1.0 PENGENALAN

Dokumen Penyata Pemakaian (*Statement of Applicability (*SoA)) menggariskan objektif kawalan dan kawalan di Annex A dalam Standard MS ISO/IEC 27001:2022 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 27001:2022.

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

(i) Menyenaraikan semua objektif kawalan dan kawalan di Annex A dalam Standard MS ISO/IEC 27001:2022;

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

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

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

(v) Memberi jawapan **"Tidak"** kepada objektif kawalan dan kawalan yang **tidak jelas atau belum dinilai lagi** 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 dikemas kini dengan mengambil kira 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 jelas atau belum dinilai lagi** diberikan alasan pengecualiannya bagi memastikan suatu kawalan tidak sengaja diabaikan.

Lampiran A: SoA Pensijilan MS ISO/IEC 27001:2022 ISMS Universiti Putra Malaysia

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
5: ORGANIZATIONAL CONTROL							
A.5.1	**Policies for information security** Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	5.1.1 Dasar Keselamatan Maklumat	Pusat Jaminan Kualiti	YA	**Optimized**	Memastikan kawalan keselamatan maklumat dibangunkan dan disahkan oleh Pengurusan Atasan dan disampaikan kepada umum.	Dasar ISMS UPM - diluluskan oleh Pengerusi Lembaga Pengarah Universiti. - dikomunikasi menerusi Portal eISO UPM.
		5.1.2 Kajian Semula Dasar unutk Keselamatan Maklumat	Pusat Jaminan Kualiti	YA	**Optimized**	Memastikan dasar sentiasa terkini berdasarkan skop dan pelaksanaan ISMS	Semakan berkala dilaksanakan semasa Mesyuarat Kajian Semula Pengurusan ISMS UPM.
		6.1.2 Pengasingan Tugas	Peneraju ISMS & Pejabat Pendaftar	YA	**Optimized**	Memastikan kawalan keselamatan maklumat dibangunkan dan disahkan oleh Pengurusan Atasan dan disampaikan kepada umum.	• Senarai tugas Akademik/Bukan Akademik/Pelaksana termasuk tugas pentadbiran. (Contoh: sebagai Dekan, Pengetua Kolej, Pengarah, Penolong Pengarah/Timbalan Pengarah). • Deskripsi tugas setiap pekerja UPM. • Struktur organisasi PTJ.

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
							• Kemas kini Deskripsi Tugas dalam HR Portal.
		6.1.3 Hubungan dengan Pihak Berkuasa	Peneraju ISMS		**Optimized**	Memastikan hubungan dengan pihak berkuasa berkaitan dikekalkan bagi permohonan pelesenan perkhidmatan	• Akta Perubatan 1971. • Akta Perlesenan Tenaga Atom 1984 (Akta 304). • Seksyen 66 Akta Imigresen 1969/63 (Akta 155) Malaysian Medical Council (PERINGATAN TEGAS KEPADA SEMUA PENGAMAL PERUBATAN UNTUK MEMPERBAHARUI PERAKUAN AMALAN TAHUNAN (PAT). • Akta Profesion Kesihatan Bersekutu 2016 (Akta 774). • Akta Jururawat 1950 (Akta 14). • Akta Jururawat 1950 – Peraturan Pendaftaran Jururawat 1985.
A.5.2	**Information security roles and responsibilities**	6.1.1 Peranan dan Tanggungjawab	Pusat Jaminan Kualiti	YA	**Optimized**	Memastikan semua tanggungjawab keselamatan maklumat	Peranan dan Tanggungjawab Jawatankuasa Keselamatan

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
	Information security roles and responsibilities shall be defined and allocated according to the organization needs.	Keselamatan Maklumat				ditakrifkan dan diperuntukkan.	Maklumat UPM - menerusi Portal eISO UPM.
A.5.3	**Segregation of duties** Conflicting duties and conflicting areas of responsibility shall be seg- regated.	6.1.2 Pengasingan Tugas	Peneraju ISMS & Pejabat Pendaftar	YA	**Optimized**	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). • Deskripsi tugas setiap pekerja UPM. • Struktur organisasi PTJ Kemas kini Deskripsi Tugas dalam HR Portal.
A.5.4	**Management responsibilities** Management shall require all personnel to apply information	7.2.1 Tanggungjawab pengurusan	Pejabat Pendaftar & Pejabat Bursar	YA	**Optimized**	Memastikan polisi dan prosedur keselamatan maklumat yang telah ditetapkan oleh organisasi	• Perintah Am. • Peraturan Kewangan.

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
	security in accordance with the established information security policy, topic-specific policies and procedures of the organization.					diikuti oleh pekerja dan pembekal.	• Dokumen Perjanjian dengan Pembekal/Kontraktor/Pihak Ketiga. • Surat Aku Janji. • Borang Perakuan untuk Ditandatangani oleh Penjawat Awam Berkenaan Akta Rahsia Rasmi 1972 (SOK/BUM/BR03/AKTA RAHSIA RASMI).
A.5.5	**Contact with authorities** The organization shall establish and maintain contact with relevant authorities.	6.1.3 Hubungan dengan pihak berkuasa	Peneraju ISMS	YA	**Optimized**	Memastikan hubungan dengan pihak berkuasa berkaitan dikekalkan.	• Akta Universiti dan Kolej Universiti 1971. • Malaysian Medical Council Lembaga Jururawat Malaysia. • Kementerian Kesihatan Malaysia. • Jabatan Tenaga Atom, Kementerian Sains, Teknologi dan Komunikasi. • Jabatan Imigresen Malaysia Perlembagaan Universiti Putra Malaysia (P.U.(A) 448/2010). • Arahan Perbendaharan (Pindaan 2023).

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
A.5.6	**Contact with special interest groups** The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	6.1.4 Hubungan dengan kumpulan berkepentingan yang khusus	Peneraju ISMS	YA	**Optimized**	Memastikan hubungan dengan pihak kepentingan atau lain-lain forum keselamatan dan persatuan profesional dikekalkan.	• Pelan Kesinambungan Perkhidmatan (PKP). • Pelan Komunikasi Krisis. • Garis Panduan Pengendalian Insiden ICT (iDEC/ISMS/GP02). • Pelan Pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT). • Pengauditan OSHA. • MyCert. • Cybersecurity Malaysia.
A.5.7	**Threat intelligence** Information relating to information security threats shall be collected and analysed to produce threat intelligence.		Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Keperluan subscription pangkalan data Threat Intelligence kepada peralatan keselamatan ICT seperti Firewall.	Dokumen ketersediaan *threat intelligence* peralatan keselamatan ICT seperti Firewall dan Web Application Firewall.
A.5.8	**Information security in project management** Information security shall be integrated into project management.	6.1.5 Keselamatan maklumat dalam pengurusan projek	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan keselamatan maklumat dalam pengurusan projek yang terlibat dalam skop pensijilan dikawal.	Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001).
		14.1.1 Analisis dan spesifikasi keperluan keselamatan maklumat	Peneraju ISMS	YA	**Optimized**	Memastikan keperluan keselamatan maklumat perlu dimasukkan ke dalam	Prosedur Perolehan Universiti (UPM/SOK/KEW-BUY/P016).

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
						sistem baharu atau sistem sedia ada.	
A.5.9	**Inventory of information and other associated assets** An inventory of information and other associated assets, including owners, shall be developed and maintained.	8.1.1 Inventori Aset	Peneraju ISMS & Pejabat Bursar	YA	**Optimized**	Memastikan aset yang terlibat dengan fasiliti pemprosesan maklumat dikenalpasti dan inventori aset tersebut disedia dan diselenggara.	• Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian D. • GPKTMK versi 6.0 para 8.0: Pengurusan Aset. • Prosedur Pengurusan Aset Alih (UPM/SOK/KEW-AST/P012).
		8.1.2 Pemilikan Aset	Peneraju ISMS & Pejabat Bursar	YA	**Optimized**	Memastikan setiap aset yang diselenggara mempunyai pemilik	• Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian D. • GPKTMK versi 6.0 para 8.0: Pengurusan Aset. Prosedur Pengurusan Aset Alih (UPM/SOK/KEW-AST/P012).
A.5.10	**Acceptable use of information and other associated assets** Rules for the acceptable use and procedures for handling information and other associated assets	8.1.3 Penggunaan Aset yang Dibenarkan	Peneraju ISMS & Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan peraturan untuk kebolehgunaan maklumat dan aset yang berkaitan dengan kemudahan pemprosesan maklumat dan maklumat itu dikenal pasti,	• Kaedah-Kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian F. • GPKTMK versi 6.0 para 8.2 Pengelasan dan Pengendalian Maklumat.

