MINIT MESYUARAT JAWATANKUASA KERJA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
KALI PERTAMA

TARIKH : 6 NOVEMBER 2015 (JUMAAT)

MASA : 3.00 PETANG

TEMPAT : BILIK LEMBAGA

KEHADIRAN : LAMPIRAN A

MINIT	AGENDA	TINDAKAN/ MAKLUMAN
1.1	**KATA ALU-ALUAN** Pengerusi: 1.1.1 mengalu-alukan kehadiran ahli mesyuarat ke Mesyuarat Jawatankuasa Kerja Sistem Pengurusan Keselamatan Maklumat Kali Pertama; 1.1.2 memaklumkan struktur Jawatankuasa ISMS seperti pada **Lampiran 1**; dan 1.1.3 memaklumkan berkaitan perubahan skop ISMS iaitu; i. Sistem Pengurusan Keselamatan Maklumat hanya melibatkan proses Pendaftaran Pelajar Baharu Prasiswazah semasa Minggu Perkasa Putra dalam Sistem Pengurusan Pelajar; ii. Sistem Pengurusan Keselamatan Maklumat untuk Pengoperasian Pusat Data bagi proses Pendaftaran Pelajar Baharu Prasiswazah; dan	 Makluman Makluman Makluman

MINIT	AGENDA	TINDAKAN/ MAKLUMAN
	iii. Sistem Pengurusan Keselamatan Maklumat untuk Pengoperasian Pusat Pemulihan Bencana bagi proses Pendaftaran Pelajar Baharu Prasiswazah.	
1.2	**MAKLUMAN BERKAITAN ISMS** Ahli mesyuarat mengambil perhatian perkara berikut: 1.2.1 **Manual ISMS** i. mengambil maklum kertas edaran 1 berkaitan Manual ISMS telah dipinda berdasarkan pindaan pada skop ISMS yang telah diluluskan dalam Mesyuarat Jawatankuasa ISO Kali Ke-23; dan ii. mengambil maklum Manual ISMS yang baharu telah kuatkuasa pada 6 November 2015 di Mesyuarat Jawatankuasa ISO Kali Ke-24 secara edaran dengan huraian pindaan seperti pada **Lampiran 2**. 1.2.2 **Objektif ISMS** i. mengambil maklum Objektif ISMS turut dipinda selaras dengan skop baharu dan telah kuatkuasa secara edaran pada Mesyuarat Jawatankuasa ISO Kali Ke-24; dan ii. bersetuju agar, objektif ISMS seperti pada **Lampiran 3** diukur dan dibuat analisis mengikut format yang akan dikeluarkan oleh sekretariat. 1.2.3 **Rumusan Penilaian Risiko** Mengambil maklum berkaitan rumusan penilaian risiko seperti pada **Lampiran 4** terhadap lapan (8) projek iaitu pembayaran pelajar baharu, sistem aplikasi maklumat pelajar, sistem pangkalan data, sistem sokongan pusat data, kad pelajar baharu, pendaftaran kolej pelajar, pengesahan laporan pemeriksaan kesihatan dan sistem aplikasi kewangan.	Makluman Makluman Makluman Pusat Jaminan Kualiti Makluman

MINIT	AGENDA	TINDAKAN/ MAKLUMAN
1.3	**<u>KUATKUASA DOKUMENTASI</u>**	
	Mesyuarat bersetuju untuk meluluskan pindaan dokumen yang akan kuatkuasa pada 16 November 2015. Dokumen yang dipinda adalah seperti berikut:	Timbalan Kawalan Dokumen
	1.3.1 Penilaian Risiko Sistem Pengurusan Keselamatan Maklumat (ISMS) (UPM/ISMS/OPR/RA)	
	1.3.1.1 Pindaan adalah disebabkan pindaan pada skop dan penilaian dibuat dengan menggunakan MyRAM yang melibatkan lima (5) perkara iaitu *hardware, software, people, services (accessibility)* dan *services (supporting).*	Makluman
	1.3.1.2 bersetuju pada penilaian risiko bagi kad pelajar jumlah *people* adalah 7 orang ini kerana mengira hari pendaftaran di kolej-kolej.	Jawatankuasa Penilaian Risiko
	1.3.2 *Statement of Aplicability (SoA)* Sistem Pengurusan Keselamatan Maklumat (ISMS) (UPM/ISMS/OPR/SoA). Slide pembentangan berkaitan SoA adalah pada **Lampiran 5**.	
	1.3.2.1 bersetuju untuk setiap PTJ/Peneraju yang terlibat dalam SoA, untuk mengambil tindakan seperti yang tertera di dalam SoA **(Rujuk Lampiran 6).**	PTJ/Peneraju yang terlibat
	1.3.2.2 bersetuju Pejabat Penasihat Undang-Undang untuk melihat kontrak-kontrak perolehan bersama dengan Pejabat Bursar bagi memasukkan perkara berkaitan keselamatan maklumat.	Pejabat Penasihat Undang-Undang
	1.3.2.3 bersetuju Seksyen Latihan, Pejabat Pendaftar untuk melihat latihan berkaitan keselamatan maklumat dan memanggil untuk perbicangan bagi takwim akan datang.	Bahagian Pembangunan Sumber Manusia, Pejabat Pendaftar
	1.3.3 Garis Panduan Pemantauan Pengukuran Analisis & Penilaian (UPM/ISMS/OPR/DC/GP07/SECURITY METRICS). Huraian pindaan adalah seperti **Lampiran 7**.	Timbalan Kawalan Dokumen

MINIT	AGENDA	TINDAKAN/ MAKLUMAN
1.4	**LAPORAN TINDAKAN SUSULAN MASYUARAT KAJIAN SEMULA PENGURUSAN ISMS** Mesyuarat mengambil maklum agenda tindakan susulan Mesyuarat Kajian Semula Pengurusan ISMS akan dibincangkan di dalam Perbincangan Input Mesyuarat Kajian Semula Pengurusan ISMS.	Makluman
1.5	**TINDAKAN KE ATAS TINDAKAN PEMBETULAN, PENCEGAHAN DAN PELUANG PENAMBAHBAIKAN** Tiada Laporan.	
1.6	**HAL-HAL LAIN** **Audit Dalaman ISMS** Mesyuarat mengambil maklum UPM akan menghadapi Audit Pensijilan Semula pada 8 hingga 9 Disember 2015. Sebagai memenuhi klausa 9.2, MS ISO/IEC 27001:2013, UPM akan mengadakan Audit Dalaman pada 18 hingga 19 November 2015 dengan melibatkan tiga (3) kumpulan. Jadual Audit Dalaman pada **Lampiran 8**.	Makluman
1.7	**PENANGGUHAN MESYUARAT** Mesyuarat ditangguhkan jam 4.50 petang.	

LAMPIRAN A

SENARAI KEHADIRAN MESYUARAT JAWATANKUASA KERJA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
KALI PERTAMA

HADIR

1. Mohd Faizal Daud - Pengerusi
2. Tuan Haji Rosdi Wah (Penasihat Jawatankuasa Kerja ISMS)
3. Encik Mohamad Farid Harun
   (Peneraju Proses Pusat Data - Jawatankuasa Kerja ISMS)
4. Puan Noraihan Noordin - Setiausaha

TURUT HADIR

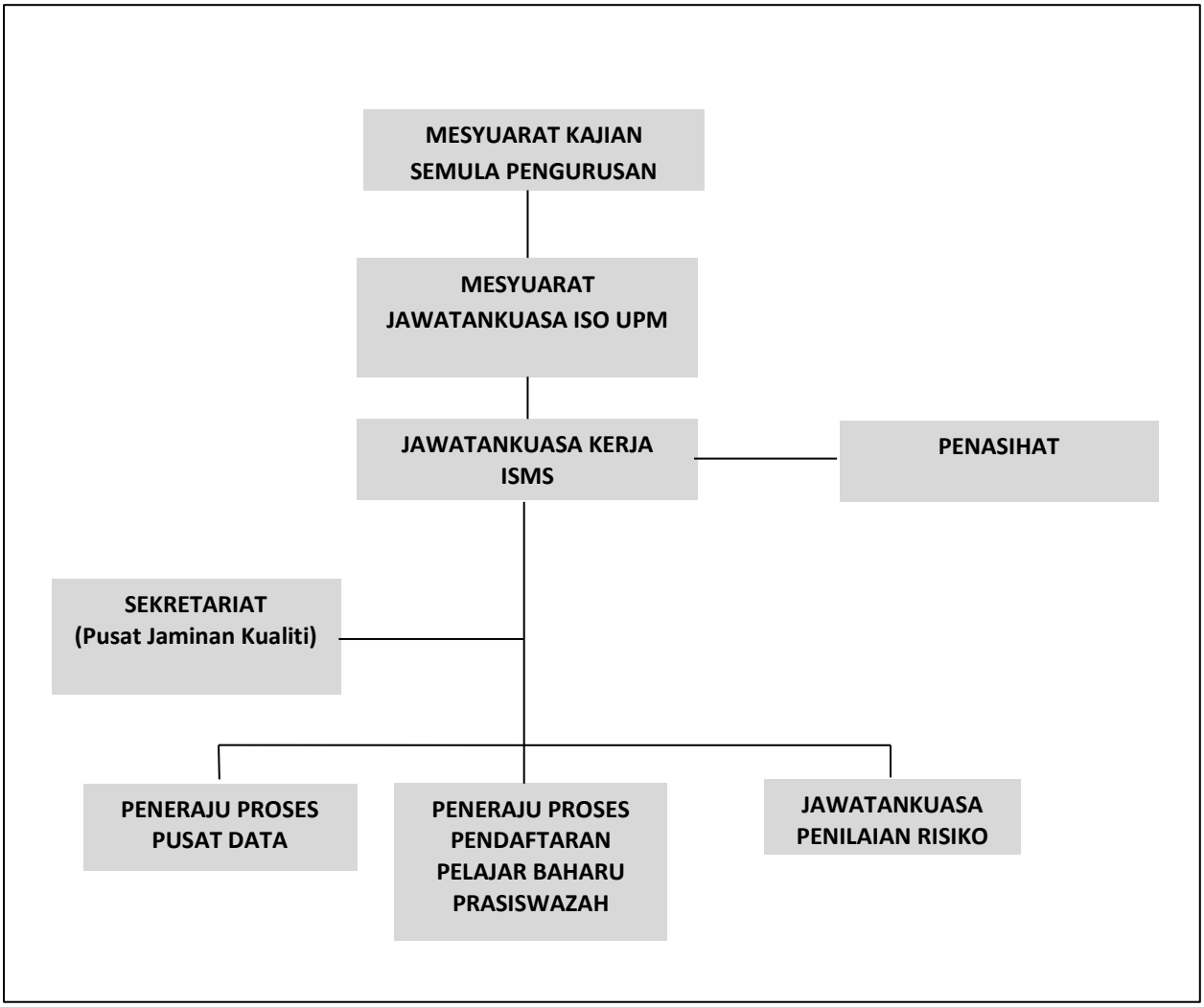
1. Puan Siti Rozana Supian
2. Puan Noorizai Mohamad Noor
3. Encik Muhazam Mansor
4. Puan Hashimah Amat Sejani (Wakil Encik Mohd Zul Mohd Yusoff)
5. Puan Mazitah Ahmad
6. Tuan Haji Mokhtar Dahari
7. Dr. Haji Latif Anwar
8. Encik Mohd Aizat Azmi (Wakil Prof. Madya Dr. Rozanah Ab. Rahman)
9. Puan Nurul Fatihah Md Marham (Timbalan Pegawai Kawalan Dokumen)
10. Puan Salmah Uzairi (Wakil Dr. Suhyna Mohamad Sulaiman)

TIDAK HADIR DENGAN KENYATAAN

1. Encik Rosmi Othan (Penasihat Jawatankuasa Kerja ISMS)
2. Puan Suhana Md Chairi
   (Peneraju Proses SMP - Jawatankuasa Kerja ISMS)
3. Encik Mohd Zul Mohd Yusoff
   (Jawatnkuasa Penilaian Risiko - Jawatankuasa Kerja ISMS)
4. Tuan Haji Hashim Md Shari
5. Encik Krishnan Mariappan
6. Encik Syemsul Bahrim Abdul
7. Dr. Suhyna Mohamad Sulaiman

LAMPIRAN 1

STRUKTUR ORGANISASI
SISTEM PENGURUSAN KELAMATAN MAKLUMAT



LAMPIRAN 2

Huraian Pindaan Dokumen		Tambahan (T) / ~~Pemotongan~~ (P)
Asal	**Pindaan**	
Nama Dokumen: MANUAL SISTEM PENGURUSAN KESELAMATAN MAKLUMAT Kod Dokumen: UPM/ISMS/PGR/MP No. Isu: 01, No. Semakan: 01, Tarikh Kuatkuasa: 10/11/2014	Nama Dokumen: MANUAL SISTEM PENGURUSAN KESELAMATAN MAKLUMAT Kod Dokumen: UPM/ISMS/PGR/MP No. Isu: 01, No. Semakan: 01,	

SEKSYEN/ RUJUKAN	TAJUK	MUKA SURAT
1.0	**PENGENALAN**	3
1.1	Tujuan	3
1.2	Skop	3
1.3	Tarikh Kuatkuasa	3
2.0	**MAKLUMAT ORGANISASI**	4
2.1	Latar Belakang	4
2.2	Visi	4
2.3	Misi	4
2.4	Matlamat UPM	4
3.0	**KEPERLUAN ISMS**	5
3.1	Latar Belakang	5
3.2	Pemetaan ISMS	7
4.0	**KONTEKS ORGANISASI**	8
4.1	Memahami Organisasi	8
4.2	~~Memahami~~ Keperluan dan Harapan Pihak Berkaitan	10
4.3	Skop ISMS	14
5.0	**KEPIMPINAN**	17
5.1	Kepimpinan dan komitmen	17
5.2	~~Polisi~~ ISMS	17
5.3	Peranan dan Tanggungjawab	19
6.0	**PERANCANGAN**	22
6.1	Tindakan untuk Menangani Risiko dan Peluang	22
6.1.1	Am	22
6.1.2	Penilaian Risiko	22

SEKSYEN/ RUJUKAN	TAJUK	MUKA SURAT
1.0	**PENGENALAN**	3
1.1	Tujuan	3
1.2	Skop	3
1.3	Tarikh Kuatkuasa	3
2.0	**MAKLUMAT ORGANISASI**	4
2.1	Latar Belakang	4
2.2	Visi	4
2.3	Misi	4
2.4	Matlamat UPM	4
3.0	**KEPERLUAN ISMS**	5
3.1	Latar Belakang	5
3.2	Pemetaan ISMS	6
4.0	**KONTEKS ORGANISASI**	7
4.1	Memahami Organisasi	7
4.2	Keperluan dan Harapan Pihak Berkaitan	11
4.3	Skop ISMS	12
5.0	**KEPIMPINAN**	15
5.1	Kepimpinan dan komitmen	15
5.2	Dasar ISMS	15
5.3	Peranan dan Tanggungjawab	18
6.0	**PERANCANGAN**	21
6.1	Tindakan untuk Menangani Risiko dan Peluang	21
6.1.1	Am	21
6.1.2	Penilaian Risiko	21

T/P

	Organisasi UPM			aktiviti yang dilaksanakan Oleh UPM dan organisasi		
Jadual 3	Pelan Perancangan Pencapaian Objektif Keselamatan Maklumat	25	Jadual 4	Justifikasi Pengecualian	13	
Jadual 4	Kaedah Komunikasi Secara Dalaman dan Luaran	24	Jadual 5	Lokasi Skop Pelaksanaan Pensijilan ISMS UPM	15	
Jadual 5	Pilihan Cadangan Kawalan Keputusan Penilaian Risiko	30	Jadual 6	Peranan dan tanggungjawab organisasi ISMS UPM	20	
~~Lampiran A~~	~~Pelan Lantai Bangunan Pusat Data Utama (DC)~~	~~37~~	Jadual 7	Kaedah Komunikasi Secara Dalaman dan Luaran	26	
~~Lampiran B~~	~~Pelan Lantai Bangunan Pusat Data Kedua (DRC)~~	~~38~~	Jadual 8	Pilihan Cadangan Kawalan Keputusan Penilaian Risiko	29	

1.3 **TARIKH BERKUAT KUASA** Manual ini berkuat kuasa mulai tarikh ~~10 November 2014.~~	**1.3** **TARIKH BERKUAT KUASA** Manual ini berkuat kuasa mulai tarikh 6 November 2015.	**P**
2.2 **VISI** Menjadi Sebuah Universiti Bereputasi Antarabangsa. **2.4** **MATLAMAT UPM** Untuk mencapai visi dan misi yang telah diwujudkan, UPM telah menggubal 5 matlamat seperti yang dinyatakan dalam Pelan Strategi UPM 2014 – 2020 iaitu: Matlamat 1 : Mempertingkatkan Kualiti dan Daya Saing Graduan Matlamat 2 : Penjanaan Nilai Melalui Ekosistem RDCE Yang Mantap Dan Lestari Matlamat 3 : Melonjakkan Perkhidmatan Jaringan Industri Dan Masyarakat Matlamat 4 : Memperkasakan UPM sebagai Pusat Kecemerlangan Pertanian Matlamat 5 : Mempertingkatkan Kualiti Tadbir Urus	**2.2** **VISI** Menjadi sebuah universiti bereputasi antarabangsa. **2.4** **MATLAMAT UPM** Untuk mencapai visi dan misi yang telah diwujudkan, UPM telah menggubal 5 matlamat seperti yang dinyatakan dalam Pelan Strategi UPM 2014 – 2020 iaitu: Matlamat 1 : Mempertingkatkan kualiti dan daya saing graduan Matlamat 2 : Penjanaan nilai melalui ekosistem RDCE yang mantap dan lestari Matlamat 3 : Melonjakkan perkhidmatan jaringan industri dan masyarakat Matlamat 4 : Memperkasakan UPM sebagai Pusat Kecemerlangan Pertanian Matlamat 5 : Mempertingkatkan kualiti tadbir urus	**P**

