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; dan

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:

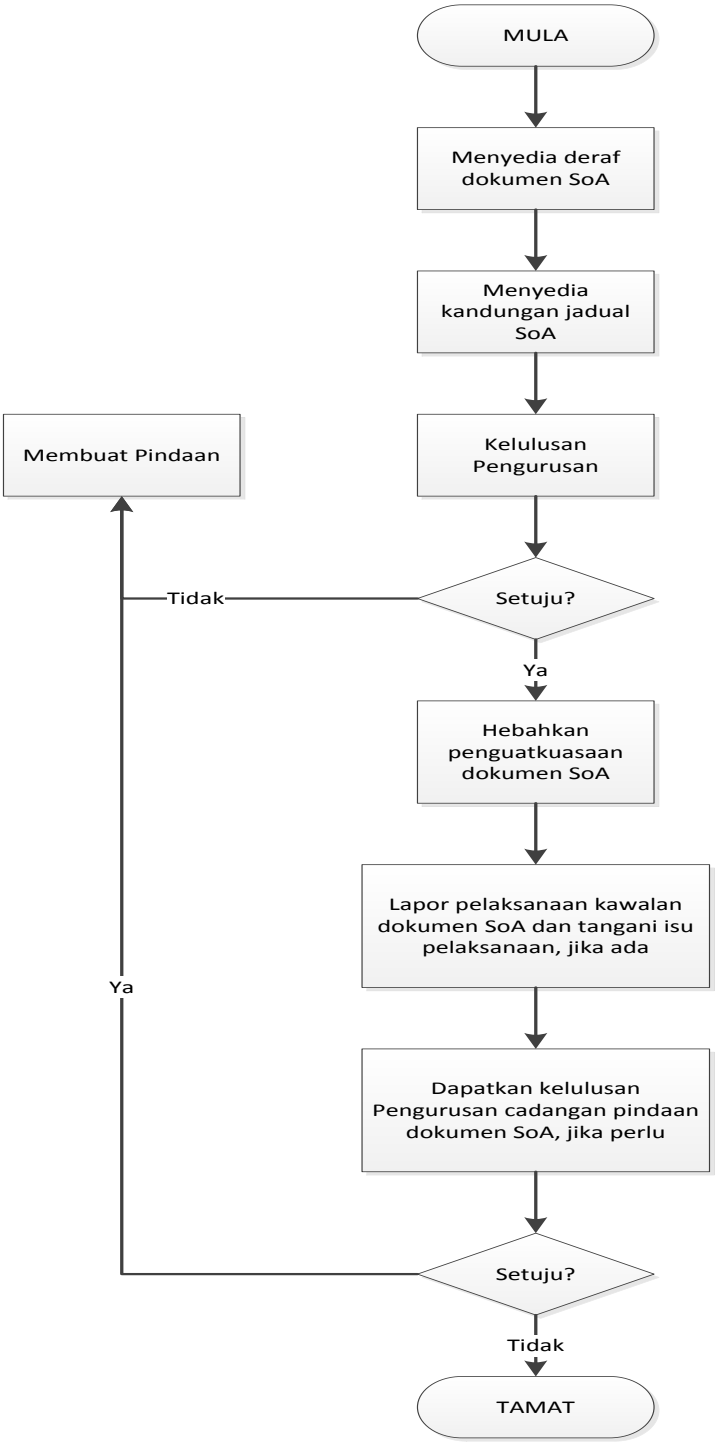
(a) Penemuan penilaian semula risiko;
(b) Perubahan justifikasi pemilihan kawalan;
(c) Perluasan skop ISMS;
(d) Penambahan atau pengecualian aset ISMS;
(e) Perubahan struktur organisasi;
(f) Penambahbaikan ke atas pelaksanaan ISMS;
(g) Pengemaskinian ke atas dokumen rujukan; dan
(h) Perubahan disebabkan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



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 INFORMATION SECURITY POLICY	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 9 Disember 2014 - dikomunikasi menerusi Portal eISO UPM
	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	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**					
		kesesuaian, kecukupan dan keberkesanannya berterusan.					
A.6 ORGANIZATION OF INFORMATION SECURITY	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