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
	shall be identified, documented and implemented.					didokumen dan dilaksanakan.	• Garis Panduan Pengurusan Data Strategik UPM. • Garis Panduan Permohonan Maklumat Rasmi UPM.
		8.2.3 Pengendalian Aset	Peneraju ISMS	YA	**Optimized**	Memastikan prosedur pengendalian aset dibangun dan dilaksanakan mengikut skema klasifikasi maklumat oleh organisasi.	• Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian D. • GPKTMK versi 6.0 para 8.0 Pengurusan Aset. • Prosedur Pengurusan Aset Alih (UPM/SOK/KEW-AST/P012). • Garis Panduan Pengendalian Maklumat (iDEC/ISMS/GP01).
A.5.11	**Return of assets** Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their	8.1.4 Pemulangan Aset	Peneraju ISMS, Pejabat Pendaftar & Pejabat Bursar	YA	**Optimized**	Memastikan aset organisasi dipulangkan selepas tamat perkhidmatan.	• Perintah–perintah Am Persekutuan Bab A: Peraturan-Peraturan Pegawai Awam (Pelantikan, Kenaikan Pangkat Dan Penamatan Perkhidmatan) 2012.

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
	employment, contract or agreement.						• 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).
A.5.12	**Classification of information** Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	8.2.1 Pengelasan Maklumat	Peneraju ISMS & Pejabat Pendaftar	YA	**Optimized**	Memastikan maklumat dikelaskan untuk mengelak daripada pendedahan atau pengubahsuaian yang tidak dibenarkan.	• Arahan Keselamatan Kerajaan Malaysia. Akta Arkib Negara 2003 (Akta 629). • GPKTMK versi 6.0 para 8.2 Pengelasan dan Pengendalian Maklumat. • Garis Panduan Pengurusan Keselamatan Perlindungan Dokumen Rasmi Universiti Putra Malaysia. • Garis Panduan Pengendalian Maklumat (iDEC/ISMS/GP01).

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
A.5.13	**Labelling of information** An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information clas-sification scheme adopted by the organization.	8.2.2 Pelabelan Maklumat	Peneraju ISMS & Pejabat Pendaftar	YA	**Optimized**	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 versi 6.0 para 8.2 Pengelasan dan Pengendalian Maklumat. • Garis Panduan Pengurusan Keselamatan Perlindungan Dokumen Rasmi Universiti Putra Malaysia. • Garis Panduan Pengendalian Maklumat (iDEC/ISMS/GP01).
A.5.14	**Information transfer** Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the	13.2.1 Dasar dan prosedur pemindahan maklumat	Peneraju ISMS	YA	**Optimized**	Memastikan polisi dan kawalan terhadap pemindahan maklumat perlu disediakan.	• Akta Rahsia Rasmi 1972. GPKTMK versi 6.0 para 13.3 : Pengurusan Perpindahan dan Pertukaran Maklumat. Prosedur Pertukaran Maklumat (UPM/ISMS/SOK/P002). • Garis Panduan Pengendalian Maklumat (iDEC/ISMS/GP01).

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
	organization and other parties.						• Aku Janji dan Akuan Penerimaan Data Calon Jaya.
		13.2.2 Perjanjian tentang pemindahan maklumat	Peneraju ISMS & Pejabat Bursar	YA	**Optimized**	Memastikan kontrak perjanjian memenuhi keperluan keselamatan penghantaran maklumat di antara pembekal dan organisasi.	• GPKTMK versi 6.0 para 13.3(a): Perpindahan atau Pertukaran Maklumat. • Dokumen Perjanjian dengan Pembekal/Kontraktor/Pihak Ketiga. • Prosedur Pertukaran Maklumat (UPM/ISMS/SOK/P002).
		13.2.3 Pesanan elektronik	Pusat Pembangunan Maklumat dan Komunikasi, Pejabat Pendaftar & Pusat Strategi dan Perhubungan Korporat	YA	**Optimized**	Memastikan kawalan terhadap pesanan elektronik dibangunkan.	• Akta Rahsia Rasmi 1972. • Akta Komunikasi dan Multimedia 1998 (Akta 588). Kaedah-Kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian F. • GPKTMK versi 6.0 para 13.3 (b): Pengurusan Mel Elektronik (e-Mel). Garis Panduan E-mel UPM versi 4.0. • Garis Panduan Media UPM.

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
							• Panduan Amalan Komunikasi Berkesan. Surat Aku Janji.
A.5.15	**Access control** Rules to control physical and logical access to information and other associated assets shall be established and implemented based on busi- ness and information security requirements.	9.1.1 Dasar Kawalan Akses	Peneraju ISMS	YA	**Optimized**	Dasar kawalan capaian hendaklah diwujudkan, didokumen dan dikaji semula berdasarkan keperluan keselamatan perniagaan dan maklumat.	• Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE-LEAD/AK01). • Arahan Keselamatan: Keselamatan Fizikal. GPKTMK versi 6.0 para 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).
		9.1.2 Akses kepada Rangkaian dan Perkhidmatan Rangkaian	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan pengguna mempunyai akses kepada perkhidmatan rangkaian yang telah dikhususkan kepada mereka.	• GPKTMK versi 6.0 para 13.2 : Keselamatan Perkhidmatan Rangkaian. • Garis Panduan Pengurusan Pengagihan Rangkaian (UPM/ISMS/OPR/GP13/ AGIHAN RANGKAIAN).

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
A.5.16	**Identity management** The full life cycle of identities shall be managed.	9.2.1 Pendaftaran dan Pembatalan Pengguna	Peneraju ISMS	YA	**Optimized**	Memastikan proses pendaftaran dan pembatalan pengguna dilaksanakan untuk membolehkan pemberian hak akses.	• GPKTMK versi 6.0 para 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-LEAD/AK01). • Garis Panduan Pengurusan Identiti Pengguna ID eKlinik (OPR/PKU/GP13/EKLINIK-ID). • Buku Panduan Perkhidmatan Perubatan Pusat Kesihatan Universiti. • Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/ GP06/PEMANTAUAN CAPAIAN). • Garis Panduan Pengurusan Identiti

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
							(UPM/ISMS/SOK/GP07/ IDENTITI). • Garis Panduan Pengurusan Identiti Pengguna (ID) Sistem Maklumat Pelajar. Garis Panduan Pengurusan Identiti Pengguna ID eKlinik (OPR/PKU/GP13/EKLINIK-ID). • Buku Panduan Perkhidmatan Perubatan Pusat Kesihatan Universiti. • Borang Permohonan ID PutraENROLL (Peranan Pentadbir). Garis Panduan Pengurusan Identiti Pengguna PutraENROLL.
A.5.17	**Authentication information** Allocation and management of authentication information shall be controlled by a management process,	9.2.4 Pengurusan Maklumat Pengesahan Rahsia Pengguna	Peneraju ISMS, Pejabat Pendaftar & Bahagian Kemasukan dan Bahagian Urus Tadbir Akademik	YA	**Optimized**	Memastikan pengesahan maklumat rahsia sentiasa dikawal.	• GPKTMK versi 6.0 para 10.0: Kriptografi. • Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE-LEAD/AK01). • Garis Panduan Pengurusan UPM-ID

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
	including advising personnel on appropriate handling of authentication information.						(UPM/ISMS/OPR/GP16/UPM-ID). • Borang Permohonan ID HRPORTAL. • Garis Panduan Pengurusan Identiti Pengguna (ID) Sistem Maklumat Pelajar.
		9.3.1 Penggunaan Maklumat Pengesahan Rahsia	Peneraju ISMS & Pejabat Pendaftar	YA	**Optimized**	Memastikan pengguna mengikut semua amalan yang telah ditetapkan dalam pengesahan maklumat.	• GPKTMK versi 6.0 para 10.0: Kriptografi. • Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/ IDENTITI). • Garis Panduan Pengurusan UPM-ID (UPM/ISMS/OPR/GP16/ UPM-ID). • Surat Aku Janji. • Garis Panduan Pengurusan Keselamatan Perlindungan Dokumen Rasmi Universiti Putra Malaysia.