4.1.2 ~~**Isu-isu yang Mempengaruhi Sistem Pengurusan Keselamatan Maklumat**~~ ~~a. Kebergantungan penggunaan ICT dalam mentadbir dan mengurus operasi Universiti untuk merealisasikan visi dan misi;~~ ~~b. Persekitaran Pusat Data yang kurang kondusif, pengendalian dan tadbir urus pemusatan data dan pangkalan data elektronik Universiti kurang mantap;~~ ~~c. Kawalan dan seliaan data digital tidak berpusat;~~ ~~d. Risiko ancaman siber seperti terdedah kepada ketirisan, kecurian dan salah guna maklumat;~~ ~~e. Tadbir urus keselamatan maklumat yang kurang mantap; dan~~ ~~f. Penyalahgunaan maklumat kakitangan dan pelajar.~~	**4.1.2** **Penentuan Skop Pelaksanaan ISMS** Dalam melaksanakan ISMS, penentuan skop pensijilan perlu merangkumi perkara-perkara berikut: a. Menentukan isu luaran dan dalaman berkaitan dengan matlamatnya yang boleh mempengaruhi pencapaian keberhasilan ISMS; b. Menentukan pihak berkepentingan serta keperluan mereka dalam pelaksanaan ISMS; dan c. Menentukan sempadan dan kebolehgunaan ISMS.	**P**

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

Jadual 1 : Keberhasilan pelaksanaan ISMS di peringkat organisasi dan isu dalaman serta luaran

BIL.	PIHAK BERKEPENTINGAN	KEPERLUAN PIHAK BERKEPENTINGAN
1.	Pelajar	Maklumat peribadi dan akademik pelajar hendaklah dilindungi
2.	Ibubapa dan penjaga	Maklumat prestasi pelajar hendaklah dilindungi
3.	Warga UPM	Maklumat peribadi hendaklah dilindungi
4.	Kementerian Pengajian Tinggi Malaysia (KPTM)	Maklumat profil Universiti, pelajar, penyelidikan, sumber manusia dan kewangan hendaklah dilindungi
5.	Penaja Pendidikan	Maklumat prestasi pelajar yang tepat
6.	Agensi Kerajaan	Maklumat yang tepat
7.	Pembekal	i. Maklumat kontrak yang dipatuhi ii. Maklumat kerjasama
9.	Badan Penarafan	Maklumat /data yang tepat

Jadual 2 : Pihak berkepentingan serta keperluan mereka

BIL.	AKTIVITI	ORGANISASI	PERTALIAN/HUBUNGKAIT
1.	Pengurusan penajaan pendidikan pelajar	Penaja pendidikan	Sistem Maklumat Pelajar – Modul Penaja
2.	Pemberian dan penerimaan maklumat	Kementerian Pengajian Tinggi Malaysia (KPTM)	Perkongsian maklumat
3.	Pemberian dan penerimaan maklumat	Agensi Kerajaan dan NGO	Perkongsian maklumat
4.	Penyelenggaraan peralatan	Sistem Pengurusan Aset Tetap UPM (FAMS)	Penyelenggaraan dilaksanakan oleh pihak vendor, penjadualan dan pengesahan perkhidmatan oleh UPM
5.	Penyelenggaraan sistem	Sistem Pengurusan Aset Tetap UPM (FAMS)	Penyelenggaraan dilaksanakan oleh pihak vendor, penjadualan dan pengesahan perkhidmatan oleh UPM

Jadual 3: Pertalian dan kebergantungan aktiviti yang dilaksanakan oleh UPM dan organisasi

4.1.3	~~**Hasil Sistem Pengurusan Keselamatan Maklumat**~~ ~~a. Pemusatan pangkalan data dan saluran akses yang terkawal dan dibenarkan;~~ ~~b. Jaminan kerahsiaan, integriti dan ketersediaan maklumat dari Pusat Data;~~ ~~c. Operasi Sistem Utama Universiti yang selamat dan boleh dipercayai; dan~~ ~~d. Memantapkan tadbir urus keselamatan maklumat di Pusat Data.~~	**4.1.3**	**Penyataan skop pelaksanaan ISMS** Skop pelaksanaan ISMS dikenalpasti dan ditentukan berdasarkan tiga (3) perkara di atas : a. Menentukan isu luaran dan dalaman berkaitan dengan matlamatnya yang boleh mempengaruhi pencapaian keberhasilan ISMS; b. Menentukan pihak berkepentingan serta keperluan mereka dalam pelaksanaan ISMS; dan c. Menentukan sempadan dan kebolehgunaan ISMS. Pernyataan skop ISMS adalah : 1. Sistem Pengurusan Keselamatan Maklumat hanya melibatkan proses Pendaftaran Pelajar Baharu Prasiswazah dalam Sistem Pengurusan Pelajar 2. Sistem Pengurusan Keselamatan Maklumat untuk Pengoperasian Pusat Data bagi proses Pendaftaran Pelajar Baharu Prasiswazah ~~3.~~ Sistem Pengurusan Keselamatan Maklumat untuk Pengoperasian Pusat Pemulihan Bencana bagi proses Pendaftaran Pelajar Baharu Prasiswazah	**P**
4.2	~~**MEMAHAMI KEPERLUAN DAN HARAPAN PIHAK BERKAITAN**~~ ~~Pihak Pengurusan UPM telah menetapkan pihak berkepentingan yang terlibat dengan skop pensijilan (Jadual 1).~~	**4.2**	**KEPERLUAN DAN HARAPAN PIHAK BERKAITAN**	**P**
~~**4.2.1**~~	~~**Model Penentuan Skop Migrasi ISMS UPM**~~			**G**
4.3	**SKOP ISMS** Skop pensijilan ISMS UPM adalah seperti berikut: ~~Pengurusan Sistem Keselamatan Maklumat (ISMS) adalah bagi operasi Pusat Data UPM merangkumi perkakasan (server dan storan) dan data/maklumat untuk aplikasi kritikal berikut:~~ ~~a. Laman Web Utama Universiti;~~ ~~b. Sistem Pengurusan Kewangan;~~	**4.3**	**SKOP ISMS** Skop pensijilan ISMS UPM adalah seperti berikut: 1. Sistem Pengurusan Keselamatan Maklumat hanya melibatkan proses Pendaftaran Pelajar Baharu Prasiswazah semasa Minggu Perkasa Putra dalam Sistem Pengurusan Pelajar 2. Sistem Pengurusan Keselamatan Maklumat untuk Pengoperasian Pusat Data bagi proses Pendaftaran Pelajar Baharu Prasiswazah	**P**

~~c. Sistem Pengurusan Sumber Manusia;~~ ~~d. Sistem Maklumat Pelajar Prasiswazah (SMP); dan~~ ~~e. Sistem Maklumat Pelajar Pasca Siswazah (iGIMS).~~	~~3.~~ Sistem Pengurusan Keselamatan Maklumat untuk Pengoperasian Pusat Pemulihan Bencana bagi proses Pendaftaran Pelajar Baharu Prasiswazah	
4.3.1 Pengecualian Skop Pensijilan ISMS ~~Pengecualian kepada skop pensijilan ISMS adalah sistem aplikasi yang tidak disenaraikan dalam skop, proses pembangunan sistem aplikasi, perkakasan (server dan storan) yang berada di luar Pusat Data UPM dan laman web PTJ.~~ ~~Justifikasi pengecualian adalah berdasarkan kepada perkara berikut:~~ ~~a. Ianya bukan proses sistem utama universiti;~~ ~~b. Proses pembangunan aplikasi dilaksanakan di luar operasi Pusat Data;~~ ~~c. Kawalan hanya kepada perkakasan (server dan storan) yang berada di parameter Pusat Data;~~ ~~d. Sumber maklumat rasmi Universiti diperolehi dari laman web utama Universiti sahaja; dan~~ ~~e. Tidak melibatkan data yang kritikal dan tidak menjejaskan sebahagian besar operasi utama UPM serta ianya merupakan aplikasi sokongan sahaja.~~	**4.3.2 Pengecualian Skop Pensijilan ISMS** Pengecualian skop pensijilan ISMS proses pendaftaran pelajar baharu prasiswazah adalah kepada pendaftaran kursus, *Meal Plan* dan aktiviti kemasukan pendaftaran pelajar baharu prasiswazah untuk: i. Pengajian Jarak Jauh; ii. Eksekutif; iii. Pesisir; iv. Luar Pesisir; v. Antarabangsa; vi. Mobiliti; dan vii. UPM Kampus Bintulu. Justifikasi pengecualian adalah berdasarkan kepada berikut:	**P**

BIL.	PERKARA	JUSTIFIKASI
1.	Pengajian Jarak Jauh	Kawalan UPM Holding
2.	Eksekutif	Perancangan dimasukkan dalam skop pensijilan 2017 (tertakluk kepada keputusan pengurusan)
3.	Pesisir	
4.	Luar Pesisir	
5.	Antarabangsa	
6.	Mobiliti	
7.	UPM Kampus Bintulu	

Jadual 4 : Justifikasi pengecualian

<table>
<tr>
<td>4.3.2 PROSES PERKHIDMATAN SKOP ISMS UPM
Perkhidmatan operasi Pusat Data yang terlibat dalam skop pensijilan ISMS merangkumi proses berikut:</td>
<td>4.3.2 PROSES PERKHIDMATAN SKOP ISMS UPM
Proses lapor diri pelajar baharu prasiswazah yang melibatkan aktiviti berikut:

a. Menyemak tawaran
b. Menerima salinan pendua slip bayaran yuran CIMB
c. Menerima borang permohonan kad pelajar
d. Mengesah status kesihatan
e. Pengesahan pendaftaran
f. Pendaftaran kolej

Perkhidmatan operasi Pusat Data dan Pusat Pemulihan Bencana bagi proses Pendaftaran Pelajar Baharu Prasiswazah yang terlibat dalam skop pensijilan ISMS merangkumi aktiviti berikut:</td>
<td>T/P</td>
</tr>
<tr>
<td>Dokumen Rujukan:
a. Prosedur Pengoperasian Pengurusan Pusat Data (UPM/ISMS/OPR/DC/P001)</td>
<td>Dokumen Rujukan:
b. Prosedur Pengoperasian Pengurusan Pusat Data (UPM/ISMS/OPR/DC/P001)
c. Disaster Recovery Plan (DRP) UPM (UPM/IDEC/100-23/1/4)
d. Prosedur Persediaan Penempatan dan Pendaftaran Masuk pelajar Baharu (UPM/OPR/KOLEJ/P002)
e. Prosedur Pengambilan Pelajar Baharu Program Pengajian Prasiswazah (UPM/PU/PS/P003)
f. Arahan Kerja Permohonan Kad Pintar (UPM/OPR/BKU/AK01/KAD PINTAR)</td>
<td>T</td>
</tr>
<tr>
<td>4.3.4 LOKASI SKOP PENSIJILAN ISMS UPM
Lokasi skop pelaksanaan pensijilan ISMS UPM adalah seperti butiran berikut:
<table><tr><th>LOKASI UTAMA</th></tr><tr><td>Universiti Putra Malaysia
Pejabat Naib Canselor
Universiti Putra Malaysia
43400 UPM Serdang
Selangor</td></tr><tr><th><s>LOKASI PERTAMA</s></th></tr><tr><td><s>Pusat Data Utama (DC)</s>
<s>Pusat Pembangunan Maklumat dan Komunikasi (iDEC-BETA)</s>
<s>Universiti Putra Malaysia</s></td></tr></table></td>
<td>4.3.4 LOKASI SKOP PENSIJILAN ISMS UPM
Lokasi skop pelaksanaan pensijilan ISMS UPM adalah seperti butiran berikut:
<table><tr><th colspan="2">LOKASI</th></tr><tr><td>Kolej Tujuh Belas (K17)</td><td>Kolej Enam Belas (K16)</td></tr><tr><td>Kolej Lima Belas (K15)</td><td>Kolej Empat Belas (K14)</td></tr><tr><td>Kolej Tiga Belas (K13)</td><td>Kolej Dua Belas (K12)</td></tr><tr><td>Kolej Sebelas (K11)</td><td>Kolej Sepuluh (K10)</td></tr><tr><td>Kolej Keenam (K6)</td><td>Kolej Kelima (K5)</td></tr><tr><td>Kolej Kedua (K2)</td><td>Kolej Canselor</td></tr><tr><td>Kolej Mohamed Rashid (KMR)</td><td>Kolej Tun Dr Ismail (KTDI)</td></tr><tr><td>Kolej Pendeta Za’ba (KPZ)</td><td>Kolej Tun Perak (KTP)</td></tr><tr><td colspan="2">Kolej Sultan Aleiddin Suleiman Shah (KOSASS)
Universiti Putra Malaysia,</td></tr></table></td>
<td>P</td>
</tr>
</table>

~~43400 UPM Serdang~~ ~~Selangor~~	
~~Tel : 03-8947 1236~~	~~Fax : 03-8946 7035~~
~~Tanggungjawab~~	~~Ketua Unit Pusat Data~~
~~Pelan Aras~~	~~Rujuk plan lantai bangunan di Lampiran A~~
~~LOKASI KEDUA~~	
~~Pusat Data Kedua (DRC)~~ ~~Pusat Pembangunan Maklumat dan Komunikasi (iDEC-EPSILON)~~ ~~Blok 2, UPM-MTDC Server Farm Complex~~ ~~43400 UPM Serdang~~ ~~Selangor~~	
~~Tel : 03-8947 1236~~	~~Fax : 03-8946 7035~~
~~Tanggungjawab~~	~~Ketua Unit Pusat Data~~
~~Pelan Aras~~	~~Rujuk plan lantai bangunan di Lampiran B~~

Rajah 3: Lokasi Pelaksanaan Pensijilan ISMS UPM

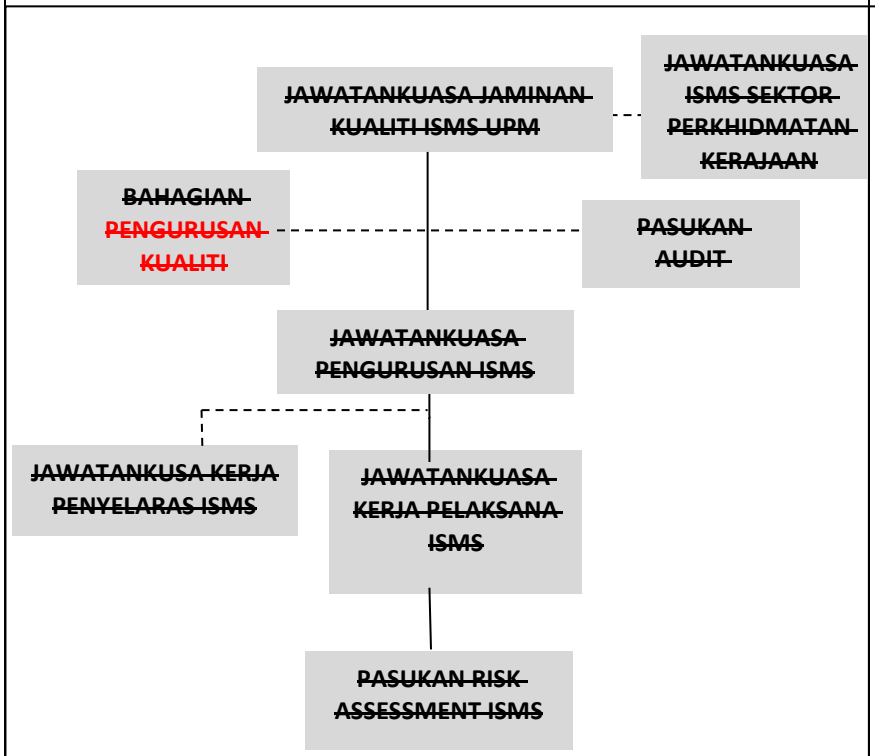
43400 UPM Serdang, Selangor	
Pusat Data Utama (DC) Pusat Pembangunan Maklumat dan Komunikasi (iDEC-BETA) Universiti Putra Malaysia 43400 UPM Serdang Selangor	
Pusat Pemulihan Bencana (DRC) Pusat Pembangunan Maklumat dan Komunikasi (iDEC-EPSILON) Blok 2, UPM-MTDC Server Farm Complex 43400 UPM Serdang Selangor	