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.6.1.2	**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 dalam ELPPT Akademik/Bukan Akademik/Pelaksana ▪ Termasuk tugas pentadbiran. (Contoh: sebagai Dekan, Pengetua Kolej, Pengarah, Penolong Pengarah/Timbalan Pengarah)
	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 • Seksyen 66 Akta Imigresen 1969/63 (Akta 155)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.6.1.4	**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 • Pelan Tindak Balas Insiden • Pelan Pemulihan Bencana ICT (DRP ICT) • Pengauditan OSHA • MyCert – MAMPU • Cybersecurity Malaysia
	A.6.1.5	**Keselamatan maklumat dalam pengurusan projek** Keselamatan maklumat hendaklah ditangani dalam pengurusan projek, tanpa mengambil kira jenis projek.		TIDAK	TIDAK	Tiada sebarang pengurusan projek terlibat dalam pelaksanaan ISMS di bawah skop pensijilan	

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	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-a) Panduan Pengkomputeran 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 staf yang dibenarkan sahaja.	• Garis Panduan Pemantauan Capaian ke Sistem (UPM/ISMS/OPR/GP06/ PEMANTAUAN CAPAIAN) Perkara 4.0 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.7 HUMAN RESOURCE SECURITY	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 pengesahan latar belakang dilaksanakan terhadap staf bagi memenuhi keperluan perundangan dan organisasi	• Prosedur Pelantikan Staf Tetap Bagi Kumpulan Pengurusan dan Profesional (Bukan Akademik) dan Kumpulan Sokongan (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 (kaedah kawalan sedang dibina bagi memastikan semua staf baharu mengisi borang) • Rekod Kenyataan Perkhidmatan (RKP) bagi calon yang dilantik dari agensi luar • Borang Butir-Butir Perkhidmatan Yang Lepas Dengan Badan-Badan Awam/Swasta (SOK/BUM/BR03/BUTIR)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
							• Borang Senarai Semak Temuduga (Sekretariat temuduga menyemak salinan sijil adalah sama dengan sijil asal yang dibawa oleh calon semasa sesi temuduga)
	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 staf dan pembekal menyatakan tanggungjawab organisasi terhadap keselamatan maklumat	• Prosedur Pendaftaran Syarikat dan Staf/Individu (UPM/OPR/BUR-BUY/P003) • Garis Panduan Lapor Diri (Aku Janji Staf UPM) (UPM/SOK/BUM/GP03/LAPOR DIRI) • Borang Perakuan untuk ditandatangani Oleh penjawat Awam Berkenaan Dengan Akta Rahsia Rasmi 1972

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	**Dalam tempoh penjawatan** Memastikan kakitangan dan kontraktor mengetahui dan memenuhi tanggungjawab keselamatan maklumat mereka.					
	A.7.2.1	**Tanggungjawab pengurusan** Pengurusan hendaklah menghendaki semua kakitangan dan kontraktor supaya mengamalkan keselamatan maklumat menurut dasar dan prosedur organisasi yang ditetapkan.	Pejabat Pendaftar & Pejabat Bursar	YA	YA	Memastikan polisi dan prosedur keselamatan maklumat yang telah ditetapkan oleh organisasi diikuti oleh staf dan pembekal	• Perintah Am • Peraturan Kewangan • Prosedur Perolehan Universiti (UPM/SOK/KEW-BUY/P016) • Garis Panduan Lapor Diri (Aku Janji Staf UPM) (UPM/SOK/BUM/GP03/LAPOR DIRI) • Borang Perakuan untuk Ditandatangani oleh Penjawat Awam Berkenaan Akta Rahsia Rasmi 1972