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
		9.4.3 Sistem Pengurusan Kata Laluan	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan sistem pengurusan kata laluan adalah interaktif dan kata laluan berkualiti.	• GPKTMK versi 6.0 para 9.2 : Penyediaan dan Semakan Capaian Pengguna. • Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/ IDENTITI). • Garis Panduan Pengurusan Identiti Pengguna (ID) Sistem Maklumat Pelajar. • Garis Panduan Pengurusan UPM-ID (UPM/ISMS/OPR/GP16/ UPM-ID).
A.5.18	**Access rights** Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	9.2.2 Peruntukan Akses Pengguna	Peneraju ISMS	YA	**Optimized**	Memastikan hak capaian pengguna disemak semula.	• GPKTMK versi 6.0 para 9.2: Penyediaan dan Semakan Capaian Pengguna. • Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/GP06/ PEMANTAUAN CAPAIAN). • Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/ IDENTITI).

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
							• Garis Panduan Pengurusan Identiti Pengguna (ID) Sistem Maklumat Pelajar. • Garis Panduan Pengurusan PutraENROLL (ID) Sistem Maklumat Pelajar. • Borang Permohonan ID PutraENROLL (Peranan Pentadbir). • Garis Panduan Pengurusan Identiti Pengguna PutraENROLL.
		9.2.5 Kajian Semula Hak Akses Pengguna	Peneraju ISMS & Pejabat Pendaftar	YA	**Optimized**	Memastikan hak capaian pengguna disemak semula.	• Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE-LEAD/AK01). • Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR /GP06/PEMANTAUAN CAPAIAN). • Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/ IDENTITI).

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
							• Garis Panduan Pengurusan Identiti Pengguna (ID) Sistem Maklumat Pelajar. Garis Panduan Pengurusan Identiti Pengguna ID eKlinik (OPR/PKU/GP13/EKLINIK-ID). • Semakan semula ID pengguna HRPORTAL dilaksanakan sekurang-kurangnya setahun sekali. • Garis Panduan Pengurusan Identiti Pengguna PutraENROLL.
		9.2.6 Penyingkiran atau Pelarasan hak Akses	Peneraju ISMS	Y	**Optimized**	Memastikan hak akses kepada maklumat dan kemudahan dikeluarkan selepas tamat perkhidmatan atau apabila berlaku perubahan.	• GPKTMK versi 6.0 para 9.2 : Penyediaan dan Semakan Capaian Pengguna. • Prosedur Kawalan dan Pemantauan Capaian ke Sistem di Pusat Data (UPM/ISMS/OPR/P003). • Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE-LEAD /AK01). • Garis Panduan Pemantauan Capaian Ke Sistem

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
							(UPM/ISMS/OPR/GP06/ PEMANTAUAN CAPAIAN). • Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/ IDENTITI). • Garis Panduan Pengurusan Identiti Pengguna (ID) Sistem Maklumat Pelajar. • Garis Panduan Pengurusan Identiti Pengguna ID eKlinik (OPR/PKU/GP13/EKLINIK-ID). • Borang Permohonan ID PutraENROL (Peranan Pentadbir). • Garis Panduan Pengurusan Identiti Pengguna PutraENROLL.

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
A.5.19	**Information security in supplier relationships** Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	15.1.1 Dasar keselamatan maklumat untuk hubungan pembekal	Peneraju ISMS	YA	**Optimized**	Memastikan keperluan keselamatan maklumat didokumenkan dan dipersetujui oleh pihak pembekal.	• Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian F, Klausa 16 (c). • GPKTMK versi 6.0 para 15.1: Pihak Ketiga. • Prosedur Perolehan Universiti (UPM/SOK/KEW-BUY/P016). • Surat Aku Janji Pihak Luar. Kontrak Bekalan/Perkhidmatan.
A.5.20	**Addressing information security within supplier agreements** Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	15.1.2 Menangani keselamatan dalam perjanjian pembekal	Peneraju ISMS	YA	**Optimized**	Memastikan keperluan keselamatan maklumat dibangunkan dan dipersetujui oleh pihak pembekal.	• Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian F, Klausa 16 (c). • GPKTMK versi 6.0 para 15.1: Pihak Ketiga. • Dokumen Perjanjian antara UPM dan Pihak Pembekal. • Surat Aku Janji Pihak Luar.

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
A.5.21	**Managing information security in the information and communication technology (ICT) supply-chain** Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	15.1.3 Rantaian bekalan teknologi maklumat dan komunikasi	Pejabat Bursar & Pejabat Penasihat Undang-Undang	YA	**Optimized**	Memastikan dokumen perjanjian antara pihak pembekal memenuhi keperluan keselamatan maklumat.	• GPKTMK versi 6.0 para 15.1: Pihak Ketiga. • Senarai Semak Surat Cara Undang-undang (Perjanjian/Persefahaman). • Dokumen Perjanjian dengan Pembekal/Kontraktor/Pihak Ketiga.
A.5.22	**Monitoring, review and change management of supplier services** The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	15.2.1 Memantau dan mengkaji semula perkhidmatan pembekal	Pejabat Bursar	YA	**Optimized**	Memastikan pemantauan, semakan terhadap penerimaan perkhidmatan pembekal dijalankan secara berkala.	• GPKTMK versi 6.0 para 15.2: Pengurusan Penyampaian Perkhidmatan Pihak Ketiga. • Arahan Kerja Penilaian Prestasi Syarikat (UPM/SOK/KEW/AK002/BUY).
		15.2.2 Menguruskan perubahan kepada perkhidmatan pembekal	Pejabat Bursar & Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan polisi, prosedur dan kawalan bagi mengurus perubahan penyediaan perkhidmatan dilaksanakan.	• GPKTMK versi 6.0 para 15.2: Pengurusan Penyampaian Perkhidmatan Pihak Ketiga. • Dokumen Perjanjian dengan Pembekal/Kontraktor/Pihak Ketiga.

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
A.5.23	**Information security for use of cloud services** Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.		Pusat Pembangunan Maklumat dan Komunikasi, Pejabat Pendaftar	YA	**Optimized**	Bertujuan menjelaskan dasar berhubung penggunaan perkhidmatan pengkomputeran awan kepada sektor awam.	Pekeliling Bilangan 1 Tahun 2021 Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam.
A.5.24	**Information security incident management planning and preparation** The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	16.1.1 Tanggungjawab dan prosedur	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan prosedur dan tanggungjawab pengurusna 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 (IDEC/ISMS/GP02).

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
A.5.25	**Assessment and decision on information security events** The organization shall assess information security events and decide if they are to be categorized as information security incidents.	16.1.4 Penilaian dan keputusan tentang kejadian keselamatan maklumat	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	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 (IDEC/ISMS/GP02).
A.5.26	**Response to information security incidents** Information security incidents shall be responded to in accordance with the documented procedures.	16.1.5 Tindak balas terhadap insiden keselamatan maklumat	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	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 (IDEC/ISMS/GP02).
A.5.27	**Learning from information security incidents** Knowledge gained from information security incidents shall be used to strengthen and improve	16.1.6 Mempelajari daripada insiden keselamatan maklumat	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	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 (IDEC/ISMS/GP02).