Jadual 5 : Lokasi Pelaksanaan Pensijilan ISMS UPM

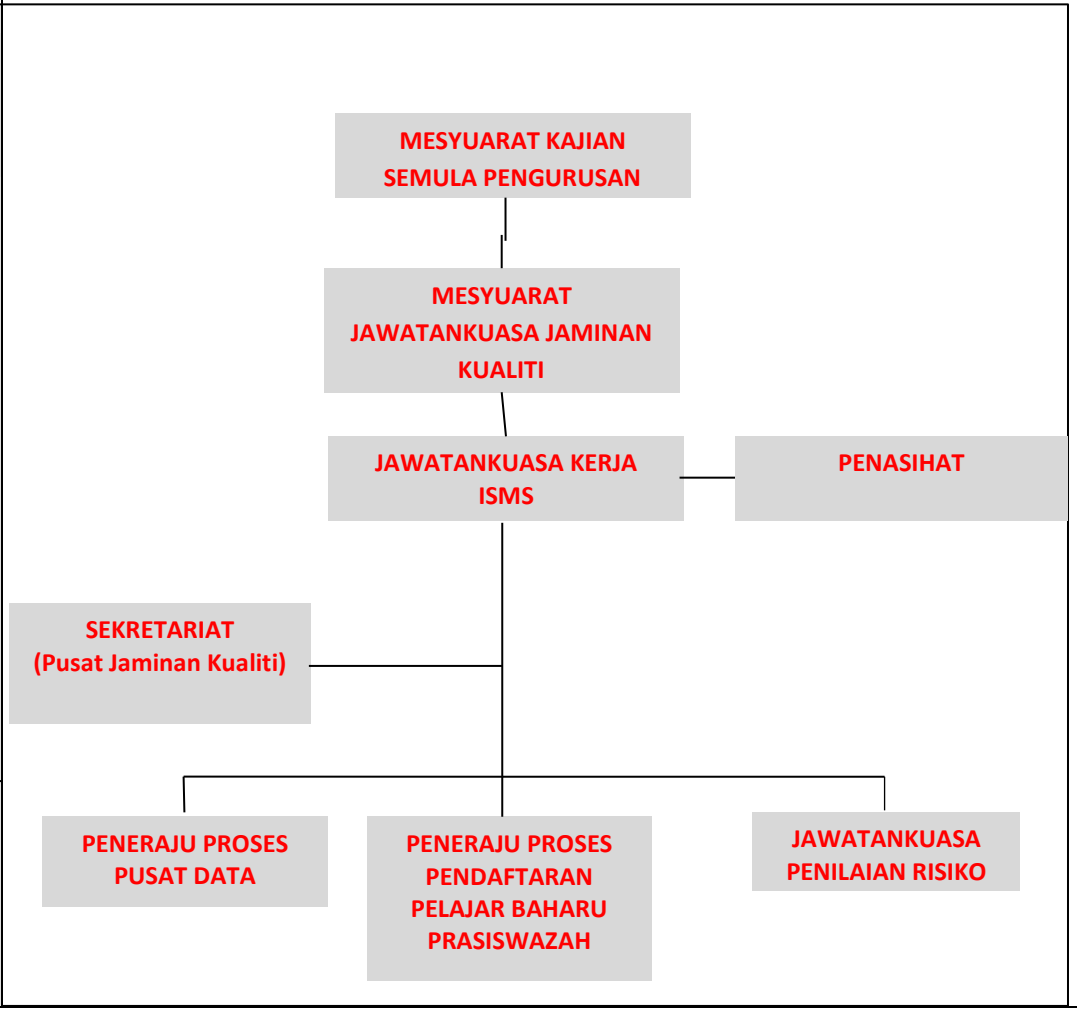
5.1	**~~KEPIMPINAN~~ DAN KOMITMEN**	**5.1** **KEPEMIMPINAN DAN KOMITMEN**	**P**
5.2.2	**Objektif Keselamatan Maklumat** Pihak Pengurusan UPM telah menetapkan Objektif Keselamatan Maklumat yang bersesuaian dengan fungsi yang terlibat bagi memastikan semua data dan maklumat di UPM adalah selamat. Untuk memastikan ISMS dilaksanakan dengan berkesan, Objektif Keselamatan Maklumat yang telah dikenalpasti adalah seperti berikut: a. Memastikan penilaian risiko dan pelan pemulihan risiko dilaksanakan apabila berlaku perubahan kepada dasar ISMS atau inventori yang termaktub dalam skop; b. Menjalankan ujian kesinambungan perkhidmatan ICT sekurang-kurangnya 1 kali setahun; c. Memastikan 80% staf telah diberi taklimat kesedaran mengenai ISMS dalam tempoh 3 tahun; d. Memastikan insiden ICT tidak melebihi 10 kali pada setiap tahun; e. Memastikan gangguan kepada ketersediaan rangkaian	**i. Objektif Keselamatan Maklumat** Pihak Pengurusan UPM telah menetapkan Objektif Keselamatan Maklumat yang bersesuaian dengan fungsi yang terlibat bagi memastikan semua data dan maklumat di UPM adalah selamat. Untuk memastikan ISMS dilaksanakan dengan berkesan, Objektif Keselamatan Maklumat yang telah dikenalpasti adalah seperti berikut: b. Memastikan semakan penilaian risiko dan pelan pemulihan risiko dilaksanakan sekurang-kurangnya sekali setahun ; c. Menjalankan ujian simulasi pelan pemulihan bencana sekurang-kurangnya 1 kali setahun; d. Memastikan 95% sokongan ICT (rangkaian, sistem aplikasi dan pangkalan data) terhadap proses pendaftaran pelajar baharu bebas dari gangguan setiap semester; e. Memastikan 100% pelajar yang berdaftar adalah pelajar yang mendapat tawaran; dan f. Memastikan 100% borang permohonan kad pelajar yang diterima diisi dengan lengkap.	**P**

(internet dan intranet) tidak melebihi 10% setiap tahun; f. Memastikan gangguan bekalan kuasa di Pusat Data dipulihkan dalam tempoh 24 jam; dan g. Memastikan 100% data dipulihkan dalam tempoh 48 jam selepas insiden.		

5.3.1 Struktur Organisasi ISMS



5.3.1 Struktur Organisasi ISMS



P

5.3.2 Peranan dan Tanggungjawab Organisasi ISMS UPM

PERANAN	TANGGUNGJAWAB
JAWATANKUASA JAMINAN KUALITI ISMS UPM	1. Memastikan kesesuaian, kecukupan dan keberkesanan pelaksanaan ISMS secara berkala; 2. Membuat penilaian ke atas peluang penambahbaikan dan keperluan perubahan kepada pengukuran keberkesanan; 3. Meluluskan sebarang cadangan pindaan dokumen skop pengurusan; dan ~~4.~~ Mengambil maklum keberkesanan pelaksanaan ISMS di peringkat ~~pentadbir proses.~~
BAHAGIAN PENGURUSAN KUALITI (BPQ)	~~1. Menyelaras Hubungan Badan Pensijilan SIRIM~~
~~**JAWATANKUASA PENGURUSAN ISMS UPM**~~	~~1. Memantau pelaksanaan ISMS;~~ ~~2. Memantau pencapaian objektif keselamatan;~~ ~~3. Melaksana penambahbaikan terhadap dokumentasi, proses dan perkhidmatan skop Sokongan dan operasi ISMS;~~ ~~4. Menyediakan laporan keberkesanan pelaksanaan ISMS;~~ ~~5. Membangunkan kriteria penerimaan risiko, tahap risiko dan pelan pemulihan risiko; dan~~ ~~6. Melaksanakan keputusan dan tindakan hasil Mesyuarat Kajian Semula Pengurusan ISMS.~~
~~**JAWATANKUASA KERJA**~~	~~1. Menyediakan analisis jurang, *Statement of Applicability* (SoA), penilaian risiko, pelan~~

5.3.2 Peranan dan Tanggungjawab Organisasi ISMS UPM

PERANAN	TANGGUNGJAWAB
MESYUARAT JAWATANKUASA JAMINAN KUALITI	1. Memastikan kesesuaian, kecukupan dan keberkesanan pelaksanaan Sistem Pengurusan ISO secara berkala; 2. Membuat penilaian ke atas peluang penambahbaikan dan keperluan perubahan kepada pengukuran keberkesanan ISMS; 3. Meluluskan sebarang cadangan pindaan dokumen skop pengurusan; dan 4. Mengambil maklum keberkesanan pelaksanaan ISO di peringkat Peneraju Proses dan Pusat Tanggungjawab (PTJ).
SEKRETARIAT PUSAT JAMINAN KUALITI	2. Merancang dan mengurus audit dalaman dan audit badan pensijilan Sistem Pengurusan ISO peringkat UPM; 3. Menyelaras dan memantau pelaksanaan tindakan penemuan audit dalaman dan audit badan pensijilan; 4. Membantu dalam Mesyuarat Jawatankuasa Kerja ISMS; dan 5. Membantu dalam pembangunan dan latihan ISMS.
JAWATANKUASA KERJA ISMS	1. Memantau keberkesanan pelaksanaan ISMS; 2. Memantau pencapaian objektif kualiti; 3. Melaksana penambahbaikan terhadap dokumentasi, proses dan perkhidmatan; ~~4.~~ Menyediakan laporan keberkesanan pelaksanaan Sistem Pengurusan Keselamatan Maklumat; 5. Memantau dan menyemak carta perbatuan ISMS; 6. Membangunkan kriteria penerimaan risiko, tahap risiko dan *risk treatment plan;* 7. Melaksanakan keputusan dan tindakan hasil Mesyuarat Kajian Semula Pengurusan ISMS; 8. Membangun dan menyelenggara pengurusan dokumen dan rekod pelaksanaan ISMS; dan

P

~~**PELAKSANA ISMS**~~	~~pemulihan risiko dan prosedur-prosedur;~~ ~~2. Melaksanakan pelan pemulihan risiko; dan~~ ~~3. Membangun dan mengukur keberkesanan kawalan ISMS.~~
~~**JAWATANKUASA KERJA PENYELARAS ISMS (URUS SETIA)**~~	~~1. Merancang latihan berkaitan ISMS;~~ ~~2. Urus setia kepada pelaksanaan Jawatankuasa ISMS; dan~~ ~~3. Memantau tindakan susulan ke atas tindakan pembetulan dan peluang penambahbaikan ISMS serta menyelenggara rekod berkaitan.~~
~~**PASUKAN AUDIT DALAMAN ISMS**~~	~~1. Melaksana Audit Dalaman ISMS berdasarkan keperluan standard.~~ ~~2. Menyediakan Laporan Audit Dalaman ISMS;~~ ~~3. Melaporkan penemuan Audit Dalaman ISMS ke Jawatankuasa Jaminan Kualiti (JKJK) ISMS dan Jawatankuasa MKSP ISMS; dan~~ ~~4. Menjalankan audit susulan bagi mengesahkan tindakan pembetulan yang dilaksanakan.~~
PASUKAN PENILAIAN RISIKO	1. Mengurus dan melaksanakan aktiviti penilaian berisiko; 2. Mengendalikan semakan semula ouput dan dokumen sebelum disampaikan kepada Penasihat Projek; 3. Menilai keputusan, menilai jurang dan menyediakan laporan *High Level Recommendation* (HLR) dan Pelan Pemulihan Risiko.

	9. Mengambil tindakan ke atas tindakan pembetulan, pencegahan dan peluang penambahbaikan.
PENERAJU PROSES	4. Menyediakan analisis jurang, Statement of Applicability (SoA) dan prosedur berkaitan; 5. Menyediakan prosedur dan kawalan dalam ISO/IEC 27001:2013; 6. Melaksanakan penilaian risiko dan pelan pemulihan risiko; 7. Menyediakan objektif keselamatan dan kaedah pengukuran keberkesanan kawalan ISMS; 8. Mengukur keberkesanan kawalan ISMS; dan 9. Memantau dan menilai pelaksanaan ISMS.
JAWATANKUASA PENILAIAN RISIKO	4. Mengurus dan melaksanakan aktiviti penilaian berisiko; 5. Mengendalikan semakan semula ouput dan dokumen sebelum disampaikan kepada Penasihat Projek; 6. Menilai keputusan, menilai jurang dan menyediakan laporan *High Level Recommendation* (HLR) dan Pelan Pemulihan Risiko.

6.1.2 Penilaian Risiko Penilaian risiko aset ICT dilaksanakan berasaskan Metodologi Penilaian Risiko Terperinci MyRAM (*Malaysian Public Sector ICT Risk Assessment Methodology*) berpandukan kepada Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.	**6.1.2 Penilaian Risiko** Sebelas (11) langkah utama dalam proses penilaian risiko aset adalah seperti berikut:  	**T**

6.2 PELAN PERANCANGAN PENCAPAIAN OBJEKTIF KESELAMATAN MAKLUMAT

Pihak pengurusan telah membangunkan Objektif Keselamatan Maklumat yang bersesuaian dengan fungsi yang terlibat. Objektif Keselamatan Maklumat yang telah diwujudkan adalah bersandarkan kepada Petunjuk Prestasi ICT atau *ICT Key Performance Indicators* (KPI) yang telah ditetapkan adalah seperti berikut:

BIL.	OBJEKTIF KESELAMATAN	SUMBER	TANGGUNGJAWAB	RUJUKAN
1.	Memastikan penilaian risiko dan pelan pemulihan risiko dilaksanakan apabila berlaku perubahan kepada polisi ISMS atau inventori yang termaktub dalam skop	Laporan Penilaian Risiko dan Pelan Pemulihan Risiko	JK ISMS	Carta perbatuan pelaksanaan ISMS
2.	Menjalankan ujian kesinambungan perkhidmatan ICT sekurang-kurangnya 1 kali setahun	Laporan ujian kesinambungan perkhidmatan	Pengarah IDEC	Pelan Pemulihan Bencana ICT (DRP ICT)
3.	Memastikan 80% staf telah diberi taklimat kesedaran mengenai ISMS dalam tempoh 3 tahun	Senarai kehadiran taklimat	JK Kerja Penyelaras ISMS	Carta perbatuan pelaksanaan ISMS

G

~~4.~~	~~Memastikan insiden ICT tidak melebihi 10 kali pada setiap tahun~~	~~KPI ICT~~	~~Pengarah IDEC~~	~~Log Insiden ICT~~
~~5.~~	~~Memastikan gangguan kepada ketersediaan rangkaian (internet & intranet) tidak melebihi 10% setiap tahun~~	~~KPI ICT~~	~~Pengarah IDEC~~	~~Refer unet~~
~~6.~~	~~Memastikan gangguan bekalan kuasa di Pusat Data dipulihkan dalam tempoh 24 jam~~	~~KPI PPPA~~	~~Pengarah PPPA~~	~~Refer pppa~~
~~7.~~	~~Memastikan 100% data dipulihkan dalam tempoh 48 jam selepas insiden~~	~~KPI ICT~~	~~Pengarah IDEC~~	~~Pelan Pemulihan Bencana ICT (DRP ICT)~~

7.4 KOMUNIKASI

BIL.	PIHAK BERKAITAN	MEDIUM KOMUNIKASI	BILA DIPERLUKAN	TANGGUNGAWAB	PROSES TERLIBAT
1.	Pelajar	~~1. u-respon~~ ~~2. email rasmi~~ ~~3. laman web PTJ~~	~~Sesi pendaftaran pelajar~~	~~1. Bahagian Akademik~~ ~~2. Bahagian Kewangan~~ ~~3. PPSK~~	~~1. Maklumat Pelajar~~ ~~2. Maklumat Kewangan Pelajar~~ ~~3. Maklumat profil Universiti~~

7.4 KOMUNIKASI

BIL.	PIHAK BERKAITAN	PERKARA YANG DIKOMUNIKASI	BILA KOMUNIKASI DILAKSANA	TANGGUNGAWAB		MEDIUM KOMUNIKASI
				UPM	Pihak berkaitan	
KOMUNIKASI DALAMAN						
1.	Pelajar	Perkara berkaitan proses pendaftaran pelajar	Minggu Perkasa Putra	Pegawai HEPA (Jwtn)	Pelajar	Hebahan melalui laman web HEPA, portal SMP dan USPOT
2.	Staf	Perkara berkaitan proses pendaftaran pelajar	Selewat-lewatnya sebulan sebelum Minggu Perkasa Putra	Pegawai HEPA	1. Pusat Data 2. Pusat Kesihatan Universiti 3. Bahagian Keselamatan 4. Pejabat Bursar	1. Program Perutusan Tahun Baru Naib Canselor 2. Taklimat khas pelaksanaan ISMS 3. Latihan

P

2.	Staf	1. Email rasmi 2. Mesyuarat 3. Surat 4. buletin	Berterusan secara berkala ~~melalui taklimat~~	~~1. Bahagian Akademik~~ ~~2. Bahagian Kewangan~~ 3. ~~PPSK~~	~~1. Maklumat Pelajar~~ ~~2. Maklumat Kewangan Staf~~ ~~3. Maklumat profil Universiti~~ 4. ~~Maklumat penyelidikan~~
~~3.~~	~~Kementerian Pendidikan Malaysia (KPM)~~	~~1. Surat~~ ~~2. Emel rasmi~~ ~~3. Mesyuarat~~	~~Mesyuarat. ..~~	~~1. Bahagian Akademik~~ ~~2. Bahagian Kewangan~~ ~~3. PPSK~~	~~1. Maklumat Pelajar~~ ~~2. Maklumat Kewangan Staf~~ ~~3. Maklumat profil Universiti~~
~~4.~~	~~Jabatan Perkhidmatan Awam~~	~~1. Surat~~ ~~2. Emel rasmi~~ ~~3. Mesyuarat~~		~~1. Bahagian Akademik~~ ~~2. Bahagian Kewangan~~ ~~3. PPSK~~	~~1. Maklumat Staf~~ ~~2. Maklumat Kewangan Staf~~ ~~3. Maklumat profil Universiti~~

						pelaksanaan ISMS
	KOMUNIKASI LUARAN					
3.	Pembekal	Perkara berkaitan proses pendaftaran pelajar	Selewat-lewatnya sebulan sebelum Minggu Perkasa Putra	Ketua Bahagian Operasi Aplikasi	Staf Encoral Digital Solution Sdn Bhd (Pengurus Projek : Suhaimi Jantan)	Surat
4.	Kementerian Pengajian Tinggi (KPT)	Maklumat pelajar ditawar masuk ke UPM	Berterusan secara berkala	Bahagian Akademik		Surat

~~5.~~	~~Pembekal~~	~~1. Urespon 2. Web 3. Papan kenyataan 4. Job sheet~~	~~Taklimat~~	~~1. Bahagian Akademik 2. Bahagian Kewangan 3. PPSK~~	~~1. Maklumat Staf/Pelajar 2. Maklumat Kewangan Staf 3. Maklumat profil Universiti~~			
~~6.~~	~~Ibu bapa~~	~~1. Surat~~	~~Surat tawaran~~	~~1. Bahagian Akademik 2. PPSK~~	~~1. Maklumat Pelajar 2. Maklumat profil Universiti~~			
~~7.~~	~~Awam~~	~~1. Laman web~~	~~Sepanjang masa~~	~~1. PPSK~~	~~Maklumat profil Universiti~~			

7.5.3 Kawalan Dokumen

Mengurus, mengawal dan melindungi semua dokumen ISMS. Dokumen ISMS yang dinyatakan dalam Senarai Utama Dokumen Terkawal selaras dengan ~~Prosedur Kawalan Dokumen ISMS.~~

Kawalan rekod dilaksanakan berdasarkan tindakan berikut:

a. Rekod ISMS (rekod fizikal dan elektronik) dan tempoh penyimpanannya dikenal pasti dalam setiap prosedur ISMS;
b. Tatacara bagi mengurus, mengawal, mengenalpasti, menyimpan, mendapatkan semula dan melupuskan rekod fizikal dan elektronik didokumenkan; dan
c. Pelupusan rekod ISMS fizikal dibuat mengikut ~~Prosedur Kawalan Rekod ISMS.~~

7.5.3 Kawalan Dokumen

Mengurus, mengawal dan melindungi semua dokumen ISMS. Dokumen ISMS yang dinyatakan dalam Senarai Utama Dokumen Terkawal selaras dengan Prosedur Kawalan Dokumen dan Rekod.