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.7.2.2	**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.	Pejabat Pendaftar, Pejabat Bursar, Pusat Jaminan Kualiti & Peneraju ISMS (Pasukan pendaftaran Pelajar Baharu Prasiswazah – Kampus Serdang)	YA	YA	Memastikan staf, pelajar dan pembekal menerima latihan dan program kesedaran berkaitan dengan polisi organisasi yang berkaitan dengan fungsi kerja masing-masing	• Prosedur Pengurusan Latihan Staf UPM (UPM/SOK/LAT/P001) • GPKTMK Perkara 7.0 (b) ii Dalam Perkhidmatan • Taklimat Keselamatan Maklumat bagi Pelaksanaan Minggu Perkasa Putra • ISMS – Latihan/Takwim di bawah Pusat Jaminan Kualiti
	A.7.2.3	**Proses tatatertib** Proses tatatertib yang formal hendaklah diadakan dan disampaikan kepada kakitangan bagi membolehkan tindakan diambil terhadap mereka yang melakukan	Pejabat Pendaftar & Unit Integriti	YA	YA	Memastikan proses tindakan keselamatan dilaksanakan terhadap staf yang telah melanggar peraturan keselamatan maklumat	• Akta 605 - Akta Badan-badan Berkanun (Tatatertib dan Surcaj) 2000 • Perintah –perintah Am Persekutuan bab D : Tatatertib • Prosedur Pengurusan Mesyuarat Tatatertib Staf (UPM/OPR/PNC-UI/P001) • Garis Panduan Pekerjaan Luar UPM • Kit Panduan Mengurus Staf Tidak Hadir

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
		pelanggaran keselamatan maklumat.					Bertugas
	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 staf atau pembekal yang telah tamat perkhidmatan atau berlaku perubahan staf hendaklah dikenal pasti dan dikuatkuasakan.	• Perintah –perintah Am Persekutuan Bab A : Peraturan-Peraturan Pegawai Awam (Pelantikan, Kenaikan Pangkat Dan Penamatan Perkhidmatan) 2005 • GPKTMK Perkara 7.0 (C) Bertukar Atau Tamat Perkhidmatan • Surat Pelantikan Jawatan Pegawai Kanan dikeluarkan oleh Pejabat Naib Canselor

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
A.8 ASSET MANAGEMENT	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.	Pejabat Bursar & Peneraju ISMS	YA	YA	Memastikan aset yang terlibat dengan fasiliti pemprosesan maklumat dikenalpasti dan inventori aset tersebut disedia dan diselenggara	• Prosedur Pengurusan Aset (UPM/SOK/KEW-AST/P012) • Kaedah-kaedah UPM (Teknologi maklumat dan Komunikasi) 2014 Bahagian D – Pengurusan Aset Teknologi Maklumat dan Komunikasi • GPKTMK 3.0 Perkara 8.0 : Pengurusan Aset
	A.8.1.2	**Pemilikan aset** Aset yang disenggara dalam inventori hendaklah mempunyai pemilik.	Pejabat Bursar & Peneraju ISMS	YA	YA	Memastikan setiap aset yang diselanggara mempunyai pemilik	• Prosedur Pengurusan Aset (UPM/SOK/KEW-AST/P012) • Kaedah-kaedah UPM (Teknologi maklumat dan Komunikasi) 2014 Bahagian D – Pengurusan Aset Teknologi Maklumat dan Komunikasi • GPKTMK 3.0 Perkara 8.0 : Pengurusan Aset

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.	Pusat Pembangunan Maklumat dan Komunikasi & Peneraju ISMS	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

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.8.1.4	**Pemulangan aset** Semua kakitangan dan pengguna pihak luar hendaklah memulangkan semua aset organisasi yang berada dalam pemilikannya apabila ditamatkan penjawatan, kontrak atau perjanjian mereka.	Pejabat Pendaftar, Pejabat Bursar & Peneraju ISMS	YA	YA	Memastikan aset organisasi dipulangkan selepas tamat kontrak	• Perintah –perintah Am Persekutuan Bab A : Peraturan-Peraturan Pegawai Awam (Pelantikan, Kenaikan Pangkat Dan Penamatan Perkhidmatan) 2005 • Prosedur Pengurusan Aset (UPM/SOK/KEW-AST/P012) • Staf : Borang Nota Serah Tugas (SOK/BUM/BR03/SERAH TUGAS) • Dokumen Kontrak Perolehan Pembekal/Pihak Ketiga • Surat Pertukaran (staf tidak lagi boleh mengakses sistem di PTJ lama)
	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	Pejabat Pendaftar & Peneraju ISMS	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)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
		pengubahsuaian yang tidak dibenarkan.					
	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.	Pejabat Pendaftar & Peneraju ISMS	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	• Prosedur Pengurusan Aset (UPM/SOK/KEW-AST/P012) • Kaedah-kaedah UPM (Teknologi maklumat dan Komunikasi) 2014 Bahagian D – Pengurusan Aset Teknologi Maklumat dan Komunikasi • GPKTMK 3.0 Perkara 8.0 Pengurusan Aset • 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) • Arahan Kerja Pelupusan Pita Backup (UPM/ISMS/OPR/AK07)