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
	the information security controls.						
A.5.28	**Collection of evidence** The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	16.1.7 Pengumpulan bahan bukti	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan pengenalpastian, pengumpulan dan pemuliharaan maklumat perlu dilaksanakan sebagai bukti tindakan.	• GPKTMK versi 6.0 para 12.4: *Logging* dan Pemantauan. • Pelan pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT). • Garis Panduan Pengendalian Insiden ICT (IDEC/ISMS/GP02).
A.5.29	**Information security during disruption** The organization shall plan how to maintain information security at an appropriate level during disruption.	17.1.1 Perancangan kesinambungan keselamatan maklumat	Pejabat Pengurusan Keselamatan dan Kesihatan Pekerjaan & Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan keperluan kesinambungan pengurusan keselamatan maklumat.	• GPKTMK versi 6.0 para 17.0 – Pengurusan Kesinambungan Perkhidmatan. • Pelan Kesinambungan Perkhidmatan. • Pelan Pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT).
		17.1.2 Pelaksanaan kesinambungan keselamatan maklumat	Pejabat Pengurusan Keselamatan dan Kesihatan Pekerjaan & Pusat	YA	**Optimized**	Memastikan prosedur dan kawalan bagi kesinambungan perkhidmatan dibangun dan didokumenkan.	• GPKTMK versi 6.0 para 17.0 – Pengurusan Kesinambungan Perkhidmatan. • Pelan Kesinambungan Perkhidmatan. • Pelan Pemulihan Bencana ICT

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
			Pembangunan Maklumat dan Komunikasi				Universiti Putra Malaysia (DRP ICT).
		17.1.3 Menentusahkan, mengkaji semula dan menilai kesinambungan keselamatan maklumat	Pejabat Pengurusan Keselamatan dan Kesihatan Pekerjaan & Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan maklumat kawalan kesinambungan keselamatan disahkan dan dilaksanakan secara berkala untuk memastikan ia berkesan sekiranya berlaku bencana.	• GPKTMK versi 6.0 para 17.0 – Pengurusan Kesinambungan Perkhidmatan. • Pelan Kesinambungan Perkhidmatan. • Pelan Pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT). • Laporan Pengujian Simulasi DRP ICT UPM.
A.5.30	**ICT readiness for business continuity** ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	A.17 Aspek keselamatan maklumat bagi pengurusan kesinambungan perniagaan	Pejabat Pengurusan Keselamatan dan Kesihatan Pekerjaan & Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam keadaan yang menjejaskan, contohnya, semasa krisis atau bencana.	• GPKTMK versi 6.0 para 17.0 – Pengurusan Kesinambungan Perkhidmatan. • Pelan Kesinambungan Perkhidmatan. • Pelan Pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT).

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
A.5.31	**Legal, statutory, regulatory and contractual requirements** Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	18.1.1 Pengenalpastian keperluan undang-undang dan kontrak terpakai	Pejabat Penasihat Undang-Undang	YA	**Optimized**	Memastikan keperluan perundangan dikenal pasti dan didokumenkan serta dikemaskini.	• GPKTMK versi 6.0 para 18.1 (d): Keperluan Perundangan. • Senarai Undang-undang sedia ada melalui Portal eISO.
		18.1.5 Peraturan kawalan kriptografi	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan kawalan kriptografi digunakan dengan mematuhi semua perjanjian berkenaan, undang-undang dan peraturan.	• Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian G, Klausa 21. • GPKTMK versi 6.0 para 10.0: Kriptografi. • Garis Panduan Pengendalian Maklumat (iDEC/ISMS/GP01).
A.5.32	**Intellectual property rights** The organization shall implement appropriate procedures to protect intellectual property rights.	18.1.2 Hak harta intelek	Peneraju ISMS & Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan polisi dan kawalan bagi pematuhan perundangan dilaksanakan.	• Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan komunikasi) 2014, Bahagian E, Klausa 12. • Kaedah- kaedah Universiti Putra Malaysia (Harta Intelek dan Eksploitasi Komersial) 2022. • Jawatankuasa Teknologi

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
							Maklumat dan Komunikasi UPM. • Dokumen Perjanjian dengan Pembekal/Kontraktor/Pihak Ketiga.
A.5.33	**Protection of records** Records shall be protected from loss, destruction, falsification, unau- thorized access and unauthorized release.	18.1.3 Perlindungan rekod	Peneraju ISMS	YA	**Optimized**	Memastikan rekod perlu dilindungi daripada kehilangan, kemusnahan, pemalsuan, akses tanpa kebenaran, peraturan, kontra atau keperluan bisnes.	• Akta Arkib Negara 2003 (Akta 629). • GPKTMK versi 6.0 para 8.3 (c) : Keselamatan Dokumentasi Sistem. • Prosedur Pengurusan Dokumen ISO (UPM/PGR/P001). • Dasar Universiti Putra Malaysia (Pengurusan Rekod dan Pentadbiran Arkib) 2023. • Garis Panduan Pengurusan Rekod dan Pentadbiran Arkib Universiti Putra Malaysia. • Garis Panduan Pengurusan Keselamatan Perlindungan Dokumen Rasmi Universiti Putra Malaysia. • Panduan Pengurusan Fail dan Rekod Universiti.

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
A.5.34	**Privacy and protection of personal identifiable information (PII)** The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	18.1.4 Privasi dan perlindungan maklumat peribadi	Peneraju ISMS & Pejabat Pendaftar	YA	**Optimized**	Memastikan perlindungan terhadap maklumat peribadi memenuhi keperluan perundangan berkaitan.	• GPKTMK versi 6.0 para 13.3: Pengurusan Perpindahan atau Pertukaran Maklumat. • Prosedur Pengurusan Dokumen ISO (UPM/PGR/P001). • Prosedur Pertukaran Maklumat. (UPM/ISMS/SOK/P002). • Log Peminjaman Fail Peribadi Staf UPM. • Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE-LEAD/AK01).
A.5.35	**Independent review of information security** The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or	18.2.1 Kajian semula keselamatan maklumat secara berkecuali	Pusat Jaminan Kualiti	YA	**Optimized**	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.

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
	when significant changes occur.						
A.5.36	**Compliance with policies, rules and standards for information security** Compliance with the organization's information security policy, top- ic-specific policies, rules and standards shall be regularly reviewed.	18.2.2 Pematuhan dasar dan standard keselamatan	Pusat Jaminan Kualiti	YA	**Optimized**	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.
		18.2.3 Kajian semula pematuhan teknikal	Peneraju ISMS & Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan sistem maklumat hendaklah dikaji semula secara berkala untuk mematuhi dadar dan standard keselamatan maklumat organisasi.	• Mesyuarat Jawatankuasa Keselamatan Teknologi Maklumat & Komunikasi. • UPM Cert. • Garis Panduan Penilaian Tahap Keselamatan (UPM/ISMS/OPR/GP09/ Tahap Keselamatan).
A.5.37	**Documented operating procedures** Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	12.1.1 Prosedur operasi yang didokumenkan	Pusat Jaminan Kualiti	YA	**Optimized**	Memastikan prosedur operasi didokumen dan disediakan kepada yang memerlukan.	• Prosedur Pengurusan Dokumen ISO (UPM/PGR/P001). • Sistem Pengurusan ISO UPM (e-ISO) - https://reg.upm.edu.my/eISO.

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
6: PEOPLE CONTROLS							
A.6.1	**Screening** Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	7.1.1 Saringan	Pejabat Pendaftar	YA	**Optimized**	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 dan Kumpulan Pelaksana (UPM/SOK/BUM/P001). • GPKTMK versi 6.0 para 7.1: Sebelum Perkhidmatan Surat Tawaran Jawatan Tetap – keperluan tapisan keselamatan Kerajaan Malaysia. • Rekod Kenyataan Perkhidmatan (RKP) bagi calon yang dilantik dari agensi luar.
A.6.2	**Terms and conditions of employment** The employment contractual agreements shall state the personnel's and the organization's	7.1.2 Terma dan syarat perjawatan	Pejabat Pendaftar & Pejabat Bursar	YA	**Optimized**	Memastikan kontrak perjanjian terhadap pekerja dan pembekal menyatakan tanggungjawab organisasi terhadap keselamatan maklumat.	• Prosedur Pendaftaran Syarikat dan Pekerja/Individu (UPM/OPR/BUR-BUY/P003). • Surat Aku Janji. • Borang Pengesahan Lapor Diri (SOK/BUM/BR03/ BORANGPENGESAHAN).

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
	responsibilities for information security.						• Borang Perakuan Untuk Ditandatangani Oleh Penjawat Awam Berkenaan Dengan Akta Rahsia Rasmi 1972 (SOK/BUM/BR03/AKTA RAHSIA RASMI). • Dokumen Perjanjian dengan Pembekal/Kontraktor/Pihak Ketiga.
A.6.3	**Information security awareness, education and training** Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	7.2.2 Kesedaran, pendidikan dan latihan tentang keselamatan maklumat	Peneraju ISMS (Pasukan pendaftaran Pelajar Baharu Prasiswazah – Kampus Serdang & Pasukan Pusat Data, Pasukan Pendaftaran Pelajar Baharu Siswazah), Pejabat Pendaftar, Pejabat Bursar & Pusat Jaminan Kualiti	YA	**Optimized**	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 versi 6.0, para 7.2, Dalam Perkhidmatan Taklimat Keselamatan Maklumat bagi Jawatankuasa Pelaksana Minggu Perkasa Putra. • Taklimat Keselamatan Maklumat dan PutraVid kepada pelajar baharu semasa Minggu Perkasa Putra. ISMS – Latihan/Takwim di bawah Pusat Jaminan Kualiti. • Surat Aku Janji Pihak Luar.