Kawalan rekod dilaksanakan berdasarkan tindakan berikut:

a. Rekod ISMS (rekod fizikal dan elektronik) dan tempoh penyimpanannya dikenal pasti dalam setiap prosedur ISMS;
b. Tatacara bagi mengurus, mengawal, mengenalpasti, menyimpan, mendapatkan semula dan melupuskan rekod fizikal dan elektronik didokumenkan; dan
c. Pelupusan rekod ISMS fizikal dibuat mengikut Prosedur Kawalan Dokumen dan Rekod.

P

9.2	**AUDIT DALAMAN** Tanggungjawab dan keperluan untuk merancang, melaksana, melapor keputusan audit dan mengurus rekod dengan merujuk kepada Prosedur Kawalan Rekod ISMS dan Prosedur Audit Dalaman ~~ISMS~~. Dokumen Rujukan: a. Prosedur Audit Dalaman ~~ISMS~~ (UPM/ISMS/PGR/P003)	**9.2**	**AUDIT DALAMAN** Tanggungjawab dan keperluan untuk merancang, melaksana, melapor keputusan audit dan mengurus rekod dengan merujuk kepada Prosedur Kawalan Dokumen dan Rekod dan Prosedur Audit Dalaman ISO. Dokumen Rujukan: b. Prosedur Audit Dalaman ISO (UPM/PGR/P004)	**P**
9.3	**KAJIAN SEMULA PENGURUSAN** Keputusan mesyuarat direkodkan dan Jawatankuasa ~~Pengurusan~~ ISMS bertanggungjawab memastikan tindakan susulan diambil. Semua rekod yang berkaitan hendaklah diselenggara dengan sempurna.	**9.3**	**KAJIAN SEMULA PENGURUSAN** Keputusan mesyuarat direkodkan dan Jawatankuasa Kerja ISMS bertanggungjawab memastikan tindakan susulan diambil. Semua rekod yang berkaitan hendaklah diselenggara dengan sempurna.	

LAMPIRAN 3

OBJEKTIF SISTEM PENGURUSAN KESELAMATAN MAKLUMAT

Pihak Pengurusan UPM telah menetapkan Objektif Keselamatan Maklumat yang bersesuaian dengan fungsi yang terlibat bagi memastikan semua data dan maklumat di UPM adalah selamat. Untuk memastikan ISMS dilaksanakan dengan berkesan, Objektif Keselamatan Maklumat yang telah dikenalpasti adalah seperti berikut:

a. Memastikan semakan penilaian risiko dan pelan pemulihan risiko dilaksanakan sekurang-kurangnya sekali setahun;

b. Menjalankan ujian simulasi pelan pemulihan bencana ICT sekurang-kurangnya 1 kali setahun;

c. Memastikan 95% sokongan ICT (rangkaian, sistem aplikasi dan pangkalan data) terhadap proses pendaftaran pelajar baharu bebas dari gangguan setiap semester;

d. Memastikan 100% pelajar yang berdaftar adalah pelajar yang mendapat tawaran; dan

e. Memastikan 100% borang permohonan kad pelajar yang diterima diisi denganlengkap.

SULIT

LAMPIRAN 4

PEMBAYARAN PELAJAR BAHARU

Risk Treatment Plan Summary Report

Control ID	Control Name	Asset Group						Total
		Hardware	Software	People	Information and Data	Services (supporting)	Services (accessibility)	
A.7 Human resource security								
A.7.2	During employment							
A.7.2.1	Management responsibilities	0	0	2	0	0	0	2
A.7.2.2	Information security awareness, education and training	0	0	28	0	0	0	28
A.8 Asset management								
A.8.1	Responsibility for assets							
A.8.1.2	Ownership of assets	0	0	0	0	2	0	2
A.11 Physical and environmental security								
A.11.2	Equipment							
A.11.2.2	Supporting utilities	2	0	0	0	0	0	2
A.18 Compliance								
A.18.1	Compliance with legal and contractual requirements							
A.18.1.1	Identification of applicable legislation and contractual requirements	0	0	11	0	0	0	11
A.18.1.2	Intellectual property rights	0	0	3	0	0	0	3

SULIT

LAMPIRAN 4

PEMBAYARAN PELAJAR BAHARU

Asset Group	Num. of Assets	Risk Level			High Level Recommendation (Decision/Recommendation)				Risk Treatment Plan	
		High	Medium	Low	Accept	Reduce	Transfer	Avoid	Yes	No
Hardware	2	1	1	0	0/0	2/2	0/0	0/0	2	0
Software	0	0	0	0	0/0	0/0	0/0	0/0	0	0
People	15	0	29	0	0/0	29/29	0/0	0/0	29	0
Information and Data	2	0	2	0	0/0	2/2	0/0	0/0	2	0
Services (supporting)	1	0	1	0	0/0	1/1	0/0	0/0	1	0
Services (accessibility)	0	0	0	0	0/0	0/0	0/0	0/0	0	0
Total	**20**	**1**	**33**	**0**	**0/0**	**34/34**	**0/0**	**0/0**	**34**	**0**

SULIT

LAMPIRAN 4

SISTEM APLIKASI KEWANGAN

Risk Treatment Plan Summary Report

Control ID	Control Name	Asset Group						Total
		Hardware	Software	People	Information and Data	Services (supporting)	Services (accessibility)	
A.7 Human resource security								
A.7.1	Prior to employment							
A.7.1.1	Screening	0	0	3	0	0	0	3
A.7.2	During employment							
A.7.2.1	Management responsibilities	0	0	3	0	0	0	3
A.7.2.2	Information security awareness, education and training	0	0	3	0	0	0	3
A.7.2.3	Disciplinary process	0	0	3	0	0	0	3
A.11 Physical and environmental security								
A.11.2	Equipment							
A.11.2.2	Supporting utilities	25	0	0	0	0	0	25
A.11.2.4	Equipment maintenance	25	0	0	0	0	0	25
A.12 Operations security								
A.12.1	Operational procedures and responsibilities							
A.12.1.3	Capacity management	8	0	0	0	0	0	8
A.13 Communications security								
A.13.1	Network security management							
A.13.1.1	Network controls	8	0	0	0	0	0	8
A.17 Information security aspects of business continuity management								
A.17.1	Information security continuity							
A.17.1.1	Planning information security continuity	16	0	0	0	0	0	16
A.17.1.2	Implementing information security continuity	16	0	0	0	0	0	16
A.17.1.3	Verify, review and evaluate information security continuity	15	0	0	0	0	0	15

SULIT

LAMPIRAN 4

SISTEM APLIKASI KEWANGAN

Asset Group	Num. of Assets	Risk Level			High Level Recommendation (Decision/Recommendation)				Risk Treatment Plan	
		High	Medium	Low	Accept	Reduce	Transfer	Avoid	Yes	No
Hardware	8	0	32	8	8/8	32/32	0/0	0/0	32	8
Software	0	0	0	0	0/0	0/0	0/0	0/0	0	0
People	3	0	3	6	6/6	3/3	0/0	0/0	3	6
Information and Data	0	0	0	0	0/0	0/0	0/0	0/0	0	0
Services (supporting)	0	0	0	0	0/0	0/0	0/0	0/0	0	0
Services (accessibility)	0	0	0	0	0/0	0/0	0/0	0/0	0	0
Total	**11**	**0**	**35**	**14**	**14/14**	**35/35**	**0/0**	**0/0**	**35**	**14**

SULIT

LAMPIRAN 4

PENGESAHAN LAPORAN
PEMERIKSAAN KESIHATAN

Asset Group	Num. of Assets	Risk Level			High Level Recommendation (Decision/Recommendation)				Risk Treatment Plan	
		High	Medium	Low	Accept	Reduce	Transfer	Avoid	Yes	No
Hardware	8	0	0	8	8/8	0/0	0/0	0/0	0	8
Software	0	0	0	0	0/0	0/0	0/0	0/0	0	0
People	114	0	0	228	228/228	0/0	0/0	0/0	0	228
Information and Data	0	0	0	0	0/0	0/0	0/0	0/0	0	0
Services (supporting)	0	0	0	0	0/0	0/0	0/0	0/0	0	0
Services (accessibility)	0	0	0	0	0/0	0/0	0/0	0/0	0	0
Total	**122**	**0**	**0**	**236**	**236/236**	**0/0**	**0/0**	**0/0**	**0**	**236**

SULIT

LAMPIRAN 4

PENDAFTARAN KOLEJ PELAJAR

Asset Group	Num. of Assets	Risk Level			High Level Recommendation (Decision/Recommendation)				Risk Treatment Plan	
		High	Medium	Low	Accept	Reduce	Transfer	Avoid	Yes	No
Hardware	0	0	0	0	0/0	0/0	0/0	0/0	0	0
Software	17	0	0	34	34/34	0/0	0/0	0/0	0	34
People	51	0	0	51	51/51	0/0	0/0	0/0	0	51
Information and Data	0	0	0	0	0/0	0/0	0/0	0/0	0	0
Services (supporting)	51	0	0	51	51/51	0/0	0/0	0/0	0	51
Services (accessibility)	18	0	0	36	36/36	0/0	0/0	0/0	0	36
Total	**137**	**0**	**0**	**172**	**172/172**	**0/0**	**0/0**	**0/0**	**0**	**172**

Asset Group	Num. of Assets	Risk Level			High Level Recommendation (Decision/Recommendation)				Risk Treatment Plan	
		High	Medium	Low	Accept	Reduce	Transfer	Avoid	Yes	No
Hardware	0	0	0	0	0/0	0/0	0/0	0/0	0	0
Software	2	0	0	4	4/4	0/0	0/0	0/0	0	4
People	1	0	0	2	2/2	0/0	0/0	0/0	0	2
Information and Data	1	0	0	1	1/1	0/0	0/0	0/0	0	1
Services (supporting)	1	0	0	1	1/1	0/0	0/0	0/0	0	1
Services (accessibility)	0	0	0	0	0/0	0/0	0/0	0/0	0	0
Total	**5**	**0**	**0**	**8**	**8/8**	**0/0**	**0/0**	**0/0**	**0**	**8**

SULIT

LAMPIRAN 4

SISTEM SOKONGAN PUSAT DATA

Risk Treatment Plan Summary Report

Control ID	Control Name	Asset Group						Total
		Hardware	Software	People	Information and Data	Services (supporting)	Services (accessibility)	
A.6 Organization of information security								
A.6.1	Internal organization							
A.6.1.1	Information security roles and responsibilities	9	0	0	0	0	12	21
A.7 Human resource security								
A.7.1	Prior to employment							
A.7.1.1	Screening	0	0	11	0	0	0	11
A.7.2	During employment							
A.7.2.1	Management responsibilities	0	0	11	0	0	0	11
A.7.2.2	Information security awareness, education and training	34	0	11	0	0	0	45
A.7.2.3	Disciplinary process	0	0	11	0	0	0	11
A.11 Physical and environmental security								
A.11.1	Secure areas							
A.11.1.1	Physical security perimeter	0	0	0	0	0	38	38
A.11.1.2	Physical entry controls	0	0	0	0	0	6	6
A.11.1.3	Securing offices, rooms and facilities	0	0	0	7	0	0	7
A.11.2	Equipment							
A.11.2.2	Supporting utilities	27	0	0	0	0	0	27
A.11.2.4	Equipment maintenance	36	0	0	0	38	34	108
A.12 Operations security								
A.12.1	Operational procedures and responsibilities							
A.12.1.1	Documented operating procedures	25	2	1	7	2	0	37
A.12.1.3	Capacity management	9	0	0	0	0	0	9
A.12.2	Protection from malware							
A.12.2.1	Controls against malware	0	2	0	0	0	0	2
A.12.4	Logging and monitoring							

SULIT

LAMPIRAN 4

SISTEM SOKONGAN PUSAT DATA

Control ID	Control Name	Asset Group						Total
		Hardware	Software	People	Information and Data	Services (supporting)	Services (accessibility)	
A.12.4.1	Event logging	8	0	1	0	0	0	9
A.13 Communications security								
A.13.1	Network security management							
A.13.1.1	Network controls	9	0	0	0	4	1	14
A.14 System acquisition, development and maintenance								
A.14.2	Security in development and support processes							
A.14.2.9	System acceptance testing	0	0	0	0	0	2	2
A.15 Supplier service delivery management								
A.15.2	Supplier service delivery management							
A.15.2.1	Monitoring and review of supplier services	0	0	0	0	17	1	18
A.17 Information security aspects of business continuity management								
A.17.1	Information security continuity							
A.17.1.1	Planning information security continuity	27	0	0	0	0	12	39
A.17.1.2	Implementing information security continuity	27	0	0	0	0	12	39
A.17.1.3	Verify, review and evaluate information security continuity	27	0	0	0	0	12	39

SULIT

LAMPIRAN 4

SISTEM SOKONGAN PUSAT DATA

Asset Group	Num. of Assets	Risk Level			High Level Recommendation (Decision/Recommendation)				Risk Treatment Plan	
		High	Medium	Low	Accept	Reduce	Transfer	Avoid	Yes	No
Hardware	9	0	57	0	0/0	57/57	0/0	0/0	57	0
Software	37	0	0	74	72/72	2/2	0/0	0/0	2	72
People	13	0	12	23	23/23	12/12	0/0	0/0	12	23
Information and Data	47	0	7	40	40/40	7/7	0/0	0/0	7	40
Services (supporting)	64	0	22	46	46/46	20/20	2/2	0/0	22	46
Services (accessibility)	36	11	41	0	0/0	52/52	0/0	0/0	52	0
Total	**206**	**11**	**139**	**183**	**181/181**	**150/150**	**2/2**	**0/0**	**152**	**181**

SULIT

LAMPIRAN 4

SISTEM PANGKALAN DATA

Risk Treatment Plan Summary Report

Control ID	Control Name	Asset Group						Total
		Hardware	Software	People	Information and Data	Services (supporting)	Services (accessibility)	
A.6 Organization of information security								
A.6.1	Internal organization							
A.6.1.1	Information security roles and responsibilities	8	0	0	0	0	0	8
A.7 Human resource security								
A.7.2	During employment							
A.7.2.2	Information security awareness, education and training	16	0	6	0	0	0	22
A.7.2.3	Disciplinary process	0	0	6	0	0	0	6
A.9 Access control								
A.9.4	System and application access control							
A.9.4.1	Information access restriction	0	0	0	7	0	0	7
A.11 Physical and environmental security								
A.11.2	Equipment							
A.11.2.2	Supporting utilities	24	0	0	0	0	0	24
A.11.2.4	Equipment maintenance	32	0	0	0	0	0	32
A.12 Operations security								
A.12.1	Operational procedures and responsibilities							
A.12.1.1	Documented operating procedures	8	0	0	7	0	0	15
A.12.1.3	Capacity management	8	0	0	0	0	0	8
A.13 Communications security								
A.13.1	Network security management							
A.13.1.1	Network controls	8	0	0	0	0	0	8
A.17 Information security aspects of business continuity management								
A.17.1	Information security continuity							
A.17.1.1	Planning information security continuity	24	0	0	0	0	0	24
A.17.1.2	Implementing information security continuity	24	0	0	0	0	0	24

