dokumen ISO (UPM/PGR/P001) • Mesyuarat Jawatankuasa Kualiti UPM
	A.18.2.3	**Kajian semula pematuhan teknikal** Sistem maklumat hendaklah dikaji semula secara tetap bagi mematuhi dasar dan standard keselamatan maklumat organisasi.	Peneraju ISMS & Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan sistem maklumat hendaklah dikaji semula secara berkala untuk mematuhi dasar dan standard keselamatan maklumat organisasi.	• Mesyuarat Jawatankuasa Keselamatan Teknologi Maklumat & Komunikasi • UPMCert • Garis Panduan Penilaian Tahap Keselamatan (UPM/ISMS/OPR/GP09/Tahap Keselamatan)

Nota: terma 'staf' ditukar kepada 'pekerja' selaras dengan pengunaan terma tersebut dalam Dasar Kualiti yang diluluskan oleh Lembaga Pengurusan Universiti pada 20 Jun 2017. Pengemaskinian ke atas dokumen terkawal dan dokumen rujukan lain yang terlibat dalam proses kerja akan dibuat secara berperingkat.

DOKUMEN RUJUKAN PELAKSANAAN SISTEM PENGURUSAN KESELAMATAN MAKLUMAT

http://www.upm.edu.my

DOKUMEN RUJUKAN PELAKSANAAN SISTEM PENGURUSAN KESELAMATAN MAKLUMAT UPM

Senarai Kandungan

1. PENGENALAN

1.1 Pengenalan Sistem Pengurusan Keselamatan Maklumat *(Information Security Management System – ISMS)*

ISO/IEC 27001:2013 ISMS merupakan piawaian yang menetapkan satu set keperluan Sistem Pengurusan Keselamatan Maklumat. Istilah maklumat, merangkumi koleksi fakta dalam bentuk kertas atau mesej elektronik bagi mencapai misi dan objektif organisasi. Maklumat merangkumi sistem dokumentasi, prosedur operasi, rekod agensi, profil pelanggan, pangkalan data, fail data dan maklumat, maklumat arkib dan lain-lain.

Pembudayaan ISMS akan mewujudkan sistem penyampaian yang bukan sahaja memenuhi tuntutan serta kepuasan pengguna dan mematuhi peraturan semasa tetapi membolehkan sistem penyampaian beroperasi dalam keadaan baik, selamat dan terkawal.

ISMS turut menyediakan tanda aras (benchmark) tahap pengurusan keselamatan maklumat Universiti berasaskan piawaian antarabangsa serta memantapkan perlindungan maklumat dalam aset ICT berteraskan prinsip kerahsiaan, integriti dan ketersediaan.

ISMS dibangunkan berdasarkan kepada keperluan dalam Klausa 4: Konteks Organisasi hingga Klausa 10: Penambahbaikan dalam piawaian ISO/IEC 27001:2013 yang hendaklah dipatuhi mengikut keperluan piawaian.

1.2 Sejarah Pelaksanaan ISMS di UPM

UPM telah memulakan tindakan melaksanakan dengan adanya arahan daripada MAMPU yang telah meminta agar semua Universiti Awam dipersijilkan dengan ISO/IEC 27001 agar keselamatan maklumat terpelihara, diperoleh dengan cepat dan keselamatannya di kawal.

UPM telah mengorak langkah ke arah ISMS mulai 8 Disember 2011. Audit Peringkat Pertama telah diadakan pada 24 Oktober 2012, disusuli oleh Audit Peringkat Kedua pada 19 hingga 20 Disember 2012. Alhamdulillah UPM telah berjaya melepasi peringkat persijilan ini dan ~~dengan memperolehi tujuh (7) peluang penambahbaikan.~~ UPM telah berjaya memperolehi sijil ISMS bernombor AR5761 pada 4 Januari 2013.

Pada tahun 2018, menerusi Audit Pensijilan Semula SIRIM (kitaran kedua) yang diadakan pada 2 September & 1 - 3 Oktober 2018, UPM telah berjaya memperluaskan skop pensijilan ISMS kepada proses penilaian pengajaran prasiswazah di Fakulti bagi Kampus Serdang dan Bintulu. Sejajar dengan itu juga, no. Pensijilan ISMS telah dipinda kepada ISMS 00150 berdasarkan ketetapan terkini oleh pihak SIRIM.