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
							• Arahan Kerja Permohonan Kad Pintar (UPM/OPR/APSEC/AK01/Kad Pintar). • Buku Panduan Pendaftaran Pelajar Baharu Dalam Sistem eDaftar (ebook). • Taklimat Keselamatan Maklumat dan PutraVid kepada pelajar baharu semasa Majlis Ikrar dan Taklimat Pelajar Pascasiswazah. • Perbincangan dan Taklimat Persediaan Minggu Pendaftaran Pelajar Baharu Siswazah UPM. Panduan Pra-Pendaftaran Pelajar Baharu (PutraEnroll).
A.6.4	**Disciplinary process** A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an	7.2.3 Proses Tatatertib	Pejabat Pendaftar	YA	**Optimized**	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 E dan F ● Prosedur Pengurusan

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
	information security policy violation.						Mesyuarat Tatatertib Pekerja (UPM/OPR/PEND/P016)
A.6.5	**Responsibilities after termination or change of employment** Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	7.3.1 Penamatan atau pertukaran tanggungjawab peraturan	Pejabat Pendaftar & Pejabat Bursar	YA	**Optimized**	Memastikan tanggungjawab keselamatan maklumat terhadap pekerja atau pembekal yang telah tamat perkhidmatan atau berlaku perubahan pekerja hendaklah dikenal pasti dan dikuat kuasakan.	• Perintah –perintah Am Persekutuan Bab A : Peraturan-Peraturan Pegawai Awam (Pelantikan, Kenaikan Pangkat Dan Penamatan Perkhidmatan) 2012. • GPKTMK versi 6.0, para 7.3, Bertukar Atau Tamat Perkhidmatan. • Borang Nota Serah Tugas (SOK/BUM/BR03/SERAH TUGAS). • Dokumen Perjanjian dengan Pembekal/Kontraktor/Pihak Ketiga.
A.6.6	**Confidentiality or non-disclosure agreements** Confidentiality or non-disclosure agreements reflecting the organ-ization's needs for the protection of information shall be identified, documented, regularly	13.2.4 Perjanjian kerahsiaan atau ketakdedahan	Pejabat Pendaftar & Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan NDA bagi keperluan melindungi maklumat perlu dikenal pasti, dipantau dan didokumenkan.	• Akta Rahsia Rasmi 1972. Akta Arkib Negara 2003 (Akta 629). • GPKTMK versi 6.0 para 15.1 : Pihak Ketiga Borang Permohonan Data (OPR/PEND/BR01/DATA). Bahagian D:Perakuan Pemohon dan Pengesahan

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
	reviewed and signed by personnel and other relevant interested parties.						Ketua PTJ/Ketua Jabatan untuk Sokongan Non Disclosure Agreement (NDA). • Surat Aku Janji. • Surat Aku Janji Pihak Luar.
A.6.7	**Remote working** Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	6.2.2 Telekerja	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan kawalan capaian kepada sistem (teleworking) oleh pekerja yang dibenarkan sahaja.	• Garis Panduan Pemantauan Capaian ke Sistem (UPM/ISMS/OPR/GP06/ PEMANTAUAN CAPAI) • Arahan Kerja Perkhidmatan Sokongan ICT (UPM/OPR/IDEC/AK31 Perkara 3.2.1 Rangkaian
A.6.8	**Information security event reporting** The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	16.1.2 Pelaporan kejadian keselamatan maklumat	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	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 (IDEC/ISMS/GP02)
		16.1.3 Pelaporan kelemahan keselamatan maklumat	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	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

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
							Insiden ICT (IDEC/ISMS/GP02)
7: PHYSICAL CONTROLS							
A.7.1	**Physical security perimeters** Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	11.1.1 Perimeter keselamatan fizikal	Peneraju ISMS	YA	**Optimized**	Memastikan perimter keselamatan ditentukan dan digunakan untuk melindungi kawasan yang mengandungi maklumat yang sensitif atau kritikal.	● Arahan Keselamatan : Keselamatan Fizikal ● Lokasi Skop Pensijilan ISMS UPM - menerusi Portal eISO UPM ● GPKTMK versi 6.0 para 11.1 (a) : Keselamatan Fizikal Kawasan ● GPKTMK versi 6.0 para 11.1(c) – Kawasan Larangan
A.7.2	**Physical entry** Secure areas shall be protected by appropriate entry controls and access points.	11.1.2 Kawalan kemasukan fizikal	Peneraju ISMS	YA	**Optimized**	Memastikan kawalan bersesuaian dilaksanakan bagi memastikan hanya pengguna yang diberi hak akses sahaja dibenarkan masuk ke dalam kawasan terkawal.	● Arahan Keselamatan : Keselamatan Fizikal ● GPKTMK versi 6.0 para 11.1(b) Kawalan Akses Fizikal ● Lokasi Skop Pensijilan ISMS UPM - menerusi Portal eISO UPM ● Prosedur Kawalan Akses (UPM/OPR/APSeC/P001) ● Prosedur Pengoperasian Pengurusan Pusat Data (UPM/ISMS/OPR/P001) ● Garis Panduan Kawalan Akses ke Pusat Data (UPM/ISMS/OPR/GP03/ KAWALAN AKSES)

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
		11.1.6 Kawasan penyerahan dan pemunggahan	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	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, Bahagian D, Klausa 9 (b) ● GPKTMK versi 6.0 para 11.1 (g) : Kawasan Penghantaran dan Pemunggahan
A.7.3	**Securing offices, rooms and facilities** Physical security for offices, rooms and facilities shall be designed and implemented.	11.1.3 Keselamatan pejabat, bilik dan kemudahan	Peneraju ISMS	YA	**Optimized**	Memastikan keselamatan fizikal direka dan digunakan.	● Arahan Keselamatan : Keselamatan Fizikal ● GPKTMK versi 6.0 para 11.1 (d) – Keselamatan Pejabat, Bilik dan Kemudahan ● Lokasi Skop Pensijilan ISMS UPM - menerusi Portal eISO UPM
A.7.4	**Physical security monitoring** Premises shall be continuously monitored for unauthorized physical access.	A.11 Keselamatan fizikal dan persekitaran	Peneraju ISMS	YA	**Optimized**	Perimeter keselamatan hendaklah ditakrifkan dan digunakan bagi melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat yang sensitif atau kritikal.	Arahan Keselamatan : Keselamatan Fizikal ● Lokasi Skop Pensijilan ISMS UPM - menerusi Portal eISO UPM ● GPKTMK versi 6.0 para 11.1 (a) : Keselamatan Fizikal Kawasan ● GPKTMK versi 6.0 para 11.1(c) – Kawasan Larangan

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
A.7.5	**Protecting against physical and environmental threats** Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	11.1.4 Perlindungan daripadan ancaman luar dan persekitaran	Peneraju ISMS	YA	**Optimized**	Memastikan perlindungan fizikal dibangun dan digunakan.	● Akta Keselamatan dan Kesihatan Pekerjaan 1994 (AKTA 514) Pindaan 2022 ● Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian D, Klausa 9 (b) ● GPKTMK versi 6.0 para 11.1 (e) : Kawalan Persekitaran
A.7.6	**Working in secure areas** Security measures for working in secure areas shall be designed and implemented.	11.1.5 Bekerja di kawasan selamat	Peneraju ISMS	YA	**Optimized**	Memastikan prosedur bagi memastikan keselamatan tempat kerja dibangun dan dilaksanakan.	● Akta Keselamatan dan Kesihatan Pekerjaan 1994 (AKTA 514) Pindaan 2022 ● GPKTMK versi 6.0 para 11.1 (f) : Bekerja dalam Kawasan Keselamatan
A.7.7	**Clear desk and clear screen** Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined	11.2.9 Dasar meja bersih dan skrin kosong	Peneraju ISMS	YA	**Optimized**	Memastikan polisi *clear desk* dan *clear screen* diguna pakai.	• GPKTMK versi 6.0 para 11.3 (i) : Panduan Clear Desk dan Clear Screen