SULIT

LAMPIRAN 4

SISTEM PANGKALAN DATA

Control ID	Control Name	Asset Group						Total
		Hardware	Software	People	Information and Data	Services (supporting)	Services (accessibility)	
A.17.1.3	Verify, review and evaluate information security continuity	24	0	0	0	0	0	24

SULIT

LAMPIRAN 4

SISTEM PANGKALAN DATA

Asset Group	Num. of Assets	Risk Level			High Level Recommendation (Decision/Recommendation)				Risk Treatment Plan	
		High	Medium	Low	Accept	Reduce	Transfer	Avoid	Yes	No
Hardware	8	0	40	0	0/0	40/40	0/0	0/0	40	0
Software	0	0	0	0	0/0	0/0	0/0	0/0	0	0
People	6	0	6	12	12/12	6/6	0/0	0/0	6	12
Information and Data	7	0	7	0	0/0	7/7	0/0	0/0	7	0
Services (supporting)	0	0	0	0	0/0	0/0	0/0	0/0	0	0
Services (accessibility)	0	0	0	0	0/0	0/0	0/0	0/0	0	0
Total	**21**	**0**	**53**	**12**	**12/12**	**53/53**	**0/0**	**0/0**	**53**	**12**

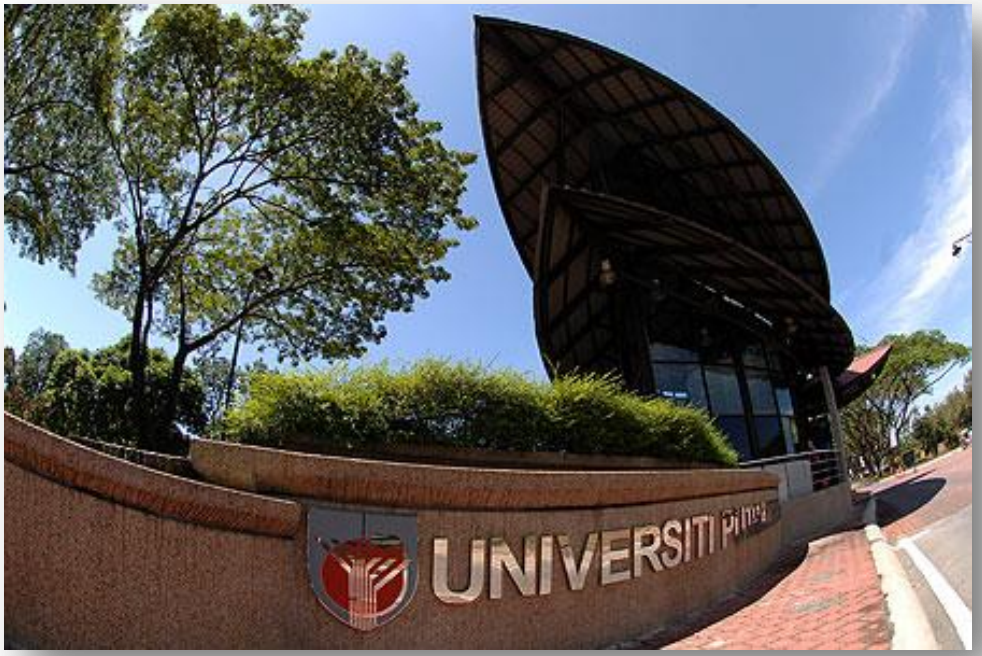
SULIT

LAMPIRAN 4

SISTEM APLIKASI MAKLUMAT PELAJAR

Asset Group	Num. of Assets	Risk Level			High Level Recommendation (Decision/Recommendation)				Risk Treatment Plan	
		High	Medium	Low	Accept	Reduce	Transfer	Avoid	Yes	No
Hardware	30	0	0	210	210/210	0/0	0/0	0/0	0	210
Software	0	0	0	0	0/0	0/0	0/0	0/0	0	0
People	5	0	0	15	15/15	0/0	0/0	0/0	0	15
Information and Data	0	0	0	0	0/0	0/0	0/0	0/0	0	0
Services (supporting)	0	0	0	0	0/0	0/0	0/0	0/0	0	0
Services (accessibility)	0	0	0	0	0/0	0/0	0/0	0/0	0	0
Total	**35**	**0**	**0**	**225**	**225/225**	**0/0**	**0/0**	**0/0**	**0**	**225**

LAMPIRAN 5



STATEMENT OF APPLICABILITY

Isu 01, Semakan 07

UNIVERSITI PUTRA MALAYSIA KE ARAH PENSIJILAN SEMULA ISMS ISO/IEC 27001:2013

ANNEX A

#	Clauses
A.5	Information security policies
A.6	Organization of information security
A.7	Human resource security
A.8	Asset management
A.9	Access control
A.10	Cryptography
A.11	Physical and environmental security
A.12	Operations security
A.13	Communications security
A.14	System acquisition, development and maintenance
A.15	Supplier relationships
A.16	Information security incident management
A.17	Information security aspects of business continuity management
A.18	Compliance

UNIVERSITI PUTRA MALAYSIA KE ARAH PENSIJILAN SEMULA ISMS ISO/IEC 27001:2013

ANNEX A

#	Clauses
A.5	Information security policies
A.6	Organization of information security
A.7	Human resource securi
A.8	Asset management
A.9	Access control
A.10	Cryptography
A.11	Physical and environm
A.12	Operations security
A.13	Communications secur
A.14	System acquisition, de
A.15	Supplier relationships
A.16	Information security incident management
A.17	Information security aspects of business continuity management
A.18	Compliance

Melibatkan :
14 klausa
35 kategori
114 kontrol

UNIVERSITI PUTRA MALAYSIA KE ARAH PENSIJILAN SEMULA ISMS ISO/IEC 27001:2013

PENGECUALIAN

A.6.1.5 Information security in project management Information security shall be addressed in project management, regardless of the type of the project

Tiada sebarang pengurusan projek terlibat dalam pelaksanaan ISMS di bawah skop pensijilan

UNIVERSITI PUTRA MALAYSIA KE ARAH PENSIJILAN SEMULA ISMS ISO/IEC 27001:2013

PENGECUALIAN

A.6.2.2 Teleworking A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.

Pusat Data : Pentadbir Sistem tidak dibenarkan untuk akses dari luar UPMNET. Akses hanya dibenarkan melalui bilik console yang telah disediakan di Pusat Data.

Proses Pendaftaran : Tidak libatkan perkhidmatan teleworking dan teleworking site

UNIVERSITI PUTRA MALAYSIA KE ARAH PENSIJILAN SEMULA ISMS ISO/IEC 27001:2013

PTJ/PIHAK TERLIBAT

1. Pusat Pembangunan Maklumat dan Komunikasi (iDEC)
2. Bahagian Pengurusan Kualiti (BPQ)
3. Pejabat Penasihat Undang-undang
4. Bahagian Pengurusan Sumber Manusia
5. Bahagian Pembangunan Sumber Manusia
6. Bahagian Perkhidmatan Sumber Manusia
7. Pejabat Bursar
8. Seksyen Latihan, Pejabat Pendaftar
9. Bahagian Akademik
10. Bahagian Hal Ehwal Pelajar & Alumni
11. 17 Kolej Kediaman UPM
12. Pejabat Strategi Korporat dan Komunikasi (COsCOMM

UNIVERSITI PUTRA MALAYSIA KE ARAH PENSIJILAN SEMULA ISMS ISO/IEC 27001:2013

Annex A

BAHAGIAN PENGURUSAN SUMBER MANUSIA
A.7 Human Resource Security
A.7.1 Prior to employment
A.7.2 During Employment
A.7.3 Termination and change of employment

BAHAGIAN PERKHIDMATAN SUMBER MANUSIA
A.8.2 Information Classification
- i. Classification
- ii. Labelling
- iii. Handling

A. 8.3 Media Handling
- i. Management of removable media
- ii. Disposal Media

UNIVERSITI PUTRA MALAYSIA KE ARAH PENSIJILAN SEMULA ISMS ISO/IEC 27001:2013

PTJ/PIHAK TERLIBAT

BAHAGIAN PEMBANGUNAN SUMBER MANUSIA
A.7.2.2 Information security awareness, education and training

BAHAGIAN HAL EHWAL PELAJAR & ALUMNI
A.12.1.2 Change management
A.12.1.3 Capacity management

PEJABAT BURSAR
A.15 Information security in supplier relationship

PTJ/PIHAK TERLIBAT

UNIVERSITI PUTRA MALAYSIA KE ARAH PENSIJILAN SEMULA ISMS ISO/IEC 27001:2013

PEJABAT STRATEGI KORPORAT DAN KOMUNIKASI (COSCOMM)
A.17.1 Information Security Continuity

PEJABAT PENASIHAT UNDANG-UNDANG
A.18.1 Compliance with legal and contractual requirements

PTJ/PIHAK TERLIBAT

UNIVERSITI PUTRA MALAYSIA KE ARAH PENSIJILAN SEMULA ISMS ISO/IEC 27001:2013

PEJABAT STRATEGI KORPORAT DAN KOMUNIKASI (COSCOMM)
A.17.1 Information Security Continuity

PEJABAT PENASIHAT UNDANG-UNDANG
A.18.1 Compliance with legal and contractual requirements

SEKIAN

TERIMAKASIH

STATEMENT OF APPLICABILITY (SoA)

UNIVERSITI PUTRA MALAYSIA

No. Semakan: 07 No. Isu: 01 Tarikh : 16/11/2015

	OPERASI PERKHIDMATAN SOKONGAN PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 1 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

STATEMENT OF APPLICABILITY

1.0 PENGENALAN

Dokumen penyataan pemakaian *Statement of Applicability (*SoA) menggariskan *control objectives* dan *controls* di Annex A dalam Standard 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 PENYATAAN PEMAKAIAN *(*SoA)

3.1 PENYEDIAAN SoA

Proses yang terlibat dalam penyediaan SoA merangkumi:

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

b) Menyediakan kandungan SoA dengan mengambil kira aspek berikut:

i. Menyenaraikan semua *control objectives dan controls* di Annex A dalam Standard ISO/IEC 27001:2013;

ii. Memberi jawapan **"Yes"** dengan justifikasi pemilihan kepada c*ontrol objectives dan controls* selaras dengan **penemuan *Risk Treatment Plan***;

iii. Memberi jawapan **"Yes"** kepada c*ontrol objectives dan controls* **yang sedang dilaksanakan**;

iv. Memberi jawapan **"Partial"** kepada kawalan yang **masih dalam pembangunan;**

v. Menyenaraikan **nama prosedur / panduan / dokumen** yang dirujuk bagi menyokong pelaksanaan *control objectives* dan *controls* tersebut; dan

vi. Memberi jawapan **"No"** kepada *control objectives* dan *controls* yang **tidak dipilih** dengan alasan pengecualiannya.

c) Membentangkan cadangan awal SoA dalam mesyuarat pengurusan ISMS; dan

d) Mendapat kelulusan dan tandatangan pihak pengurusan yang bertanggungjawab ke atas skop Pensijilan 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 pengurusan 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

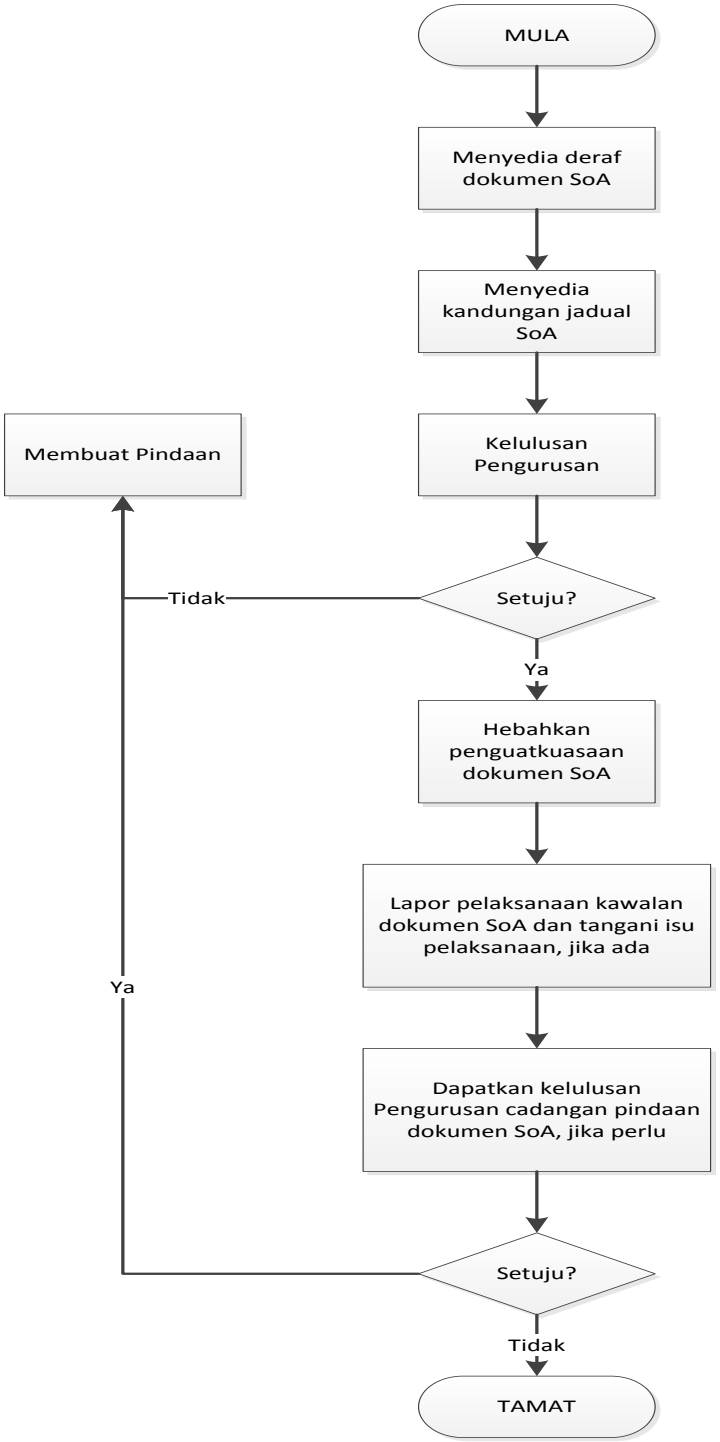
h) Perubahan disebabkan oleh keperluan lain.

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 penguraian risiko (*risk treatment*). Sebarang c*ontrol objectives dan controls* yang **tidak dipilih** diberikan alasan pengecualiannya bagi memastikan suatu kawalan tidak sengaja diabaikan.

5.0 CARTA ALIRAN



Jadual 1: SoA Pensijilan ISO/IEC 27001:2013 ISMS Universiti Putra Malaysia

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
A.5 INFORMATION SECURITY POLICY	A.5.1	**Management Directions for Information security** To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.					
	A.5.1.1	**Policies for information security** A set of policies for information security shall be defined, approved by management, published and communicated to all employees and relevant external parties.	Pej. Jaminan Kualiti UPM & Pej. Penasihat Undang-undang	YES	YES	memastikan kawalan keselamatan maklumat dibangunkan dan disahkan oleh Pengurusan Atasan dan disampaikan kepada umum	• Kaedah-Kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi 2014) : Kelulusan LPU • Garis Panduan Keselamatan Teknologi Maklumat Dan Komunikasi (GPKTMK) – Isu 2.0 Semakan 00 • Medium Komunikasi : e-iso, Buletin Putra

UPM UNIVERSITI PUTRA MALAYSIA BERILMU BERBAKTI	**OPERASI PERKHIDMATAN SOKONGAN** **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 6 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.5.1.2	**Review of the policies for information security** The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.	JK Kerja ISMS	YES	YES	memastikan dasar sentiasa terkini berdasarkan skop dan pelaksanaan ISMS	• Kaedah-Kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi 2014) Bahagian B : Pelaksanaan dan Pindaan Dasar 4 (1) oleh LPU • Garis Panduan Keselamatan Teknologi Maklumat Dan Komunikasi (GPKTMK) – Isu 2.0 Semakan 00 • GPKTMK 5.1 (c) Penyelenggaraan Perkara iv oleh iDEC
A.6 ORGANIZATION OF INFORMATION	A.6.1	**Internal organization** To establish a management framework to initiate and control the implementation of information security within the organization.					
	A.6.1.1	**Information security roles and responsibilities** All information security responsibilities shall be defined and allocated.	JK Kerja ISMS	YES	YES	Memastikan semua tanggungjawab keselamatan maklumat ditakrifkan dan diperuntukkan	• Manual Sistem Pengurusan Keselamatan Maklumat (UPM/ISMS/PGR/MP) Perkara 5.3 PERANAN DAN TANGGUNGJAWAB

UPM UNIVERSITI PUTRA MALAYSIA BERILMU BERBAKTI	**OPERASI PERKHIDMATAN SOKONGAN** **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 7 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.6.1.2	**Segregation of duties** Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	JK Kerja ISMS	YES	YES	Memastikan tugas dan bidang tugas diasingkan untuk mengurangkan peluang bagi pengubahsuaian atau penyalahgunaan aset organisasi yang tidak dibenarkan atau yang tidak disengajakan.	• GPKTMK (12.1 c) Pengasingan Tugas Dan Tanggungjawab)
	A.6.1.3	**Contact with authorities** Appropriate contacts with relevant authorities shall be maintained.	JK Kerja ISMS	YES	YES	Memastikan hubungan dengan pihak berkuasa berkaitan dikekalkan.	• Senarai agensi dan nombor dihubungi (di tampal di lokasi)
	A.6.1.4	**Contact with special interest groups** Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	JK Kerja ISMS	YES	YES	Memastikan hubungan dengan pihak kepentingan atau lain-lain forum keselamatan dan persatuan profesional dikekalkan.	• Senarai agensi dan nombor dihubungi (di tampal di lokasi • Vendor SMP : Encoral Digital Solution Sdn Bhd • Kolej : iDEC