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 • Garis Panduan Pelupusan Aset (UPM/SOK/KEW/GP020/AST) • GPKTMK 3.0 Perkara 8.3 : Pengendalian media • Garis Panduan Pengendalian Maklumat (UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT) • Arahan Kerja Pelupusan Pita *Backup* (UPM/ISMS/OPR/AK07)
	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) • Arahan Kerja Pengurusan Backup (UPM/ISMS/OPR/AK02)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
A.9 ACCESS CONTROL	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) • 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)
	A.9.2.2	**Peruntukan akses pengguna** Proses formal peruntukan akses pengguna hendaklah dilaksanakan dalam	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)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
		pemberian atau pembatalan hak akses kepada semua jenis pengguna untuk semua sistem dan perkhidmatan.					• 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)
	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) • 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)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.9.2.4	**Pengurusan maklumat pengesahan rahsia pengguna** Peruntukan maklumat pengesahan rahsia hendaklah dikawal melalui proses pengurusan formal.	Pejabat Pendaftar, Bahagian Kemasukan dan Bahagian Urus Tadbir Akademik & Peneraju ISMS	YA	YA	Memastikan pengesahan maklumat rahsia sentiasa dikawal	• GPKTMK 3.0 Perkara 10.0 : Kawalan Kriptografi • Garis Panduan Pengurusan UPM-ID (UPM/ISMS/OPR/GP16/UPM-ID) • Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE/AK01) • Kelulusan Ketua Bahagian Pengurusan Sumber Manusia bagi permohonan baru/ kemaskini bagi perolehan ID eIHRAMS. Penamatan ID bagi staf yang bertukar/berhenti/tiada peranan dilaksanakan dalam tempoh 14 hari bekerja
	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	• 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

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
							Pengajaran (UPM/OPR/CADE/AK01) • Semakan semula ID pengguna eIHRAMS dilaksanakan setahun sekali
	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) • 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)

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)	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)
	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) • Garis Panduan Kawalan Akses Ke Pusat Data (UPM/ISMS/OPR/GP03/KAWALAN AKSES) • Garis Panduan Pemantauan Capaian Ke

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
							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)
	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) • Garis Panduan Pengurusan UPM-ID (UPM/ISMS/OPR/GP16/UPM-ID) • 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**					
	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)
	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 CRYPTOGRAPHY	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) Bahagian Kawalan Keselamatan TMK 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 & Pusat Pembangunan Akademik	YA	YA	Memastikan polisi penggunaan, perlindungan dan jangka hayat kunci kriptografi dibangun dan dilaksanakan	• Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan komunikasi 2014) Bahagian Kawalan Keselamatan TMK 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 PHYSICAL AND ENVIRONMENTAL SECURITY	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 • 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 • Dokumen Rujukan Pelaksanaan Sistem Pengurusan Keselamatan Maklumat - Lokasi Skop Pensijilan ISMS UPM • GPKTMK 11.1(b) Kawalan Masuk Fizikal • 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 • Dokumen Rujukan Pelaksanaan Sistem Pengurusan Keselamatan Maklumat - Lokasi Skop Pensijilan ISMS UPM • GPKTMK 11.1 (d) – Keselamatan Pejabat, Bilik dan Kemudahan
	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) Bhgn D, 9 (b) • GPKTMK 3.0 Perkara 11.1 (e) : Kawalan Persekitaran
	A.11.1.5	**Bekerja di kawasan selamat** Prosedur bekerja di kawasan selamat hendaklah direka bentuk	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**					
		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.	Peneraju ISMS (kecuali Pasukan Pendaftaran Pelajar Baharu Prasiswazah – Kampus Serdang)	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) Bhgn D, 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) Bhgn D, 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
	A.11.2.3	**Keselamatan kabel** Kabel bekalan kuasa dan telekomunikasi yang	Pusat Pembangunan Maklumat dan	YA	YA	Memastikan kabel bekalan kuasa dan telekomunikasi dilidungi	• GPKTMK 3.0 Perkara 11.1 (i) : Keselamatan Kabel • Garis Panduan Pengurusan Sistem