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
	and appropriately enforced.						
A.7.8	**Equipment siting and protection** Equipment shall be sited securely and protected.	11.2.1 Penempatan dan perlindungan peralatan	Peneraju ISMS	YA	**Optimized**	Memastikan peralaran diletakkan di tempat yang dilindungi untuk mengurangkan risiko bahaya dan peluang akses yang tidak dibenarkan.	● Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian D, Klausa 9 (b) ● GPKTMK versi 6.0 para 11.3 : Keselamatan Peralatan
A.7.9	**Security of assets off-premises** Off-site assets shall be protected.	11.2.6 Keselamatan peralatan dan aset di luar premis	Peneraju ISMS & Pejabat Bursar	YA	**Optimized**	Memastikan keselamatan dan risiko setiap aset yang berada dilokasi luar diambil kira.	• GPKTMK versi 6.0 para 11.3 (f) : Peralatan Di Luar Premis • Prosedur Pengurusan Aset Alih (UPM/SOK/KEW-AST/P012)
A.7.10	**Storage media** Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	8.3.1 Pengurusan Media Boleh Alih	Peneraju ISMS	YA	**Optimized**	Memastikan prosedur bersesuaian dibangunkan mengikut klasifikasi yang digunakan oleh organisasi.	● Prosedur Pengurusan Aset Alih (UPM/SOK/KEW-AST/P012) ● GPKTMK versi 6.0 para 8.3 : Pengendalian media ● Garis Panduan Pengendalian Maklumat (iDEC/ISMS/GP01)
		8.3.2 Pelupusan Media	Peneraju ISMS	YA	**Optimized**	Media yang tidak lagi diperlukan perlu dilupuskan menggunakan prosedur yang dibangunkan.	● GPKTMK versi 6.0 para 8.3 : Pengendalian media ● Arahan Kerja Pelupusan Pita Backup dan Lain-lain Media Simpanan (UPM/ISMS/OPR/AK07) ● Garis Panduan Pelupusan Aset Alih (SOK/KEW/GP020/AST)

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
		8.3.3 Pemindahan Media Fizikal	Peneraju ISMS	YA	**Optimized**	Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa perpindahan.	● GPKTMK versi 6.0 para 8.3 – Pengendalian Media ● Garis Panduan Pengendalian Maklumat (iDEC/ISMS/GP01) ● Garis Panduan Pendaftaran ID Aset Alih (SOK/KEW/GP019/AST)
		11.2.5 Pengalihan aset	Peneraju ISMS & Pejabat Bursar	YA	**Optimized**	Memastikan peralatan, maklumat atau perisian tidak di bawah keluar dari lokasi tanpa kebenaran.	• GPKTMK versi 6.0 para 11.3 (f) : Peralatan di Luar Premis • Garis Panduan Pendaftaran ID Aset Alih (SOK/KEW/GP019/AST) • Garis Panduan Pengurusan Data Strategik UPM • Garis Panduan Permohonan Maklumat Rasmi UPM
A.7.11	**Supporting utilities** Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	11.2.2 Utiliti Sokongan	Peneraju ISMS	YA	**Optimized**	Memastikan peralatan dilindungi daripada kegagalan bekalan kuasa dan gangguan yang disebabkan oleh kegagalan utiliti sokongan.	● GPKTMK versi 6.0 para 11.1 (h) : Perkhidmatan Sokongan ● Prosedur Penyelenggaraan Berkala (UPM/SOK/PYG/P002) ● Garis Panduan Penyelenggaraan Operasi Pusat Data (UPM/ISMS/OPR/GP01/ PENYELENGGARAAN OPERASI)
A.7.12	**Cabling security** Cables carrying power, data or supporting information services shall	11.2.3 Keselamatan Kabel	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan kabel bekalan kuasa dan telekomunikasi dilindungi daripada	• GPKTMK versi 6.0 para 11.1 (i) : Keselamatan Kabel

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
	be protected from interception, interference or damage.					pemintasan, gangguan atau kerosakan.	
A.7.13	**Equipment maintenance** Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	11.2.4 Penyelenggaraan peralatan	Peneraju ISMS	YA	**Optimized**	Memastikan peralatan diselenggara.	• Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan komunikasi) 2014, Bahagian D, Klausa 10 • GPKTMK versi 6.0 para 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
A.7.14	**Secure disposal or re-use of equipment** Items of equipment containing storage media shall be verified to en-sure that any sensitive data and licensed software has been	11.2.7 Pelupusan yang selamat atau penggunaan semula peralatan	Peneraju ISMS & Pejabat Bursar	YA	**Optimized**	Memastikan aset yang terlibat dengan storan media perlu disemak dan data sensitif dibuang 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 versi 6.0 para 11.3 (g) : Pelupusan Peralatan

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
	removed or securely overwritten prior to disposal or re-use.						• Garis Panduan Pelupusan Aset Alih (SOK/KEW/GP020/AST)
8: TECHNOLOGICAL CONTROLS							
A.8.1	**User end point devices** Information stored on, processed by or accessible via user end point devices shall be protected.	6.2.1 Dasar peranti mudah alih	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan polisi dan sokongan kepada pengukuran keselamatan diambil kira bagi mengurus risiko daripada penggunaan peranti mudah alih.	● GPKTMK versi 6.0 para 8.4 Media Mudah Alih Persendirian *(Bring Your Own Device)* ● Garis Panduan Keselamatan Peralatan Mudah Alih (UPM/ISMS/SOK/ GP05/PERALATAN MUDAH ALIH)
		11.2.8 Peralatan pengguna tanpa jagaan	Peneraju ISMS	YA	**Optimized**	Memastikan peralatan yang ditinggalkan dikawal dengan sempurna.	• GPKTMK versi 6.0 para 11.3 (h) : Peralatan Ditinggalkan Pengguna
A.8.2	**Privileged access rights** The allocation and use of privileged access rights shall be restricted and managed.	9.2.3 Pengurusan Hak Akses Istimewa	Peneraju ISMS	YA	**Optimized**	Memastikan kebenaran hak akses dihadkan dan dikawal.	● GPKTMK versi 6.0 para 9.2 : Penyedian dan Semakan 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

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
							Maklumat Pelajar ● Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE-LEAD/AK01) ● Garis Panduan Pengurusan Identiti Pengguna ID EKLINIK (OPR/PKU/GP13/EKLINIK-ID) ● Buku Panduan Perkhidmatan Perubatan Pusat Kesihatan Universiti ● Borang Permohonan ID PutraENROLL (Peranan Pentadbir) ● Garis Panduan Pengurusan Identiti Pengguna PutraENROLL
A.8.3	**Information access restriction** Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	9.4.1 Sekatan Akses Maklumat	Peneraju ISMS	YA	**Optimized**	Memastikan akses kepada maklumat dan sistem aplikasi dihadkan mengikut prosedur kawalan akses.	● GPKTMK versi 6.0 para 9.1 : Dasar Kawalan Akses ● Prosedur Kawalan dan Pemantauan Capaian ke Sistem di Pusat Data (UPM/ISMS/OPR/P003) ● Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE-LEAD/AK01) ● Garis Panduan Kawalan Akses Ke Pusat Data (UPM/ISMS/OPR/GP03/ KAWALAN AKSES)

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
							● 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 ● Garis Panduan Pengurusan Identiti Pengguna ID eKlinik (OPR/PKU/GP13/EKLINIK-ID) ● Garis Panduan Pengendalian Maklumat (iDEC/ISMS/GP01) ● Borang Permohonan ID PutraENROLL (Peranan Pentadbir) ● Garis Panduan Pengurusan Identiti Pengguna PutraENROLL
A.8.4	**Access to source code** Read and write access to source code, development tools and software libraries shall be appropriately managed.	9.4.5 Kawalan akses kepada kod sumber program	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan akses kepada program kod sumber perlu dihadkan.	● GPKTMK versi 6.0 para 9.5 : Keselamatan Fail Sistem

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
A.8.5	**Secure authentication** Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	9.4.2 Prosedur Log Masuk yang Selamat	Pusat Pembangunan Maklumat dan Komunikasi & Pusat Pembangunan dan Kecemerlangan Kepimpinan Akademik	YA	**Optimized**	Memastikan akses kepada sistem dan aplikasi dikawal menggunakan prosedur bersesuaian.	● GPKTMK versi 6.0 para 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-LEAD/AK01) ● Garis Panduan Pengurusan UPM-ID (UPM/ISMS/OPR/GP16/ UPM-ID)
A.8.6	**Capacity management** The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	12.1.3 Pengurusan Kapasiti	Peneraju ISMS	YA	**Optimized**	Memastikan penggunaan sumber dipantau dan unjuran dibuat untuk keperluan masa depan untuk memastikan keperluan prestasi sistem.	• GPKTMK versi 6.0 para 12.1 (d): Pengurusan Kapasiti • Prosedur Penyelenggaraan ICT (UPM/OPR/IDEC/P003)
A.8.7	**Protection against malware** Protection against malware shall be implemented and supported by appropriate user awareness.	12.2.1 Kawalan daripada perisian hasad	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan kawalan ke atas perisian hasad (malware) dibangunkan.	• GPKTMK versi 6.0 para 12.2 (a) : Perlindungan daripada Perisian Berbahaya