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.6.1.5	**Information security in project management** Information security shall be addressed in project management, regardless of the type of the project.		NO	NO	tiada sebarang pengurusan projek terlibat dalam pelaksanaan ISMS di bawah skop pensijilan	
	A.6.2	**Mobile devices and teleworking** To ensure the security of teleworking and use of mobile devices.					
	A.6.2.1	**Mobile device policy** A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices	Pemilik alat	YES	YES	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)

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.6.2.2	**Teleworking** A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.		NO	NO	Pentadbir Sistem tidak dibenarkan untuk akses dari luar UPMNET. Akses hanya dibenarkan melalui bilik console yang telah disediakan di Pusat Data. **Proses Pendaftaran :** Tidak libatkan perkhidmatan *teleworking* dan *teleworking site*	
A.7 HUMAN RESOURCE	A.7.1	**Prior to employment** To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.					
	A.7.1.1	**Screening** Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics,	Bahagian pengurusan Sumber Manusia	YES	YES	Memastikan pengesahan latar belakang dilaksanakan terhadap staf bagi memenuhi keperluan	• GPKTMK Perkara 7.0 (a) : Sebelum Perkhidmatan • Prosedur Pelantikan Staf Tetap Bagi Kumpulan Pengurusan dan Profesional (Bukan Akademik) dan Kumpulan Sokongan (UPM/SOK/BUM/P001)

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
		and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.				perundangan dan organisasi	• sistem e-vetting : https://evetting.cgso.gov.my
	A.7.1.2	**Terms and conditions of employment** The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	Bahagian Pengurusan Sumber Manusia & Pejabat Bursar	YES	YES	memastikan kontrak perjanjian terhadap staf dan pembekal menyatakan tanggungjawab organisasi terhadap keselamatan maklumat	• 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
	A.7.2	**During Employment** To ensure that employees and external party users are aware of, and fulfill, their information security responsibilities.					
	A.7.2.1	**Management responsibilities** Management shall require employees and contractors to apply information security in accordance with the	Pejabat Bursar	YES	YES	memastikan polisi dan prosedur keselamatan maklumat yang telah ditetapkan oleh organisasi diikuti oleh staf dan pembekal	• Akta Rahsia rasmi 1972 • Garis Panduan Lapor Diri (Aku Janji Staf UPM) (UPM/SOK/BUM/GP03/LAPOR DIRI)

	OPERASI PERKHIDMATAN SOKONGAN **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
		established policies and procedures of the organization.					
	A.7.2.2	**Information security awareness, education and training** All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	Bahagian Pembangunan Sumber Manusia	YES	YES	memastikan staf dan pembekal menerima latihan dan program kesedaran berkaitan dengan polisi organisasi yang berkaitan dengan fungsi kerja masing-masing	• GPKTMK Perkara 7.0 (b) ii Dalam Perkhidmatan • Program Kesedaraan pelaksanaan ISMS
	A.7.2.3	**Disciplinary process** There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	Unit Intergriti	YES	YES	memastikan proses tindakan keselamatan dilaksanakan terhadap staf yang telah melanggar peraturan keselamatan maklumat	• GPKTMK Perkara 7.0 (b) iii Dalam Perkhidmatan • Prosedur Pengurusan Tatatertib Staf (UPM/OPR/PNC-UI/ P001)

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.7.3	**Termination and change of employment** To protect the organization's interests as part of the process of changing or terminating employment					
	A.7.3.1	**Termination or change of employment responsibilities** Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	Pejabat Bursar & Bahagian Pengurusan Sumber Manusia	YES	YES	memastikan tanggungjawab keselamatan maklumat terhadap staf atau pembekal yang telah tamat perkhidmatan atau berlaku perubahan staf hendaklah dikenal pasti dan dikuatkuasakan.	• GPKTMK Perkara 7.0 (c) Bertukar Atau Tamat Perkhidmatan

	OPERASI PERKHIDMATAN SOKONGAN **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 13 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
A.8 ASSET MANAGEMENT	A.8.1	**Responsibility for Assets** To identify organizational assets and appropriate protection responsibilities.					
	A.8.1.1	**Inventory of assets** Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	FAMS - Pegawai Aset PTJ MyRAM - JK Penilaian Risiko	YES	YES	memastikan aset yang terlibat dengan fasiliti pemprosesan maklumat dikenalpasti dan inventori aset tersebut disedia dan diselenggara	• Kaedah-kaedah UPM (Teknologi maklumat dan Komunikasi) 2014 Bahagian D – 8.0 (MS7) • GPKTMK 8.1a(i) (MS10) • Prosedur Pengurusan Aset (UPM/SOK/KEW-AST/P012) • MyRAm - Step 3: Identification of Asset • FAMS
	A.8.1.2	**Ownership of assets** Assets maintaned in the inventory shall be owned.	FAMS - Pegawai Aset PTJ MyRAM - JK Penilaian Risiko	YES	YES	memastikan setiap aset yang diselanggara mempunyai pemilik	• GPKTMK 8.1a(ii) (MS10) • UPM/SOK/KEW-AST/P012 : Prosedur Pengurusan Aset • MyRAm - Step 3: Identification of Asset • FAMS

	OPERASI PERKHIDMATAN SOKONGAN **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 14 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.8.1.3	**Acceptable use of assets** Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented, and implemented.	Pejabat Bursar	YES	YES	memastikan peraturan untuk kebolehgunaan maklumat dan aset yang berkaitan dengan kemudahan pemprosesan maklumat dan maklumat itu dikenal pasti, didokumen dan dilaksanakan.	• Pekeliling Bendahari Bil. 1 Tahun 2008 :Tatacara Pengurusan Aset Alih Universiti Putra Malaysia Bab C : Penggunaan, Penyimpanan dan Pemeriksaan Perkara 15, 16 dan 17
	A.8.1.4	**Return of assets** All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	Pejabat Bursar & Bahagian Pengurusan Sumber Manusia	YES	YES	memastikan aset organisasi dipulangkan selepas tamat kontrak	• Staf : Nota Serah Tugas (SOK/BUM/BR03/SERAH TUGAS)
	A.8.2	**Information classification** To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.					

	OPERASI PERKHIDMATAN SOKONGAN **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 15 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			**Owner**	**Applicable (Yes/No)**	**Implemented (Yes/Partial/ No)**	**Justification**	**Current Controls**
Clause	**Sec**	**Control Objective/Control**					
	A.8.2.1	**Classification of information** Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.	Pegawai Kawalan Dokumen & Bahagian Perkhidmatan Sumber Manusia	YES	YES	memastikan maklumat dikelaskan untuk mengelak daripada pendedahan atau pengubahsuaian yang tidak dibenarkan	• Arahan Keselamatan Kerajaan Malaysia • Akta Arkib Negara 2003 (Akta 629) • GPKTMK 8.2a (MS10) • Garis Panduan Pengendalian Maklumat (UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT)
	A.8.2.2	**Labeling of information** An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Pegawai Kawalan Dokumen & Bahagian Perkhidmatan Sumber Manusia	YES	YES	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 8.2a (MS10) • Garis Panduan Pengendalian Maklumat (UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT) • Garis Panduan Pengurusan Backup Pangkalan Data (UPM/ISMS/OPR/PD/GP14/BACKUP)

	OPERASI PERKHIDMATAN SOKONGAN **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 16 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.8.2.3	**Handling of assets** Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Pegawai Kawalan Dokumen & Bahagian Perkhidmatan Sumber Manusia	YES	YES	memastikan prosedur pengendalian aset dibangun dan dilaksanakan mengikut skema klasifikasi maklumat oleh organisasi	• GPKTMK 8.1a (iv) dan 8.2b (MS 10 & 11) • Pekeliling Bendahari Bil. 1 Tahun 2008 :Tatacara Pengurusan Aset Alih Universiti Putra Malaysia • Garis Panduan Pengendalian Maklumat (UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT) • Arahan Keselamatan Kerajaan Malaysia
	A.8.3	**Media Handling** To prevent unauthorized disclosure, modification, removal or destruction of information stored on media					
	A.8.3.1	**Management of removable media** Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	Pegawai Kawalan Dokumen & Bahagian Perkhidmatan Sumber Manusia	YES	YES	memastikan perosedur bersesuaian dibangunkan mengikut klasifikasi yang digunakan oleh organisasi	• GPKTMK 8.3 : Pengendalian media (MS11) • Tatacara Pengurusan Aset Aleh Kerajaan : pelupusan • Arahan Kerja Pelupusan Pita Backup (UPM/ISMS/OPR/PD/AK07)

UPM UNIVERSITI PUTRA MALAYSIA BERILMU BERBAKTI	**OPERASI PERKHIDMATAN SOKONGAN** **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 17 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.8.3.2	**Disposal of media**Media shall be disposed of securely when no longer required, using formal procedures.	Pegawai Kawalan Dokumen & Bahagian Perkhidmatan Sumber Manusia	YES	YES	media yang tidak lagi diperlukan perlu dilupuskan menggunakan prosedur yang dibangunkan	• GPKTMK 8.2b(vi) & 8.3b(vi) (MS11)• UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT : Garis Panduan Pengendalian Maklumat • Garis Panduan pelupusan aset (UPM/SOK/KEW/GP020/AST)
	A.8.3.3	**Physical media transfer** Media containing information shall be protected against unauthorized access, misuse or corruption during transportion.	Pegawai Kawalan Dokumen & Bahagian Perkhidmatan Sumber Manusia	YES	YES	Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa perpindahan	• GPKTMK 8.3 (MS11) - UPDATE • Garis Panduan Pengendalian Maklumat (UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT)

	OPERASI PERKHIDMATAN SOKONGAN **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 18 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
A.9 ACCESS CONTROL	A.9.1	**Business requirement for access control** To limit access to information and information processing facilities.					
	A.9.1.1	**Access control policy** An access control policy shall be established, documented, and reviewed based on business and information security requirements.	Seksyen Pusat Data	YES	YES	Dasar kawalan capaian hendaklah diwujud , didokumen dan dikaji semula berdasarkan keperluan keselamatan perniagaan dan maklumat.	• GPKTMK Perkara 9.1 : Dasar Kawalan Capaian • Garis Panduan Kawalan Akses Ke Pusat Data (UPM/ISMS/OPR/DC/ GP03/KAWALAN AKSES) • Garis Panduan Pemantauan Capaian Ke Sistem Di Pusat Data (UPM/ISMS/OPR/ DC/GP06/ PEMANTAUAN CAPAIAN)
	A.9.1.2	**Access to networks and networks services** Users shall only be provided with acess to the network and network services that they have specifically authorized to used.	Seksyen Rangkaian	YES	YES	memastikan pengguna mempunyai akses kepada perkhidmatan rangkaian yang telah dikhususkan kepada mereka	• GPKTMK Perkara 13.2 : Kawalan Akses Rangkaian • Garis Panduan Pengurusan Pengagihan Rangkaian (UPM/ISMS/OPR/NET/ GP13/AGIHAN RANGKAIAN)
	A.9.2	**User access management** To ensure authorized user access and to prevent unauthorized access to systems and services.					
	A.9.2.1	**User registration and de-registration** A formal user registration	Seksyen Pusat Data	YES	YES	Memastikan proses pendaftaran dan pembatalan pengguna	• GPKTMK Perkara 9.2 : Pengurusan Capaian Pengguna • Prosedur Kawalan dan Pemantauan

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
		and de-registration process shall be implemented to enable assignment of access rights.	& PTJ terlibat			dilaksanakan untuk membolehkan pemberian hak akses	Capaian ke Sistem di Pusat Data (UPM/ISMS/OPR/DC/P003) • Garis Panduan Pemantauan Capaian Ke Sistem Di Pusat Data (UPM/ISMS/OPR/ DC/GP06/PEMANTAUAN CAPAIAN)
	A.9.2.2	**User access provisioning** A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	Seksyen Pusat Data & PTJ terlibat	YES	YES	memastikan penetapan dan pembatalan hak akses untuk semua jenis pengguna dilaksanakan	• GPKTMK Perkara 9.2 : Pengurusan Capaian Pengguna • Garis Panduan Pemantauan Capaian Ke Sistem Di Pusat Data (UPM/ISMS/OPR/DC/GP06/ PEMANTAUAN CAPAIAN)
	A.9.2.3	**Management of privileged access rights** The allocation and use of priviledge access rights shall be restricted and controlled.	Seksyen Pusat Data & PTJ terlibat	YES	YES	memastikan kebenaran hak akses dihadkan dan dikawal	• GPKTMK Perkara 9.2 : Pengurusan Capaian Pengguna • Garis Panduan Pemantauan Capaian Ke Sistem Di Pusat Data (UPM/ISMS/OPR/DC/GP06/ PEMANTAUAN CAPAIAN)

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.9.2.4	**Management of secret authentication information of users** The allocation of a secret authentication information shall be controlled through a formal management process.	Seksyen Pengurusan Data & PTJ terlibat	YES	YES	memastikan pengesahan maklumat rahsia sentiasa dikawal	• GPKTMK Perkara 10.0 : Kawalan Kriptografi • Garis Panduan Pengurusan UPM-ID (UPM/ISMS/OPR/PD/GP16/UPM-ID)
	A.9.2.5	**Review of user access rights** Assets owners shall review user's access rights at regular intervals.	Seksyen Pusat Data & PTJ terlibat	YES	YES	memastikan hak capaian pengguna disemak semula	• Garis Panduan Pemantauan Capaian Ke Sistem Di Pusat Data (UPM/ISMS/OPR/DC/GP06/ PEMANTAUAN CAPAIAN)
	A.9.2.6	**Removal or adjustment of access rights**The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their	Seksyen Pusat Data & PTJ terlibat	YES	YES	memastikan hak akses kepada maklumat dan kemudahan dikeluarkan selepas tamat perkhidmatan atau apabila berlaku perubahan	• GPKTMK Perkara 9.2 : Pengurusan Capaian Pengguna • Prosedur Kawalan dan Pemantauan Capaian ke Sistem di Pusat Data (UPM/ISMS/OPR/DC/P003) • Garis Panduan Pemantauan Capaian Ke Sistem Di Pusat Data (UPM/ISMS/OPR/DC/GP06/ PEMANTAUAN CAPAIAN)

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
		employment, contract or agreement, or adjusted upon change.					
	A.9.3	**User responsibilities** To make users accountable for safeguarding their authentication information.					
	A.9.3.1	**Use of secret authentication information** Users shall be required to follow the organization's practices in the use of secret authentication information.	Seksyen Keselamatan	YES	YES	memastikan pengguna mengikut semua amalan yang telah ditetapkan dalam pengesahan maklumat	• GPKTMK Perkara 10.0 : Kawalan Kriptografi • Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI)
	A.9.4	**System and application access control** To prevent unauthorized access to systems and applications.					