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
		membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan.	Komunikasi			daripada pemintasan, gangguan atau kerosakan	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) Bhgn D, 10 • GPKTMK 3.0 Perkara 11.3 (e) : Penyelenggaraan Peralatan • Prosedur Perkhidmatan ICT (UPM/OPR/IDEC/P002) • Prosedur Penyelenggaraan ICT (UPM/OPR/IDEC/P003)
	A.11.2.5	**Pengalihan aset** Peralatan, maklumat atau perisian tidak boleh dibawa keluar dari premis tanpa mendapat kebenaran terlebih dahulu.	Peneraju ISMS	YA	YA	Memastikan peralatan, maklumat atau perisian tidak di bawa keluar dari lokasi tanpa kebenaran	• Prosedur Pengurusan Aset (UPM/SOK/KEW-AST/P012) • Prosedur Perkhidmatan ICT (UPM/OPR/IDEC/P002) • GPKTMK Perkara 11.3 (f) : Peralatan di Luar Premis

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.11.2.6	**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	YA	YA	Memastikan keselamatan dan risiko setiap aset yang berada dilokasi luar diambil kira	• Prosedur Pengurusan Aset (UPM/SOK/KEW-AST/P012) • Prosedur Perkhidmatan ICT (UPM/OPR/IDEC/P002) • GPKTMK Perkara 11.3 (f) : Peralatan Di Luar Premis
	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 dilupuskan atau diguna semula.	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 13 (g) : Pelupusan Peralatan • Prosedur Pengurusan Aset (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.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*

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
A.12 OPERATION SECURITY	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	YA	YA	Memastikan perubahan kepada organisasi, proses bisnes dan fasiliti pemprosesan maklumat dikawal	• Bidang kuasa Lembaga Pengarah Universiti • Bidang kuasa Senat Universiti • Bidang kuasa Jawatankuasa Tetap Kewangan • 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**					
	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 • 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 kepada persekitaran operasi.	Peneraju ISMS	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 • Garis Panduan Penyediaan Server Di Pusat Data (UPM/ISMS/OPR/GP02/PENYEDIAAN SERVER)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	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 *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 tetap menurut dasar sandaran yang dipersetujui.	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 (UPM/ISMS/OPR /GP14/BACKUP) • Garis Panduan Penggunaan Data Pengujian (UPM/ISMS/OPR/GP15/DATA PENGUJIAN)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
							• Arahan Kerja Pengurusan Backup (UPM/ISMS/OPR/AK02)
	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 • Sistem Log Aktiviti Bepusat (Log Central System)
	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)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	A.12.4.3	**Log pentadbir dan pengendali** Aktiviti pentadbir sistem dan pengendali sistem hendaklah direkodkan dan log tersebut hendaklah dilindungi dan dikaji semula secara tetap.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan aktiviti pentadbir sistem direkod, dikawal dan di pantau berkala	• 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	**Penyegerakan 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 prosedur kawalan ke atas perisian dibangunkan	• GPKTMK 12.5: Kawalan Ke atas Perisian Pengoperasian • *Manual installation*
	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)

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 • Garis Panduan Kawalan Instalasi Perisian (UPM/ISMS/SOK/GP06/INSTALASI PERISIAN) • *Manual installation*

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	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	YA	YA	Memastikan keperluan audit dan aktiviti yang melibatkan pengesahan terhadap sistem operasi perlu dirancang dan bersetuju untuk mengurangkan gangguan kepada proses bisnes	• GPKTMK 12.7: Kawalan Audit Sistem Maklumat • Audit Dalaman ISMS
A.13 COMMUNICATION SECURITY	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/