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
A.8.8	**Management of technical vulnerabilities** Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	12.6.1 Pengurusan kerentanan teknikal	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan maklumat berkaitan kelemahan terhadap sistem dinilai dan diukur.	• GPKTMK versi 6.0 para 12.6: Pengurusan Kerentanan Teknikal • Garis Panduan Penilaian Tahap Keselamatan (UPM/ISMS/OPR/ /GP09/TAHAP KESELAMATAN) • Panduan Penilaian Risiko Aset Sistem Pengurusan Keselamatan Maklumat
A.8.9	**Configuration management** Configurations, including security configurations, of hardware, software, services and networks hall be established, documented, implemented, monitored and reviewed		Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan perubahan kepada -fasiliti pemprosesan maklumat dikawal	● Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) Prosedur Perkhidmatan ICT (UPM/OPR/IDEC/P002) ● Senarai Semak Perubahan Sistem Infrastruktur (IDEC/ISMS/SS01)
A.8.10	**Information deletion** Information stored in information systems, devies or in any other storage media shall be	A.11.2.7 Pelupusan yang selamat atau penggunaan semula peralatan	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan aset yang terlibat dengan storan media perlu disemak dan data sensitif dibuang 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 versi 6.0 para 11.3

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
	deleted when no longer required.						(g) : Pelupusan Peralatan • Garis Panduan Pelupusan Aset Alih (SOK/KEW/GP020/AST)
A.8.11	**Data masking** Data masking shall be used in accordance with the organizations's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.		Pusat Pembangunan Maklumat dan Komunikasi	YA	**Initial**	Memastikan maklumat sensitif dalam pangkalan data dapat dilindungi semasa pembangunan dilakukan.	• Pekeliling Bilangan 1 Tahun 2021 Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam. • PERKHIDMATAN SOKONGAN ICT (UPM/OPR/IDEC/AK31).
A.8.12	**Data leakage prevention** Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.		Pusat Pembangunan Maklumat dan Komunikasi	YA	**Initial**	Mengesan, memantau, dan melindungi data sensitif daripada kebocoran, sama ada secara sengaja atau tidak sengaja, ke pihak yang tidak dibenarkan. Ia bertujuan untuk memastikan maklumat organisasi yang kritikal sentiasa berada dalam kawalan dan digunakan dengan selamat	* GPKTMK versi 6.0 para 8.0 : Pengurusan Aset. * GPKTMK versi 6.0 para 9.0 : Kawalan Akses. * GPKTMK versi 6.0 para 13.0 : Keselamatan Komunikasi~~,~~. * GPKTMK versi 6.0 para 14.1 : Keselamatan dalam Pembangunan Sistem dan Aplikasi. * Pekeliling Bilangan 1 Tahun 2021 Dasar Perkhidmatan

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
							Pengkomputeran Awan Sektor Awam.
A.8.13	**Information backup** Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	12.3.1 Sandaran maklumat	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan salinan pendua dilaksanakan dan diuji mengikut perancangan.	• GPKTMK versi 6.0 para 12.3 (a) :*Backup* • Garis Panduan Pengurusan Backup Pangkalan Data dan Aplikasi (UPM/ISMS/OPR/GP14/ BACKUP)
A.8.14	**Redundancy of information processing facilities** Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	17.2.1 Ketersediaan kemudahan pemprosesan maklumat	Peneraju ISMS & Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan fasiliti pemprosesan dibangunkan bagi memenuhi keperluan ketersediaan maklumat.	• Pelan Kesinambungan Perkhidmatan • Pelan Pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT)
A.8.15	**Logging** Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	12.4.1 Pengelogan kejadian	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan event log dijana, disimpan dan dikaji secara berkala.	• GPKTMK versi 6.0 para 12.4: *Logging* dan Pemantauan
		12.4.2 Perlindungan maklumat log	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan kemudahan dan maklumat dilindungi daripada akses yang tidak dibenarkan.	• GPKTMK versi 6.0 para 12.4 (b): Perlindungan Maklumat Log • Garis Panduan Pemantauan Capaian Ke Sistem

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
							(UPM/ISMS/OPR/GP06/ Pemantauan Capaian)
		12.4.3 Log pentadbir dan pengendali	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan aktiviti pentadbir sistem direkod, dikawal dan dipantau berkala.	• GPKTMK versi 6.0 para 12.4 (c): Pentadbir dan Operator Log • 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 Server (UPM/ISMS/OPR/GP08/ MAKLUMAT LOG)
A.8.16	**Monitoring activities** Networks, systems and applicatons shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potention information security incidents.		Pusat Pembangunan Maklumat dan Komunikasi	YA		Memastikan sebarang aktiviti yang terkait dengan ancaman keselamatan ICT dipantau.	GPKTMK versi 6.0 para 14.2 (b): Pemantauan Perkhidmatan Sistem Maklumat
A.8.17	**Clock synchronization** The clocks of information	12.4.4 Penyegerakkan jam	Pusat Pembangunan	YA	**Optimized**	Memastikan masa bagi semua pemprosesan	• GPKTMK versi 6.0 para 12.4 (d): Pelarasan Masa

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
	processing systems used by the organization shall be synchronized to approved time sources.		Maklumat dan Komunikasi			malkumat diselaraskan dengan satu sumber rujukan masa.	• Network Time Protocol (time.upm.edu.my)
A.8.18	**Use of privileged utility programs** The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.	9.4.4 Penggunaan Program Utiliti yang mempunyai hak istimewa	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan utiliti program yang boleh menganggu sistem aplikasi perlu dihad dan dikawal.	● GPKTMK versi 6.0 para 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)
A.8.19	**Installation of software on operational systems** Procedures and measures shall be implemented to securely manage software installation on operational systems.	12.5.1 Pemasangan perisian pada sistem yang beroperasi	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan kawalan pemasangan perisian ke atas sistem pengoperasian.	• GPKTMK versi 6.0 para 12.5: Kawalan Ke atas Perisian Pengoperasian • Prosedur Perkhidmatan ICT (UPM/OPR/IDEC/P002) • Panduan Instalasi Sistem yang berkaitan
A.8.20	**Networks security** Networks and network devices shall be secured, managed and controlled	13.1.1 Kawalan rangkaian	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan rangkaian perlu urus dan dikawal.	• GPKTMK versi 6.0 para 13.1 : Pengurusan Keselamatan Rangkaian • GPKTMK versi 6.0 para 13.2 : Keselamatan Perkhidmatan

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
	to protect information in systems and applications.						Rangkaian • Garis Panduan Pengurusan Pengagihan Rangkaian (UPM/ISMS/OPR/ /GP13/AGIHAN RANGKAIAN) • Garis Panduan Pengurusan UPM-ID (UPM/ISMS/OPR/GP16/ UPM-ID)
A.8.21	**Security of network services** Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	13.1.2 Keselamatan perkhidmatan rangkaian	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Tidak melibatkan *Internet Service Provider.* Hanya menggunakan intranet (UPMNET).	• GPKTMK versi 6.0 para 13.1 Pengurusan Keselamatan Rangkaian • Kontrak perkhidmatan Firewall dan WAF dengan pembekal • Rangkaian UPMNet pada peringkat Super Core Switch, Core Switch, Distribution Switch dan Access Switch di Fakulti UPM Serdang
A.8.22	**Segregation of networks** Groups of information services, users and information systems shall be segregated in the organization's networks.	13.1.3 Pengasingan dalam rangkaian	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan pengasingan rangkaian dilaksanakan.	• Garis Panduan Pengurusan Pengagihan Rangkaian (UPM/ISMS/OPR /GP13/AGIHAN RANGKAIAN)
A.8.23	**Web filtering** Access to external websites shall be		Pusat Pembangunan	YA	**Optimized**	Memastikan penapisan dan kawalan kepada laman web yang mempunyai isi	GPKTMK versi 6.0 para 13.1 Pengurusan Keselamatan Rangkaian