2. PELAKSANAAN ISMS

2.1 Dasar ISMS

Pemakaian Dasar Sistem Pengurusan Keselamatan Maklumat (ISMS) yang terkini adalah sebagaimana paparan dalam Sistem Pengurusan ISO (eISO) UPM (http://reg.upm.edu.my/eISO).

2.2 Skop Pensijilan, Pengecualian Skop dan Pusat Tanggungjawab (PTJ) yang Terlibat

Skop pensijilan ISMS UPM adalah:

i. Sistem Pengurusan Keselamatan Maklumat bagi Proses Pendaftaran Pelajar Baharu Prasiswazah Merangkumi Aktiviti Semakan Tawaran Hingga Pendaftaran Kolej Kediaman; dan

ii. Sistem Pengurusan Keselamatan Maklumat bagi Proses Penilaian Pengajaran Prasiswazah di Fakulti.

Pengecualian skop pensijilan ISMS proses pendaftaran pelajar baharu prasiswazah adalah kepada pendaftaran kursus, *Meal Plan* dan aktiviti kemasukan pendaftaran pelajar baharu prasiswazah untuk:

i. Pengajian Jarak Jauh;
ii. Program untuk Eksekutif; dan
iii. Antarabangsa.

~~**PTJ terlibat** adalah:~~

~~i. Pusat Jaminan Kualiti;~~
~~ii. Bahagian Kemasukan dan Bahagian Urus Tadbir Akademik;~~
~~iii. Pusat Pembangunan Maklumat dan Komunikasi;~~
~~iv. Pejabat Penasihat Undang-Undang;~~
~~v. Pejabat Strategi Korporat dan Komunikasi;~~
~~vi. Pejabat Pendaftar;~~
~~vii. Pejabat Bursar;~~
~~viii. Pusat Kesihatan Universiti;~~
~~ix. Bahagian Hal Ehwal Pelajar;~~
~~x. Bahagian Keselamatan Universiti;~~
~~xi. Perpustakaan Sultan Abdul Samad;~~
~~xii. Pejabat Pembangunan dan Pengurusan Aset;~~
~~xiii. Pusat Pembangunan Akademik;~~
~~xiv. Semua Kolej Kediaman;~~
~~xv. Semua Fakulti; dan~~
~~xvi. Universiti Putra Malaysia Kampus Bintulu, Sarawak.~~

Senarai Pusat Tanggungjawab yang terlibat dengan pelaksanaan Sistem Pengurusan Keselamatan Maklumat UPM adalah sebagaimana paparan dalam Sistem Pengurusan ISO (eISO) UPM (http://reg.upm.edu.my/eISO).

2.3 Objektif ISMS

Penetapan Objektif ISMS yang terkini adalah sebagaimana paparan dalam Sistem Pengurusan ISO (eISO) UPM (http://reg.upm.edu.my/eISO).

Nota: Pemantauan pencapaian objektif keselamatan maklumat di buat melalui Mesyuarat Jawatankuasa Kualiti sebanyak dua kali setahun (pertengahan dan akhir tahun) dan penilaian keseluruhan bagi tujuan penambahbaikan dibuat melalui Mesyuarat Kajian Semula Pengurusan ISMS setiap tahun.

2.4 Pihak Berkepentingan dan Keperluan Mereka

Pihak Berkepentingan dan Keperluan Mereka yang terlibat dengan pelaksanaan Sistem Pengurusan Keselamatan Maklumat UPM adalah sebagaimana paparan dalam Sistem Pengurusan ISO (eISO) UPM (http://reg.upm.edu.my/eISO).