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
							/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 dimasukkan dalam perjanjian perkhidmatan rangkaian, sama ada perkhidmatan ini disediakan secara dalaman atau oleh khidmat luaran.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Tidak melibatkan Internet service provider. Hanya menggunakan intranet (UPMNET)	• KPI iDEC – (Perkhidmatan rangkaian _ketersediaan rangkaian & jaminan jalur lebar) • Kontrak sambungan WAN 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**					
	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 melalui penggunaan semua jenis kemudahan komunikasi.	Peneraju ISMS	YA	YA	Memastikan polisi dan kawalan terhadap pemindahan maklumat perlu disediakan	• Prosedur Pertukaran Maklumat (UPM/ISMS/SOK/P002) • GPKTMK 13.3 : Pengurusan Pertukaran 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.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 • Prosedur Pertukaran Maklumat (UPM/ISMS/SOK/P002) • Peraturan Kewangan
	A.13.2.3	**Pesanan elektronik** Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan kawalan terhadap mesej elektronik dibangunkan	• GPKTMK Perkara 13.3 (b): Pengurusan Mel Elektronik • Aku Janji Staf • Akta Rahsia Rasmi 1972

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 • Akta Arkib Negara • Aku Janji Staf • GPKTMK Perkara 15.1 : Pihak Ketiga • *Non Discloser Aggreement* (NDA) • Borang Permohonan Data (OPR/PEND/BR01/DATA). Bahagian D:Perakuan Pemohon dan Pengesahan Ketua PTJ/Ketua Jabatan untuk Sokongan
A.14 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE	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	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**					
		dalam keperluan untuk 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 • Perlaksanaan *Network Authentication* UPM https://authenticate.upm.edu.my/
	A.14.1.3	**Melindungi transaksi perkhidmatan aplikasi** Maklumat yang terlibat	Pusat Pembangunan Maklumat dan	YA	YA	Memastikan maklumat yang terlibat dalam transaksi perkhidmatan	• GPTMK 14.1 (c) – Melindungi Transaksi Perkhidmatan Aplikasi • Perlakanaan *Secure Socket Layer-SSL* di

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
		dalam transaksi perkhidmatan aplikasi hendaklah dilindungi bagi mengelakkan penghantaran tidak sempurna, salah hala, pindaan mesej tanpa kebenaran, pendedahan tanpa kebenaran, duplikasi atau ulang tayang mesej tanpa kebenaran.	Komunikasi			aplikasi dilindungi untuk menghalang penghantaran yang tidak lengkap, tersalah laluan , pengubahan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan , duplikasi mesej yang tidak dibenarkan atau ulangan	Sistem Aplikasi
	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	• 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 • 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 • 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) • Kontrak Dokumen • 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.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	• 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)

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	**Data ujian** Memastikan perlindungan bagi data yang digunakan untuk pengujian.					
	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 • Garis Panduan Penggunaan Data Pengujian (UPM/ISMS/SOK/GP15/DATA PENGUJIAN)
A.15 SUPPLIER RELATIONSHIP	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	Peneraju ISMS	YA	YA	Memastikan keperluan keselamatan maklumat didokumenkan dan dipersetujui oleh pihak pembekal	• Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan komunikasi 2014) Bhgn F, 16 (c) • GPKTMK Perkara 15.1 : Pihak Ketiga • Prosedur Perolehan Universiti (UPM/SOK/KEW-BUY/P016) • 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**					
		pembekal dan didokumenkan.					
	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	• Dokumen Perjanjian antara UPM dan Pihak Pembekal