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
	managed to reduce expousre to malicious content.		Maklumat dan Komunikasi			kandungan yang tidak selamat	Arahan Kerja Perkhidmatan Sokongan ICT (UPM/OPR/IDEC/AK31)
A.8.24	**Use of cryptography** Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	10.1.1 Dasar penggunaan kawalan kriptografi	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan polisi penggunaan kawalan kriptografi untuk perlindungan maklumat dibangun dan dilaksanakan.	● Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian G, Klausa 21(a) ● GPKTMK versi 6.0 para 10.0 : Kriptografi ● Garis Panduan Pengendalian Maklumat (iDEC/ISMS/GP01)
		10.1.2 Penggunaan kekunci	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan polisi penggunaan, perlindungan dan jangka hayat kunci kriptografi dibangun dan dilaksanakan.	● Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan komunikasi) 2014, Bahagian G, Klausa 21(c) ● GPKTMK versi 6.0 para 10.0 (b) Pengurusan Kunci Kriptografi *(Key Management)* ● Garis Panduan Pengendalian Maklumat (iDEC/ISMS/GP01)
A.8.25	**Secure development life cycle** Rules for the secure development of software and systems shall be established and applied.	14.2.1 Dasar pembangunan selamat	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan polisi keselamatan pembangunan sistem dan aplikasi dibangun dan diguna pakai.	• GPKTMK versi 6.0 para 14.1 : Keselamatan dalam Pembangunan Sistem dan Aplikasi • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001)

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
A.8.26	**Application security requirements** Information security requirements shall be identified, specified and approved when developing or acquiring applications.	14.1.2 Melindungi perkhidmatan aplikasi dalam rangkaian awam	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan kawalan terhadap rangkaian awam perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan atau pengubahsuaian yang tidak dibenarkan.	• GPKTMK versi 6.0 para 13.1 : Pengurusan Keselamatan Rangkaian • Garis Panduan Keselamatan Peralatan Mudah Alih (UPM/ISMS/SOK/GP05/ PERALATAN MUDAH ALIH) 2.0 Panduan 1(viii)
		14.1.3 Melindungi transaksi perkhidmatan aplikasi	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan maklumat yang terlibat dalam transaksi perkhidmatan 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.	• GPKTMK versi 6.0 para 14.1 (c) – Melindungi Transaksi Perkhidmatan Aplikasi • Pelaksanaan Secure Socket Layer-SSL di Sistem Aplikasi
A.8.27	**Secure system architecture and engineering principles** Principles for engineering secure systems shall be established, docu-	14.2.5 Prinsip kejuruteraan sistem yang selamat	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan prinsip persekitaran pembangunan selamat diamalkan dalam setiap projek pembangunan sistem aplikasi.	• GPKTMK versi 6.0 para 14.3 : Persekitaran Pembangunan Selamat • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001)

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
	mented, maintained and applied to any information system development activities.						
A.8.28	**Secure coding** Secure coding principles shall be applied to software development.		Pusat Pembangunan Maklumat dan Komunikasi	YA	**Initial**	Memastikan sistem yang dibangunkan untuk kegunaan UPM mempunyai ciri-ciri keselamatan ICT yang bersesuaian di setiap fasa pembangunan serta mengikut prosedur pembangunan ICT yang telah ditetapkan oleh Universiti.	• GPKTMK versi 6.0 para 14.1 : Keselamatan dalam Pembangunan Sistem dan Aplikasi. • Arahan Kerja Pembangunan Aplikasi Secara Dalaman (UPM/OPR/IDEC/AK34).
A.8.29	**Security testing in development and acceptance** Security testing processes shall be defined and implemented in the development life cycle.	14.2.8 Pengujian keselamatan sistem	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	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)
		14.2.9 Pengujian penerimaan sistem	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan ujian penerimaan perlu dilaksanakan bagi sistem baru atau naik taraf.	• Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001)
A.8.30	**Outsourced development**	14.2.7 Pembangunan oleh khidmat luaran	Pusat Pembangunan	YA	**Optimized**	Memastikan aktiviti pembangunan oleh pihak	• GPKTMK versi 6.0 para 14.3 (C) : Pembangunan Sistem Aplikasi oleh Pihak Ketiga

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
	The organization shall direct, monitor and review the activities related to outsourced system development.		Maklumat dan Komunikasi			luar perlu diselia dan dipantau.	• Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) • Prosedur Perolehan Universiti (UPM/SOK/KEW-BUY/P016) • Dokumen Kontrak
A.8.31	**Separation of development, test and production environments** Development, testing and production environments shall be separated and secured.	12.1.4 Pengasingan persekitaran pembangunan, pengujian dan operasi	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan pembangunan, pengujian dan operasi persekitaran diasingkan untuk mengurangkan risiko kepada akses yang tidak dibenarkan.	• GPKTMK versi 6.0 para 14.3(a) : Prosedur Kawalan Persekitaran Selamat • Garis Panduan Penyediaan Server Di Pusat Data (UPM/ISMS/OPR/GP02/ PENYEDIAAN SERVER)
		14.2.6 Persekitaran pembangunan selamat	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan persekitaran pembangunan selamat diamalkan dalam setiap proses pembangunan sistem aplikasi.	• GPKTMK versi 6.0 para 14.3 : Persekitaran Pembangunan Selamat • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001)
A.8.32	**Change management** Changes to information processing facilities and information systems shall be subject to change management procedures.	12.1.2 Pengurusan perubahan	Pusat Jaminan Kualiti & Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	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

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
							● Bidang kuasa Mesyuarat Kajian Semula Pengurusan ● Bidang kuasa Jawatankuasa Kualiti ● Bidang kuasa Jawatankuasa Kerja ISMS ● Bidang kuasa PTJ ● Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) ● Prosedur Perkhidmatan ICT (UPM/OPR/IDEC/P002) ● Senarai Semak Perubahan Sistem Infrastruktur (IDEC/ISMS/SS01)
		14.2.2 Prosedur kawalan perubahan sistem	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan perubahan kepada proses pembangunan perlu dikawal menggunakan prosedur kawalan perubahan.	• GPKTMK versi 6.0 para 14.2 (a) : Prosedur Kawalan Perubahan • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001)
		14.2.3 Kajian semula teknikal bagi aplikasi selepas perubahan platform operasi	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan perubahan ke atas aplikasi perlu disemak dan diuji untuk memastikan tiada kesan buruk terhadap organisasi atau keselamatan.	• GPKTMK versi 6.0 para 14.2 (a) : Prosedur Kawalan Perubahan • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001)

SEKSYEN	KAWALAN KESELAMATAN MAKLUMAT		PEMILIK PROSES	PELAKSANAAN (YA/TIDAK)	STATUS PELAKSANAAN	JUSTIFIKASI	KAWALAN SEMASA
	MS ISO/IEC 27001:2022	MS ISO/IEC 27001:2013					
		14.2.4 Sekatan ke atas perubahan dalam pakej perisian	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan sebarang perubahan atau pengubahsuaian pakej aplikasi perlu dikawal.	• GPKTMK versi 6.0 para 14.2 (a) : Prosedur Kawalan Perubahan. • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001).
A.8.33	**Test information** Test information shall be appropriately selected, protected and managed.	14.3.1 Perlindungan data ujian	Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan data pengujian dipilih, dilindungi dan dikawal.	• GPKTMK versi 6.0 para 14.3 (b): Pengujian Pembangunan atau Penaiktarafan Sistem. • Arahan Kerja Perkhidmatan Sokongan ICT (UPM/OPR/IDEC/AK31).
A.8.34	**Protection of information systems during audit testing** Audit tests and other assurance activities involving assessment of op- erational systems shall be planned and agreed between the tester and appropriate management.	12.7.1 Kawalan audit sistem maklumat	Pusat Jaminan Kualiti & Pusat Pembangunan Maklumat dan Komunikasi	YA	**Optimized**	Memastikan keperluan audit dan aktiviti yang melibatkan pengesahan terhadap sistem operasi dirancang dengan teliti dan dipersetujui untuk meminimumkan gangguan (disruption) pada proses sesebuah organisasi.	GPKTMK versi 6.0 para 12.7: Pertimbangan Audit Sistem Maklumat. • Audit Dalaman ISMS.