	OPERASI PERKHIDMATAN SOKONGAN **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 22 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.9.4.1	**Information access restriction** Access to information and application system functions shall be restricted in accordance with the access control policy.	Seksyen Pusat Data & PTJ terlibat	YES	YES	memastikan akses kepada maklumat dan sistem aplikasi dihadkan mengikut prosedur kawalan akses	• GPKTMK Perkara 9.1 : Dasar Kawalan Capaian • Prosedur Kawalan dan Pemantauan Capaian ke Sistem di Pusat Data (UPM/ISMS/OPR/DC/P003) • Garis Panduan Kawalan Akses Ke Pusat Data (UPM/ISMS/OPR/DC/ GP03/KAWALAN AKSES) • Garis Panduan Pemantauan Capaian Ke Sistem Di Pusat Data (UPM/ISMS/OPR/DC/GP06/ PEMANTAUAN CAPAIAN) • Garis Panduan Pengendalian Maklumat (UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT)
	A.9.4.2	**Secure log-on procedures** Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	Seksyen Pusat Data & PTJ terlibat	YES	YES	memastikan akses kepada sistem dan aplikasi dikawal menggunakan prosedur bersesuaian	• GPKTMK Perkara 9.3 : Kawalan Akses Sistem Pengoperasian Server • Prosedur Kawalan dan Pemantauan Capaian ke Sistem di Pusat Data (UPM/ISMS/OPR/DC/P003)

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.9.4.3	**Password management system** Password management systems shall be interactive and shall ensure quality passwords.	Seksyen Pusat Data & PTJ terlibat	YES	YES	memastikan sistem pengurusan kata laluan adalah interaktif dan kata laluan berkualiti	• GPKTMK Perkara 9.2 : Pengurusan Capaian Pengguna • Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI)
	A.9.4.4	**Use of priviledge utility program** The use of utility programs that might be capable of overriding systems and application controls shall be restricted and tightly controlled	Seksyen Pusat Data & PTJ terlibat	YES	YES	memastikan utiliti program yang boleh mengganggu sistem aplikasi perlu dihad dan dikawal	• UPM/ISMS/OPR/DC/P003: Prosedur Kawalan dan Pemantauan Capaian ke Sistem di Pusat Data • Garis Panduan Pemantauan Capaian Ke Sistem Di Pusat Data (UPM/ISMS/OPR/DC/GP06/ PEMANTAUAN CAPAIAN)
	A.9.4.5	**Access control to program source code** Access to program source code shall be restricted	Bahagian Operasi Aplikasi	YES	YES	memastikan akses kepada program kod sumber perlu dihadkan	• GPKTMK 9.4 [a (iii)]

	OPERASI PERKHIDMATAN SOKONGAN **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 24 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
A.10 CRYPTOGRAPHY	A.10.1	**Cryptographic controls** To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.					
	A.10.1.1	**Policy on the use of cryptographic control** A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	Seksyen Keselamatan	YES	YES	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) • Garis Panduan Pengendalian Maklumat (UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT)
	A.10.1.2	**Key management** A policy on the use, protection and lifetime of cyptographic keys shall be developed and implemented through their whole lifecycle.	Seksyen Keselamatan	YES	YES	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) • Garis Panduan Pengendalian Maklumat (UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT)

	OPERASI PERKHIDMATAN SOKONGAN **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 25 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
A.11 PHYSICAL AND ENVIRONMENTAL SECURITY	A.11.1	**Secure areas**To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.					
	A.11.1.1	**Physical security perimeter** Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	Seksyen Pusat Data & PTJ berkaitan	YES	YES	memastikan perimeter keselamatan ditentukan dan digunakan untuk melindungi kawasan yang mengandungi maklumat yang sensitif atau kritikal.	• Manual Sistem Pengurusan Keselamatan Maklumat (ISMS) (UPM/ISMS/PGR/MP) Perkara 4.3.4 : Lokasi Skop Pensijilan ISMS UPM **Pusat Data :** Kad Access Control Biometrik System Log Keluar Masuk Pusat Data (Staf) Log Keluar Masuk Pusat Data (Pelawat) Borang Pendaftaran Masuk Pusat Data (Pelawat) cctv **PTJ:** Pejabat Pengurusan Kolej

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.11.1.2	**Physical entry controls** Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Seksyen Pusat Data & PTJ berkaitan	YES	YES	memastikan kawalan bersesuaian dilaksanakan bagi memastikan hanya pengguna yang diberi hak akses sahaja dibenarkan masuk	• Manual Sistem Pengurusan Keselamatan Maklumat (ISMS) (UPM/ISMS/PGR/MP) Perkara 4.3.4 : Lokasi Skop Pensijilan ISMS UPM **Pusat Data :** Kad Access Control Biometrik System Log Keluar Masuk Pusat Data (Staf) Log Keluar Masuk Pusat Data (Pelawat) Borang Pendaftaran masuk Pusat Data (Pelawat) CCTV **PTJ:** Pejabat Pengurusan Kolej

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.11.1.3	**Securing offices, rooms and facilities** Physical security for offices, rooms, and facilities shall be designed and applied.	Seksyen Pusat Data & PTJ berkaitan	YES	YES	memastikan keselamatan fizikal direka dan digunakan	• Manual Sistem Pengurusan Keselamatan Maklumat (ISMS) (UPM/ISMS/PGR/MP) Perkara 4.3.4 : Lokasi Skop Pensijilan ISMS UPM **Pusat Data :** Kad Access Control Biometrik System Kabinet Berkunci Pintu berkunci CCTV
	A.11.1.4	**Protecting against external and environmental threats** Physical protection against natural disaster, malicious attack or accidents shall be designed and applied.	Seksyen Pusat Data	YES	YES	memastikan perlindungan fizikal dibangun dan digunakan.	• Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan komunikasi 2014) Bhgn D, 9 (b) dan Bhgn G, 20 (1) • GPKTMK Perkara 11.1 : Persekitaran Selamat • Akta Keselamatan dan Kesihatan Pekerjaan 1994 (AKTA 514) • Agronite System (Sistem Pencegahan Kebakaran) • Fire Extinguisher

	OPERASI PERKHIDMATAN SOKONGAN **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 28 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			**Owner**	**Applicable (Yes/No)**	**Implemented (Yes/Partial/ No)**	**Justification**	**Current Controls**
Clause	**Sec**	**Control Objective/Control**					
	A.11.1.5	**Working in secure areas** Procedures for working in secure areas shall be designed and applied.		YES	YES	memastikan prosedur bagi memastikan keselamatan tempat kerja dibangun dan dilaksanakan	• Akta Keselamatan dan Kesihatan Pekerjaan 1994 (AKTA 514) • GPKTMK Perkara 11.1 : Persekitaran Selamat
	A.11.1.6	**Delivery and loading areas** Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	Seksyen Pusat Data & INSPEM	YES	YES	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) dan Bhgn G, 20 (1) • GPKTMK Perkara 11.1 : Persekitaran Selamat • Prosedur kawalan Akses (UPM/OPR/BKU/P001) • Loading Area : Main Entrance INSPEM • Staging Room
	A.11.2	**Equipment** To prevent loss, damage, theft or compromise of assets and interruption to the organization's operation.					

	OPERASI PERKHIDMATAN SOKONGAN **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 29 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			**Owner**	**Applicable (Yes/No)**	**Implemented (Yes/Partial/ No)**	**Justification**	**Current Controls**
Clause	**Sec**	**Control Objective/Control**					
	A.11.2.1	**Equipment sitting and protection** Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Seksyen Pusat Data & PTJ berkaitan	YES	YES	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) dan Bhgn G, 20 (1) • GPKTMK Perkara 11.3 : Keselamatan Peralatan
	A.11.2.2	**Supporting utilities** Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Seksyen Pusat Data	YES	YES	memastikan peralatan dilindungi daripada kegagalan bekalan kuasa dan gangguan yang disebabkan oleh kegagalan utiliti sokongan	• GPKTMK Perkara 11.1 (h) : Perkhidmatan Sokongan dan Perkara 17.1 (a) • Genset • UPS
	A.11.2.3	**Cabling security** Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	Seksyen Rangkaian, Telekomunikasi PPPA	YES	YES	memastikan kabel bekalan kuasa dan telekomunikasi dilidungi daripada pemintasan, gangguan atau kerosakan	• Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan komunikasi 2014) Bhgn D, 11 • GPKTMK Perkara 11.1 (i) : Keselamatan Kabel • Garis Panduan Pengurusan Sistem Pengkabelan (UPM/ISMS/OPR/NET/GP12/ PEMASANGAN KABEL)

	OPERASI PERKHIDMATAN SOKONGAN **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 30 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			**Owner**	**Applicable (Yes/No)**	**Implemented (Yes/Partial/ No)**	**Justification**	**Current Controls**
Clause	**Sec**	**Control Objective/Control**					
	A.11.2.4	**Equipment maintenance** Equipment shall be correctly maintained to ensure its continued availability and integrity.	Seksyen Rangkaian Telekomunikasi Pusat Data Zon ICT (Kolej)	YES	YES	memastikan peralatan diselenggara	• Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan komunikasi 2014) Bhgn D, 10 • GPKTMK Perkara 11.3 (e) : Penyelenggaraan Peralatan • Prosedur Penyelenggaraan ICT (UPM/SOK/ICT/P001) • Prosedur Baik Pulih ICT (UPM/SOK/ICT/P002) • Garis Panduan Penyelenggaraan Berkala (PPPA) (UPM/SOK/PYG/GP02) • Prosedur Penyelenggaraan Baik Pulih (PPPA) (UPM/SOK/PYG/P001)
	A.11.2.5	**Removal of asset**Equipment, information or software shall not be taken off-site without prior authorization	Seksyen Rangkaian Telekomunikasi Pusat DataZon ICT (Kolej) PTJ berkaitan	YES	YES	memastikan peralatan, maklumat atau perisian di bawa keluar dari lokasi tanpa kebenaran	• Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan komunikasi 2014) Bhgn D, 9 (a)• GPKTMK Perkara 11.3 (a) : Peralatan ICT • Prosedur Pengurusan Aset (UPM/SOK/KEW-AST/P012) • Prosedur Baik Pulih ICT (UPM/SOK/ICT/P002) • Prosedur Penyelenggaraan Baik Pulih (PPPA) (UPM/SOK/PYG/P001)

UPM UNIVERSITI PUTRA MALAYSIA BERILMU BERBAKTI	**OPERASI PERKHIDMATAN SOKONGAN** **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 31 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.11.2.6	**Security of equipment and asset off-premises** Security shall be applied to off-site asset taking into account the different risks of working outside the organization's premises	Seksyen Rangkaian Telekomunikasi Pusat Data Zon ICT (Kolej) PTJ berkaitan	YES	YES		• UPM/SOK/KEW-AST/P012 : Prosedur Pengurusan Aset • GPKTMK Perkara 11.3 (f) : Peralatan Di Luar Premis • Prosedur Baik Pulih ICT (UPM/SOK/ICT/P002) • Prosedur Penyelenggaraan Baik Pulih (PPPA) (UPM/SOK/PYG/P001)
	A.11.2.7	**Secure disposal or re-use of equipment** All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use	Seksyen Rangkaian Telekomunikasi Pusat Data Zon ICT (Kolej) PTJ berkaitan	YES	YES		• Pekeliling perbendaharaan Bil 5/2007 : Bab E : Pelupusan (m/s : 36) • GPKTMK Perkara 13 (g) : Pelupusan Peralatan • Prosedur Pengurusan Aset (UPM/SOK/KEW-AST/P01) • Pekeliling Bendahari Bil 1 2008 : Bahagian E Pelupusan
	A.11.2.8	**Unattended user equipment** Users shall ensure that unattended equipment	Seksyen Rangkaian Telekomunikasi Pusat Data	YES	YES	memastikan peralatan yang ditinggalkan di kawal dengan dengan sempurna	• GPKTMK Perkara 11.3 (h) : Peralatan Ditinggalkan Pengguna

	OPERASI PERKHIDMATAN SOKONGAN **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 32 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
		has appropriate protection.	PTJ berkaitan				
	A.11.2.9	**Clear desk and clear screen policy** A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted	Seksyen Rangkaian Telekomunikasi Pusat Data PTJ berkaitan	YES	YES	memastikan polisi clear desk dan clear screen diguna pakai	• GPKTMK Perkara 11.3 (i) : Panduan Clear Desk dan Clear Screen
A.12 OPERATION SECURITY	A.12.1	**Operational procedures and responsibility** To ensure correct and secure operations of processing facilities.					
	A.12.1.1	**Documented operating procedures** Operating procedures shall be documented and made available to all users who need them.	Bahagian Pengurusan Kualiti	YES	YES	memastikan prosedur operasi didokumen dan disediakan kepada yang memerlukan	• Laman Web e-ISO www.spk.upm.edu.my

	OPERASI PERKHIDMATAN SOKONGAN **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 33 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.12.1.2	**Change management** Changes to the organizations, business processes, information processing facilities and systems that affect information security shall be controlled.	Bahagian Hal Ehwal pelajar & Alumni iDEC	YES	YES	memastikan perubahan kepada organisasi, proses bisnes dan fasiliti pemprosesan maklumat dikawal	• Mesyuarat Minggu Perkasa Putra • Mesyuarat Pengurusan iDEC
	A.12.1.3	**Capacity management** The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	Bahagian Hal Ehwal pelajar & Alumni iDEC	YES	YES	memastikan penggunaan sumber dipantau dan unjuran dibuat untuk keperluan masa depan untuk memastikan keperluan prestasi sistem	• Mesyuarat Minggu Perkasa Putra • Mesyuarat Bahagian Operasi Aplikasi, iDEC
	A.12.1.4	**Separation of development, testing and operational environments** Development, testing and operational environments shall be separated to reduce the risks of unauthorized	Seksyen Pusat Data	YES	YES	memastikan pembangunan, pengujian dan operasi persekitaran diasingkan untuk mengurangkan risiko kepada akses yang tidak dibenarkan	• GPKTMK Perkara 14.0 : Perolehan, pembangunan dan penyelenggaraan sistem maklumat

	OPERASI PERKHIDMATAN SOKONGAN **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 34 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
		access or changes to the operational environment.					
	A.12.2	**Protection from malware** To ensure that information and information processing facilities are protected					
	A.12.2.1	**Controls against malware** Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Seksyen Keselamatan	YES	YES	memastikan kawalan ke atas malware dibangunkan	• GPKTMK Perkara 12.2 (a) : Perlindungan daripada Perisian Berbahaya • Microsoft Endpoint Protection • Intrusion Prevention System • Firewall • Secured Email Relay
	A.12.3	**Backup**To protect againsts loss of data					
	A.12.3.1	**Information backup** Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	Seksyen Pengurusan Data	YES	YES		• GPKTMK Perkara 12.3 (a) : Backup • Garis Panduan Pengurusan Backup Pangkalan Data (UPM/ISMS/OPR/PD/GP14/BACKUP) • Garis Panduan Penggunaan Data Pengujian (UPM/ISMS/OPR/PD/GP15/DATA PENGUJIAN)

	OPERASI PERKHIDMATAN SOKONGAN **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 35 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.12.4	**Logging and monitoring** To record events and generate evidence.					
	A.12.4.1	**Event logging** Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed	Seksyen Pusat Data	YES	YES	memastikan event log dijana, disimpan dan dikaji secara berkala	• GPKTMK Perkara 12.4: Logging dan Pemantauan
	A.12.4.2	**Protection of log information** Logging facilities and log information shall be protected against tampering and unauthorized access.	Seksyen Pusat Data	YES	YES		• GPKTMK Perkara 12.4 (b): Perlindungan Maklumat Log
	A.12.4.3	**Administrator and operator logs** System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	Bahagian Operasi Aplikasi & HEPA	YES	YES	memastikan aktiviti pentadbir sistem direkod, dikawal dan di pantau berkala	• Prosedur Kawalan dan Pemantauan Capaian ke Sistem di Pusat Data (UPM/ISMS/OPR/DC/P003) • Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI)

	OPERASI PERKHIDMATAN SOKONGAN **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 36 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.12.4.4	**Clock synchronization** The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source.	Seksyen Pusat Data	YES	YES	memastikan masa bagi semua pemprosesan maklumat diselaraskan dengan satu sumber rujukan masa	• GPKTMK Perkara 12.4 (d): Pelarasan Masa • Network Time Protocol (time.upm.edu.my)
	A.12.5	**Control of operational software** To ensure the integrity of operational system					
	A.12.5.1	**Installation of software on operational systems** Procedures shall be implemented to control the installation of software on operational systems.	Seksyen Pusat Data	YES	YES	memastikan prosedur kawalan ke atas perisian dibangunkan	• GPKTMK Perkara 12.5: Kawalan Ke atas Perisian Pengoperasian • Garis Panduan Kawalan Instalasi Perisian (UPM/ISMS/SOK/GP06/ INSTALASI PERISIAN) • Manual installation
	A.12.6	**Technical vulnerability management** To prevent exploitation of technical vulnerabilities.					

UPM UNIVERSITI PUTRA MALAYSIA BERILMU BERBAKTI	**OPERASI PERKHIDMATAN SOKONGAN** **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 37 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.12.6.1	**Management of technical vulnerabilities** Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	JK Penilaian Risiko	YES	YES		• GPKTMK Perkara 12.6: Pengurusan Kerentanan Teknikal • Garis Panduan Penilaian Tahap Keselamatan (UPM/ISMS/OPR/KES/GP09/TAHAP KESELAMATAN) • MyRAM Step 5, 6, 7 & 8
	A.12.6.2	**Restrictions on software installation** Rules governing the installation of software by users shall be established and implemented	Seksyen Pusat Data	YES	YES	memastikan peraturan kawalan instalasi perisian dibangun dan dilaksanakan	• GPKTMK Perkara 12.6 (b): Menghadkan Instalasi Perisian •: Garis Panduan Kawalan Instalasi Perisian (UPM/ISMS/SOK/ GP06/INSTALASI PERISIAN) Manual installation
	A.12.7	**Information systems audit considerations** To minimise the impact of audit activities on operational systems.					