~~BIL.~~	~~PIHAK BERKEPENTINGAN~~	~~KEPERLUAN PIHAK BERKEPENTINGAN~~
~~1.~~	~~Pelajar~~	~~Maklumat/data peribadi dan akademik pelajar yang dilindungi~~
~~2.~~	~~Warga UPM~~	~~Maklumat/data peribadi yang dilindungi~~
~~3.~~	~~Ibubapa dan penjaga~~	~~Maklumat/data prestasi pelajar yang dilindungi~~
~~4.~~	~~Kementerian Pendidikan Malaysia (KPM)~~	~~Maklumat/data profil Universiti, pelajar, penyelidikan, sumber manusia dan kewangan yang dilindungi~~
~~5.~~	~~Penaja Pendidikan~~	~~Maklumat/data prestasi pelajar yang tepat~~
~~6.~~	~~Agensi Kerajaan~~	~~Maklumat/data yang tepat~~
~~7.~~	~~Pembekal~~	~~i. Maklumat/data kontrak yang dipatuhi~~ ~~ii. Maklumat/data kerjasama yang jelas~~
~~8.~~	~~Badan Penarafan~~	~~Maklumat /data yang tepat~~
~~9.~~	~~Jabatan Ketua Menteri Sarawak~~	~~Maklumat/data Universiti yang tepat~~
~~10.~~	~~Pejabat Residen Bintulu~~	~~Maklumat/data Universiti yang tepat~~

2.5 Isu Dalaman dan Isu Luaran

Isu Dalaman dan Isu Luaran yang terlibat dengan pelaksanaan Sistem Pengurusan Keselamatan Maklumat UPM adalah sebagaimana paparan dalam Sistem Pengurusan ISO (eISO) UPM (http://reg.upm.edu.my/eISO).

~~BIL.~~	~~KEBERHASILAN~~	~~ISU DALAMAN~~	~~ISU LUARAN~~
~~1.~~	~~Meningkatkan reputasi Universiti~~	~~i. Pembudayaan pengurusan~~	~~i. Perubahan Dasar Kerajaan~~

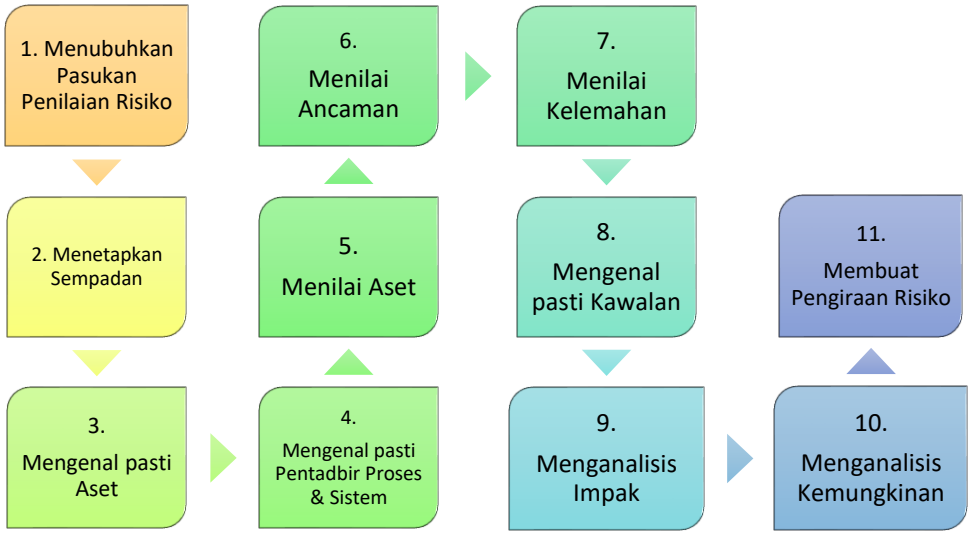
BIL.	KEBERHASILAN	ISU DALAMAN	ISU LUARAN
2.	Mengekalkan status Universiti Penyelidikan (RU)	keselamatan maklumat setiap warga UPM a) Kurang kefahaman dalam kalangan pekerja b) Ketidakjelasan tanggungjawab dan proses ii. Tahap kebolehpercayaan, integriti dan ketersediaan data iii. Kekangan sumber manusia dan kewangan iv. Infrastruktur tidak menyokong proses	ii. Perkembangan teknologi dan inovasi yang pantas iii. Ekonomi tidak menentu iv. Ancaman ekologi v. Ekspektasi pelanggan terlalu tinggi vi. Kriteria penarafan yang berubah vii. Gangguan media sosial viii. Masalah komunikasi
3.	Mengekalkan status Swa Akreditasi		
4.	Mencapai kedudukan 200 universiti terbaik dunia (QS *World Ranking*) menjelang 2020		
5.	Mengekalkan status autonomi tadbir urus		
6.	Mencapai kedudukan 200 laman web universiti terbaik dalam *Webometrics Ranking* menjelang 2020		
7.	Mengekalkan kedudukan 50 universiti terbaik dalam *Green Metric World Ranking*		
8.	Kebolehpasaran graduan (80% semasa konvokesyen)		
9.	Melonjakkan jaringan industri dan masyarakat		
10.	Memperkasakan UPM sebagai Pusat Kecemerlangan Pertanian		
11.	Mempertingkatkan kualiti tadbir urus		