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 Semakan Perjanjian
	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	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**					
		perkhidmatan pembekal secara tetap.					
	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 INFORMATION SECURITY INCIDENT MANAGEMENT	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.	Pejabat Strategi Korporat Komunikasi & 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 Kesinambungan Perkhidmatan (PKP) • 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.	Pejabat Strategi Korporat dan Komunikasi & Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan insiden keselamatan dilapor dengan cepat melalui saluran pengurusan yang betul	• Pelan Kesinambungan Perkhidmatan (PKP) • Pelan Pemulihan Bencana ICT (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.	Pejabat Strategi Korporat dan Komunikasi & Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan staf dan pembekal melaporkan kelemahan keselamatan yang terdapat pada sistem atau perkhidmatan	• Pelan Kesinambungan Perkhidmatan (PKP) • Pelan pemulihan Bencana ICT (DRP ICT) • 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.	Pejabat Strategi Korporat dan Komunikasi & Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan insiden keselamatan dinilai dan diputuskan sekiranya diklasifikasikan sebagai insiden keselamatan maklumat	• Pelan Kesinambungan Perkhidmatan (PKP) • Pelan pemulihan Bencana ICT (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.16.1.5	**Tindak balas terhadap insiden keselamatan maklumat** Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan.	Pejabat Strategi Korporat dan Komunikasi & Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan pengurusan insiden keselamatan mengikut prosedur	• Pelan Kesinambungan Perkhidmatan (PKP) • Pelan pemulihan Bencana ICT (DRP ICT) • 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.	Pejabat Strategi Korporat dan Komunikasi & 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 Kesinambungan Perkhidmatan (PKP) • Pelan Pemulihan Bencana ICT (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.	Pejabat Strategi Korporat dan Komunikasi & Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan pengenalpastian, pengumpulan dan pemuliharaan maklumat perlu dilaksanakan sebagai bukti tindakan	• Pelan Kesinambungan Perkhidmatan (PKP) • Pelan pemulihan Bencana ICT (DRP ICT) • Garis Panduan Pengendalian Insiden ICT (UPM/ISMS/OPR/GP18/ PENGENDALIAN INSIDEN)
INFROMATION SECURITY ASPECTS OF BUSINESS CONTINUITY	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	Pejabat Strategi Korporat dan Komunikasi & Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan keperluan kesinambungan pengurusan keselamatan maklumat	• Pelan Kesinambungan Perkhidmatan • Pelan Pemulihan Bencana ICT (DRP ICT)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
		maklumat dalam keadaan yang menjejaskan, contohnya, semasa krisis atau bencana.					
	A.17.1.2	**Pelaksanaan kesinambungan keselamatan maklumat** Organisasi hendaklah mewujudkan, mendokumenkan, melaksanakan dan menyenggarakan proses, prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan.	Pejabat Strategi Korporat dan Komunikasi & Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan prosedur dan kawalan bagi kesinambungan perkhidmatan dibangun dan didokumenkan	• Pelan Kesinambungan Perkhidmatan • Pelan Pemulihan Bencana ICT (DRP ICT)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
	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 & 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 (MS33) • Pelan Kesinambungan Perkhidmatan • Pelan Pemulihan Bencana ICT (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.	Pusat Pembangunan Maklumat dan Komunikasi	YA	YA	Memastikan fasiliti pemprosesan dibangunkan bagi memenuhi keperluan ketersediaan maklumat	• Pelan Kesinambungan Perkhidmatan • Pelan pemulihan Bencana ICT (DRP ICT)
A.18 COMPLIANCE	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 berkaitan dan pendekatan organisasi bagi memenuhi	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

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
		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.	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) Perkara 12 : Perlindungan Hak Cipta dan Pelesenan • Jawatankuasa Teknologi Maklumat dan Komunikasi UPM
	A.18.1.3	**Perlindungan rekod** Rekod perlu dilindungi daripada kehilangan, kemusnahan, pemalsuan, akses tanpa izin dan	Peneraju ISMS	YA	YA	Memastikan rekod perlu di lindungi daripada kehilangan, kemusnahan, pemalsuan, akses tanpa kebenaran, peraturan,	• GPKTMK Perkara 8.3 (c) : Keselamatan Dokumen • Prosedur Pengurusan Dokumen ISO (UPM/PGR/P001) • Akta Arkib Negara 2003 (Akta 629)

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
		pengeluaran tanpa kebenaran, mengikut keperluan undang-undang, kawal selia, kontrak dan perniagaan.				kontra atau keperluan bisnes	
	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.	Pejabat Pendaftar & Peneraju ISMS	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) Perkara 21 : Kawalan Kriptografi • GPKTMK Perkara 10.0 : Kawalan Kriptografi • 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.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

PENYATA PEMAKAIAN
(*STATEMENT OF APPLICABILITY*)
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**					
	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.	Pusat Jaminan Kualiti	YA	YA	Memastikan sistem maklumat hendaklah dikaji semula secara berkala untuk mematuhi dasar dan standard keselamatan keselamatan maklumat organisasi.	• Jawatankuasa Kajian Semula Pengurusan (MKSP) • Jawatankuasa Kualiti