2.6 Pengurusan Risiko

Penilaian Risiko

Penilaian risiko aset yang berkaitan dilaksanakan berasaskan Metodologi Penilaian Risiko Terperinci MyRAM (*Malaysian Public Sector ICT Risk Assessment Methodology*) berpandukan kepada Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

Sebelas (11) langkah utama dalam proses penilaian risiko aset adalah seperti berikut:



Pemulihan Risiko

Perkara yang perlu dikenalpasti dan dilaksanakan semasa proses pemulihan risiko adalah seperti berikut:

a. Membuat pilihan cadangan pemulihan risiko (menerima, mengurangkan, memindahkan, atau mengelakkan);
b. Mengenal pasti kawalan yang bersesuaian terhadap cadangan pemulihan risiko yang telah dipilih;
c. Melaksanakan perbandingan antara kawalan yang dipilih dengan Annex A;
d. Mewujudkan Penyata Pemakaian [*Statement of Applicability (SoA)]* yang mengandungi kawalan bersesuaian;
e. Menyediakan Pelan Pemulihan Risiko; dan
f. Mendapatkan kelulusan Pentadbir Proses dan Pentadbir Sistem serta penerimaan ke atas risiko yang telah dipilih.

Panduan Penilaian Risiko Aset Sistem Pengurusan Keselamatan Maklumat memperincikan mengenai tatacara pengurusan penilaian risiko aset ISMS. Panduan yang juga merupakan lampiran kepada dokumen rujukan pelaksanaan ISMS ini boleh dirujuk melalui Portal eISO UPM di bawah pautan "Panduan Penilaian Risiko Aset Sistem Pengurusan Keselamatan Maklumat".

3. PENYATA PEMAKAIAN *[(STATEMENT OF APPLICABILITY (SOA)]*

Penyata Pemakaian *(Statement of Applicability)* atau SoA menjelaskan justifikasi kawalan dan dokumen rujukan dalam melindungi keselamatan aset ICT dalam skop ISMS. Pemilihan kawalan dalam SoA adalah hasil Pemulihan Risiko dan peraturan-peraturan perlindungan aset ICT dalam Kaedah-Kaedah ~~UPM~~ Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) dan Garis Panduan Keselamatan Teknologi Maklumat dan Komunikasi (GPKTMK).

SoA terkini yang juga merupakan lampiran kepada dokumen rujukan ini boleh dirujuk melalui Portal eISO UPM di bawah pautan "Penyata Pemakaian *[(Statement of Applicability (SoA)]*".

4. JAWATANKUASA DAN PERANAN

4.1 Struktur Organisasi ISMS

Struktur Organisasi ISMS yang terkini adalah sebagaimana paparan dalam Sistem Pengurusan ISO (eISO) UPM (http://reg.upm.edu.my/eISO).

4.2 Peranan dan Tanggungjawab

Peranan dan tanggungjawab Jawatankuasa ISMS yang terkini adalah sebagaimana paparan dalam Sistem Pengurusan ISO (eISO) UPM (http://reg.upm.edu.my/eISO).

PERANAN	TANGGUNGJAWAB
~~**MESYUARAT KAJIAN SEMULA PENGURUSAN**~~	~~1. Melaksanakan semakan pengurusan ke atas sistem pengurusan ISO secara berkala bagi memastikan terus sesuai, mencukupi, dan berkesan;~~ ~~2. Membuat penilaian ke atas peluang penambahbaikan dan keperluan perubahan kepada dasar dan objektif keselamatan ISMS; dan~~ ~~3. Meneliti laporan yang berkaitan dan membuat keputusan yang sesuai.~~
~~**MESYUARAT JAWATANKUASA KUALITI UPM**~~	~~1. Memastikan kesesuaian, kecukupan dan keberkesanan pelaksanaan Sistem Pengurusan ISO secara berkala;~~ ~~2. Membuat penilaian ke atas peluang penambahbaikan dan keperluan perubahan kepada pengukuran keberkesanan ISMS;~~ ~~3. Meluluskan sebarang cadangan pindaan dokumen skop pengurusan; dan~~ ~~4. Mengambil maklum keberkesanan pelaksanaan ISO di peringkat Peneraju Proses dan Pusat Tanggungjawab (PTJ).~~
~~**WAKIL PENGURUSAN**~~	~~1. Memastikan pembangunan dan pelaksanaan ISMS mematuhi keperluan piawaian; dan~~ ~~2. Melaporkan pencapaian ISMS dalam Mesyuarat Kajian Semula Pengurusan (MKSP).~~
~~**SEKRETARIAT PUSAT JAMINAN KUALITI**~~	~~1. Merancang dan mengurus audit dalaman dan audit badan pensijilan Sistem Pengurusan ISO peringkat UPM;~~ ~~2. Menyelaras dan memantau pelaksanaan tindakan penemuan audit dalaman dan audit badan pensijilan;~~ ~~3. Membantu dalam Mesyuarat Jawatankuasa Kerja ISMS; dan~~ ~~4. Membantu dalam pembangunan dan latihan ISMS.~~

PERANAN	TANGGUNGJAWAB
~~**JAWATANKUASA KERJA ISMS**~~	1. ~~Memantau keberkesanan pelaksanaan ISMS;~~ 2. ~~Memantau pencapaian objektif kualiti;~~ 3. ~~Melaksana penambahbaikan terhadap dokumentasi, proses dan perkhidmatan;~~ 4. ~~Menyediakan laporan keberkesanan pelaksanaan Sistem Pengurusan Keselamatan Maklumat;~~ 5. ~~Memantau dan menyemak carta perbatuan ISMS;~~ 6. ~~Membangunkan kriteria penerimaan risiko, tahap risiko dan *risk treatment plan;*~~ 7. ~~Melaksanakan keputusan dan tindakan hasil Mesyuarat Kajian Semula Pengurusan ISMS;~~ 8. ~~Membangun dan menyelenggara pengurusan dokumen dan rekod pelaksanaan ISMS; dan~~ 9. ~~Mengambil tindakan ke atas kawalan ketakakuran, tindakan pembetulan dan peluang penambahbaikan.~~
~~**PASUKAN PUSAT DATA, PASUKAN PENDAFTARAN PELAJAR BAHARU PRASISWAZAH (KAMPUS SERDANG DAN KAMPUS BINTULU) DAN PASUKAN PENILAIAN PENGAJARAN PRASISWAZAH DI FAKULTI**~~	1. ~~Menyediakan analisis jurang, *Statement of Applicability* (SoA) dan prosedur berkaitan;~~ 2. ~~Menyediakan prosedur dan kawalan dalam ISO/IEC 27001:2013;~~ 3. ~~Melaksanakan penilaian risiko dan pelan pemulihan risiko;~~ 4. ~~Menyediakan objektif keselamatan dan kaedah pengukuran keberkesanan kawalan ISMS;~~ 5. ~~Mengukur keberkesanan kawalan ISMS; dan~~ 6. ~~Memantau dan menilai pelaksanaan ISMS.~~ 7. ~~Mengurus dan melaksanakan aktiviti penilaian berisiko;~~ 8. ~~Mengendalikan semakan semula *output* dan dokumen sebelum disampaikan kepada Penasihat Projek;~~ 9. ~~Menilai keputusan, menilai jurang dan menyediakan laporan *High Level Recommendation* (HLR) dan Pelan Pemulihan Risiko.~~

5. SENARAI *STANDARD OPERATION PROCEDURE* (SOP) YANG DIRUJUK

SOP ISMS YANG DIRUJUK DALAM PELAKSANAAN ISMS DI UPM			
Bil	**Kod Dokumen**	**Nama Dokumen**	**Peneraju Proses**
Dokumentasi ISMS ISO/IEC 27001 sebagaimana paparan Portal eISO UPM			
SOP QMS YANG DIRUJUK DALAM PELAKSANAAN ISMS DI UPM			
Bil	**Kod Dokumen**	**Nama Dokumen**	**Peneraju Proses**
1.	UPM/PGR/P001	Prosedur Pengurusan Dokumen ISO	Pusat Jaminan Kualiti
2.	UPM/PGR/P003	Prosedur Kawalan Ketakakuran, Tindakan Pembetulan, dan Peluang Penambahbaikan	Pusat Jaminan Kualiti
3.	UPM/PGR/P004	Prosedur Audit Dalaman ISO	Pusat Jaminan Kualiti
4.	UPM/PGR/P008	Prosedur Mesyuarat Kajian Semula Pengurusan ISO UPM	Pusat Jaminan Kualiti
5.	PU/PS/GP010/SMP-ID	Garis Panduan Pengurusan Identiti Pengguna (ID) Sistem Maklumat Pelajar	Bahagian Kemasukan dan Bahagian Urus Tadbir Akademik
6.	UPM/SOK/BUM/P001	Prosedur Pelantikan Staf Tetap Bagi Kumpulan Pengurusan dan Professional (Bukan Akademik) dan Kumpulan Pelaksana	Pejabat Pendaftar
~~7.~~	~~UPM/SOK/BUM/GP03/Lapor Diri~~	~~Garis Panduan Lapor Diri~~	~~Pejabat Pendaftar~~
8.	UPM/SOK/KEW-BUY/P016	Prosedur Perolehan Universiti	Pejabat Bursar
9.	UPM/SOK/KEW-AST/P012	Prosedur Pengurusan Aset Alih	Pejabat Bursar
10.	UPM/SOK/KEW/GP020/AST	Garis Panduan Pelupusan Aset Alih	Pejabat Bursar
11.	UPM/SOK/KEW/AK002/BUY	Arahan Kerja Penilaian Prestasi Syarikat	Pejabat Bursar
12.	UPM/SOK/LAT/P001	Prosedur Pengurusan Latihan Pekerja Universiti Putra Malaysia	Pejabat Pendaftar
13.	UPM/OPR/PNC-UI/P001	Prosedur Pengurusan Mesyuarat Tatatertib Staf	~~Pejabat Naib Canselor (Unit Integriti)~~Bahagian Governan dan Integriti, Pejabat Naib Canselor
14.	UPM/OPR/BUR-BUY/P003	Prosedur Pendaftaran Syarikat dan Pekerja/Individu	Pejabat Bursar
15.	UPM/OPR/iDEC/P001	Prosedur Pembangunan ICT	Pusat Pembangunan Maklumat dan Komunikasi
16.	UPM/OPR/iDEC/P002	Prosedur Perkhidmatan ICT	Pusat Pembangunan Maklumat dan Komunikasi
17.	UPM/OPR/iDEC/P003	Prosedur Penyelenggaraan ICT	Pusat Pembangunan Maklumat dan Komunikasi

SOP QMS YANG DIRUJUK DALAM PELAKSANAAN ISMS DI UPM			
Bil	**Kod Dokumen**	**Nama Dokumen**	**Peneraju Proses**
18.	UPM/OPR/CADE/AK01	Arahan Kerja Pelaksanaan Penilaian Pengajaran	Pusat Pembangunan Akademik
19.	OPR/iDEC/GP06/ Pengaturcaraan Aplikasi	Garis Panduan Perlaksanaan Pengaturcaraan Sistem Aplikasi	Pusat Pembangunan Maklumat dan Komunikasi
20.	OPR/IDEC/GP07/ IMPLEMENTASI APLIKASI	Garis Panduan Pelaksanaan Implementasi Aplikasi	Pusat Pembangunan Maklumat dan Komunikasi
21.	UPM/OPR/BKU/P001	Prosedur Kawalan Akses	Bahagian Keselamatan Universiti
22.	UPM/SOK/PYG/P002	Prosedur Penyelenggaraan Berkala	Pejabat Pembangunan dan Pengurusan Aset

Kemaskini: ~~29 Julai 2020~~ 30 Mac 2021