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.12.7.1	**Information systems audit controls** Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise distruptions to business processes.	Bahagian Pengurusan Kualiti	YES	YES	memastikan keperluan audit dan aktiviti yang melibatkan pengesahan terhadap sistem operasi perlu dirancang dan bersetuju untuk mengurangkan gangguan kepada proses bisnes	• GPKTMK Perkara 12.7(a) : Kawalan Audit Sistem Maklumat • Garis Panduan Penilaian Tahap Keselamatan ICT (UPM/ISMS/OPR/KES/GP09/TAHAP KESELAMATAN) • Badan Pensijilan SIRIM • Audit Dalaman ISMS
A.13 COMMUNICATION SECURITY	A.13.1	**Network security management** To ensure the protection of information in networks and its supporting information processing facilities.					
	A.13.1.1	**Network controls** Networks shall be managed and controlled to protect information in systems and application.	Seksyen Rangkaian	YES	YES	memastikan rangkaian perlu urus dan dikawal	• GPKTMK Perkara 13.2 : Kawalan Akses Rangkaian • Garis Panduan Pengurusan Pengagihan Rangkaian (UPM/ISMS/OPR/NET/GP13/AGIHAN RANGKAIAN) • ID & Password Staf • Private network (SMP) - network conceptual diagram
	A.13.1.2	**Security of network services**	Seksyen Rangkaian	YES	YES	Tidak melibatkan Internet service	• Dokumen kontrak antara UPM dan ISP

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
		Security mechanisms, service levels, and management requirements of all network services shall be identified and included in network services agreement, whether these services are provided in-house or outsourced.				provider. Hanya menggunakan intranet (UPMNET)	
	A.13.1.3	**Segregation in network** Groups of information services, users, and information systems shall be segregated on networks.	Seksyen Rangkaian	YES	YES	memastikan pengasingan rangkaian dilaksanakan	• Garis Panduan Pengurusan Pengagihan Rangkaian (UPM/ISMS/OPR/NET/GP13/AGIHAN RANGKAIAN) • VLAN USPOT • VLAN Kolej/Fakulti/Institut • VLAN Pusat Data
	A.13.2	**Information transfer** To maintain the security of information transferred within an organization and with any external entity.					
	A.13.2.1	**Information transfer policies and procedures** Formal transfer policies, procedures and controls		YES	YES	memastikan polisi dan kawalan terhadap pemindahan maklumat perlu disediakan	• GPKTMK Perkara 13.3 : Pengurusan Pertukaran Maklumat • Garis Panduan Pengendalian Maklumat (UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT)

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
		shall be in place to protect the transfer of information through the use of all types of communication facilities.					• Prosedur Pertukaran Maklumat (UPM/ISMS/SOK/P002)
	A.13.2.2	**Agreements on information transfer** Agreements shall address the secure transfer of business information between the organization and external parties.	Pejabat Bursar	YES	YES	memastikan kontrak perjanjian memenuhi keperluan keselamatan penghantaran maklumat diantara pembekal dan organisasi	• GPKTMK Perkara 13.3(a) : Pertukaran Maklumat • Prosedur Pertukaran Maklumat (UPM/ISMS/SOK/P002)
	A.13.2.3	**Electronic messaging** Infromation involved in electronic messaging shall be appropriately protected.	Seksyen Pusat Data	YES	YES	memastikan kawalan terhadap mesej elektronik dibangunkan	• GPKTMK Perkara 13.3 (b): Pengurusan Mel Elektronik
	A.13.2.4	**Confidentiality or non-disclosure agreements** Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for	Pejabat Penasihat Undang-undang	YES	YES	memastikan NDA bagi keperluan melindungi maklumat perlu dikenal pasti, di pantau dan didokumenkan	• GPKTMK Perkara 15.1 : Pihak Ketiga • Non Discloser Aggreement (NDA)

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
		the protection of information shall be identified, regularly reviewed and documented.					
A.14 SYSTEM ACQUISITION, DEVELOPMENT AND	A.14.1	**Security requirements of information systems** To ensure that information security is an intergral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.					
	A.14.1.1	**Information security requirements analysis and specification** The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	Bahagian Akademik / iDEC	YES	YES	memastikan keperluan keselamatan maklumat perlu dimasukkan ke dalam sistem baru atau sistem sedia ada	• Dokumen perjanjian antara UPM dan Vendor (Encoral Digital Solution Sdn Bhd)

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.14.1.2	**Securing application services on public networks.**Infromation involved in application services passing over public neworks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	Seksyen Keselamatan Seksyen Rangkaian Seksyen Operasi Aplikasi	YES	YES	memastikan kawalan terhadap rangkaian awam perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan atau pengubahsuaian yang tidak dibenarkan	• IPS di Pusat Data • Firewall • ID & Password • Network Segmentation • Disclaimer
	A.14.1.3	**Protecting application services transactions** Information involved in application services transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	Seksyen Keselamatan Seksyen Rangkaian Seksyen Operasi Aplikasi	YES	YES	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	• IPS di Pusat Data • Firewall • ID & Password • Network Segmentation • Disclaimer

UPM UNIVERSITI PUTRA MALAYSIA BERILMU BERBAKTI	**OPERASI PERKHIDMATAN SOKONGAN** **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 43 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
						tidak dibenarkan atau ulangan	
	A.14.2	**Security in development and support processes** To ensure that information security is designed and implemented within the development lifecycle of information systems.					
	A.14.2.1	**Secure development policy** Rules fro the development of software and systems shall be established and applied to developments within the organization.	Perancangan & Governan	YES	YES	memastikan polisi keselamatan pembangunan sistem dan aplikasi dibangun dan diguna pakai	• GPKTMK Perkara 14.1 : Keselamatan dalam Pembangunan Sistem dan Aplikasi
	A.14.2.2	**System change control procedures** Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	Bahagian pembangunan Aplikasi	YES	YES	memastikan perubahan kepada proses pembangunan perlu dikawal menggunakan prosedur kawalan perubahan	• Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) • Borang Permohonan Perubahan Spesifikasi Pembangunan ICT (OPR/ICT/BR06/Perubahan Spesifikasi)
	A.14.2.3	**Technical review of applications after operating platform changes**	Bahagian pembangunan Aplikasi	YES	YES	memastikan perubahan ke atas aplikasi perlu di semak dan diuji untuk	• GPKTMK Perkara 14.2 (a) : Prosedur Kawalan Perubahan • Dokumen Perancangan Pengujian Sistem (STP) (OPR/IDEC/DF02/

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
		When operating platforms are change, business critical applications shall be reviewd and tested to ensure there is no adverse impact on organizational operations or security.				memastikan tiada kesan buruk terhadap organisasi atau keselamatan	Perancangan Pengujian Sistem) • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001)
	A.14.2.4	**Restriction on changes to software packages** Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	Bahagian pembangunan Aplikasi	YES	YES	memastikan sebarang perubahan atau pengubahsuaian pakej aplikasi perlu dikawal	• GPKTMK Perkara 14.2 (a) : Prosedur Kawalan Perubahan • Dokumen Perancangan Pengujian Sistem (STP) (OPR/IDEC/DF02/ Perancangan Pengujian Sistem) • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001)
	A.14.2.5	**Secure system engineering principles** Principles for engineering secure systems shall be established documented, maintained and applied	Bahagian pembangunan Aplikasi	YES	YES	Skop pensijilan ISMS UPM tidak melibatkan sistem pembangunan aplikasi.	• GPKTMK 14.3 : Persekitaran Pembangunan Selamat

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
		to any information syste implementation efforts.					
	A.14.2.6	**Secure development environment** Organizations shall establish and appropriately protect secure development environments for system development and intergration efforts that cover the entire system development lifecycle.	Bahagian pembangunan Aplikasi	YES	YES	Skop pensijilan ISMS UPM tidak melibatkan sistem pembangunan aplikasi.	• GPKTMK 14.3 : Persekitaran Pembangunan Selamat
	A.14.2.7	**Outsourced development** The organization shall supervise and monitor the activity of outsourced system development.	Bahagian pembangunan Aplikasi	YES	YES	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)
	A.14.2.8	**System security testing**Testing of security functionality shall be carried out during development.	Seksyen Keselamatan Bahagian Pembangunan Aplikasi	YES	YES	memastikan ujian keselamatan perlu dilaksanakan semasa pembangunan aplikasi	• Garis Panduan Penilaian Tahap Keselamatan (UPM/ISMS/OPR/KES/ GP09/TAHAP KESELAMATAN)

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.14.2.9	**System acceptance testing** Acceptance testing programs and related criteria shall be established fro new information systems, upgrades and new versions.	Seksyen Keselamatan Bahagian Pembangunan Aplikasi	YES	YES	memastikan ujian penerimaan perlu dilaksanakan bagi sistem baru atau naik taraf	• Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) • Skrip Pengujian Penerimaan Pengguna (UAT Test Script) (OPR/IDEC/DF04/ SKRIP PENGUJIAN UAT)
	A.14.3	**Test data** To ensure the protection of data used for testing.					
	A.14.3.1	**Protection of test data** Test data shall be selected carefully, protected and controlled.	Seksyen Pengurusan Data	YES	YES	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)

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
A.15 SUPPLIER RELATIONSHIP	A.15.1	**Information security in supplier relationship** To ensure protection of the organization's assets that is accessible bu suppliers.					
	A.15.1.1	**Information security policy for supplier relationship** Information security requirements fro mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	Seksyen Pusat Data	YES	YES	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 Pengoperasian Pengurusan Pusat Data (UPM/ISMS/OPR/DC/P001)
	A.15.1.2	**Addressing security within supplier agreements** All relevent information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide	Bahagian Akademik / iDEC	YES	YES	memastikan keperluan keselamatan maklumat dibangunkan dan dipersetujui oleh pihak pembekal	• Dokumen Perjanjian antara UPM dan Vendor (Encoral)

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
		IT infrastructure components for the organization's infromation.					
	A.15.1.3	**Information and communication technology supply chain** Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	Pejabat Bursar	YES	YES	memastikan dokumen perjanjian antara pihak pembekal memenuhi keperluan keselamatan maklumat	• GPKTMK Perkara 15.1 : Pihak Ketiga • Prosedur Sebut Harga Universiti (UPM/SOK/KEW-BUY/P005) • Prosedur Tender (UPM/SOK/KEW-BUY/P006)
	A.15.2	**Supplier service delivery management** To maintain an agreed level of information security and service delivery in line with supplier agreements.					

	OPERASI PERKHIDMATAN SOKONGAN **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 49 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.15.2.1	**Monitoring and review of supplier services** Organizations shall regularly monitor, review and audit supplier service delivery.	Pejabat Bursar	YES	YES	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)
	A.15.2.2	**Managing changes to supplier services** Changes to the provision of services by suppliers, including maintaning and improving existing information security policies, procedures and controls, shall be managed, taking account of the critically of business information, systems and processes involved and re-assessment of risks.	Pejabat Bursar	YES	YES	memastikan polisi, prosedur dan kawalan bagi mengurus perubahan penyediaan perkhidmatan dilaksanakan	• GPKTMK Perkara 15.2 : Pengurusan Penyampaian Perkhidmatan Pihak Ketiga

UPM UNIVERSITI PUTRA MALAYSIA BERILMU BERBAKTI	**OPERASI PERKHIDMATAN SOKONGAN** **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 50 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
A.16 INFORMATION SECURITY INCIDENT MANAGEMENT	A.16.1	**Management of information security incidents and improvements** To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.					
	A.16.1.1	**Responsibilities and procedures** Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.	Seksyen Keselamatan	YES	YES	memastikan prosedur dan tanggungjawan pengurusan dibangunkan untuk memastikan tindak balas yang cepat dan berkesan terhadap insiden keselamatan	• GPKTMK Perkara 16.2 (a) : Pengurusan Maklumat Insiden Keselamatan ICT • Prosedur Pengendalian Insiden ICT (UPM/ISMS/OPR/KES/P004)
	A.16.1.2	**Reporting information security events** Information security events shall be reported through appropriate management channels as quickly as possible	Seksyen Keselamatan	YES	YES	memastikan insiden keselamatan dilapor dengan cepat melalui saluran pengurusan yang betul	• GPKTMK Perkara 16.1 (a) : Mekanisme Pelaporan Insiden Keselamatan ICT • Prosedur Pengendalian Insiden ICT (UPM/ISMS/OPR/KES/P004)

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.16.1.3	**Reporting security weaknesses** Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.	IDEC	YES	YES	memastikan staf dan pembekal melaporkan kelemahan keselamatan yang terdapat pada sistem atau perkhidmatan	• Prosedur penyelenggaraan ICT (UPM/SOK/ICTP001)
	A.16.1.4	**Assessment of and decision on information security events** Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	Seksyen Keselamatan	YES	YES	memastikan insiden keselamatan dinilai dan diputuskan sekiranya diklasifikasikan sebagai insiden keselamatan maklumat	• Pasukan UPMCERT • Prosedur Pengendalian Insiden ICT (UPM/ISMS/OPR/KES/P004)

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.16.1.5	**Response to information security incidents** Information security incidents shall be responded to in accordance with the documented procedures.	Seksyen Keselamatan	YES	YES	memastikan pengurusan insiden keselamatan mengikut prosedur	• Pasukan UPMCERT • Prosedur Pengendalian Insiden ICT (UPM/ISMS/OPR/KES/P004)
	A.16.1.6	**Learning from information security incidents** Knowledge gained from analysing and resolving information security incidents shall be used to reduced the likelihood or impact of future incidents.	Seksyen Keselamatan	YES	YES	memastikan analisis dan penyelesaian terhadap insiden keselamatan berlaku boleh digunakan untuk mengurangkan kemungkinan atau kesan pada masa akan datang	• Pasukan UPMCERT • Prosedur Pengendalian Insiden ICT (UPM/ISMS/OPR/KES/P004)
	A.16.1.7	**Collection of evidence** The organization shall define and apply procedures for the identification, collection, acquisition and preservation of	Seksyen Keselamatan	YES	YES	memastikan pengenalpastian, pengumpulan dan pemuliharaan maklumat perlu dilaksanakan sebagai bukti	• Pasukan UPMCERT • Prosedur Pengendalian Insiden ICT (UPM/ISMS/OPR/KES/P004)

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
		information, which can serve as evidence.					
A.17 INFROMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT	A.17.1	**Information security continuity** Infromation security continuity shall be embedded					
	A.17.1.1	**Planning information security continuity** The organization shall determine its requirements for information security and the continuity of information security management in adverse situation, eg. During a crisis or disaster.	CosCOMM	YES	YES	memastikan keperluan kesinambungan pengurusan keselamatan maklumat	• Pelan Kesinambungan Perkhidmatan
	A.17.1.2	**Implementing information security continuity** The organization shall establish, documen, implement and maintain processes, procedures and controls to ensure	CosCOMM	YES	YES	memastikan prosedur dan kawalan bagi kesinambungan perkhidmatan dibangun dan didokumenkan	• Pelan Kesinambungan Perkhidmatan

UPM UNIVERSITI PUTRA MALAYSIA BERILMU BERBAKTI	**OPERASI PERKHIDMATAN SOKONGAN** **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 54 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
		the required level of continuity for information security during an adverse situation.					
	A.17.1.3	**Verify, review and evaluate information security continuity** The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situation.	CosCOMM	YES	YES	memastikan maklumat kawalan kesinambungan keselamatan disahkan dan dilaksanakan secara berkala untuk memastikan ia berkesan sekiranya berlaku bencana	• GPKTMK 17.0 (MS33) • Pelan Kesinambungan Perkhidmatan • Laporan Pengujian Simulasi DRP ICT UPM
	A.17.2	**Redundancies** To ensure availability of information processing facilities.					
	A.17.2.1	**Availability of information processing facilities** Information processing facilities shall be implemented with with	Seksyen Pusat Data	YES	YES	memastikan fasiliti pemprosesan dibangunkan bagi memenuhi keperluan ketersediaan maklumat	• Server dan storan Pemulihan bencana (DR) (Aplikasi utama Universiti • Storan khas arkib harian (pangkalan data universiti)

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
		redundancy sufficient to meet availability requirements.					
A.18 COMPLIANCE	A.1.8.1	**Compliance with legal and contractual requirements** To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requiments.					
	A.18.1.1	**Identification of applicable legislation and contractual requirements** All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented, and kept up to date for each information system and the organization.	Pejabat penasihat Undang-undang	YES	YES	memastikan keperluan perundangan dikenal pasti dan didokumenkan serta dikemaskini	• GPKTMK Perkara 18.1 (d) : Keperluan Perundangan

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
	A.18.1.2	**Intellectual property rights** Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements related to intellectual property rights and use of proprietary software products.		YES	YES	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
	A.18.1.3	**Protection of records** Records shall be protected from loss, destruction and falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual, and business requirements.		YES	YES	memastikan rekod perlu di lindungi daripada kehilangan, kemusnahan, pemalsuan, akses tanpa kebenaran, peraturan, kontra atau keperluan bisnes	• GPKTMK Perkara 8.3 (c) : Keselamatan Dokumen • Prosedur Kawalan Dokumen dan Rekod ISO (UPM/PGR/P001) • Akta Arkib Negara 2003 (Akta 629)
	A.18.1.4	**Privacy and protection of personally**		YES	YES	memastikan perlindungan	• GPKTMK Perkara 13.3 : Pengurusan Pertukaran Maklumat

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
		identifiable infromation Privacy and protection of personally identifiable infromation shall be assured as required in relevant legislation and regulation where applicable.				terhadap maklumat peribadi memenuhi keperluan perundangan berkaitan	• Prosedur Pertukaran Maklumat (UPM/ISMS/SOK/P002) • Prosedur Kawalan Dokumen dan Rekod ISO (UPM/PGR/P001)
	A.18.1.5	**Regulation of cryptographic controls** Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.		YES	YES		• 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)
	A.18.2	**Information security reviews** To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.					
	A.18.2.1	**Independent review of information security** The organization's approach to managing information security and		YES	YES	memastikan pengurusan keselamatan maklumat dikaji	• Mesyuarat Jawatankuasa Kerja ISMS • Mesyuarat Keberkesanan Semakan Pengurusan ISMS (MKSP) • Audit Dalaman ISMS • Audit Badan Pensijilan

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/ No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
		its implementation (i.e. control onjectives, controls, policies, processes and procedures for information security) shall be reviewed independantly at planned intervals or when significant changes occur.				semula secara berkala atau apabila perubahan ketara berlaku	
	A.18.2.2	**Compliance with security policies and standards** Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.		YES	YES	memastikan pematuhan ke atas proses dan prosedur disemak semula dengan dasar-dasar keselamatan yang sesuai , standard dan sebarang keperluan keselamatan yang lain	• Mesyuarat Jawatankuasa Kerja ISMS • Mesyuarat Keberkesanan Semakan Pengurusan ISMS (MKSP)

	OPERASI PERKHIDMATAN SOKONGAN **PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI** Kod Dokumen : UPM/ISMS/OPR/SOA	Halaman 59 / 60 No. Semakan: 07 No. Isu: 01
	STATEMENT OF APPLICABILITY	Tarikh : 16/11/2015

ISO/IEC 27001:2013 Controls			**Owner**	**Applicable (Yes/No)**	**Implemented (Yes/Partial/ No)**	**Justification**	**Current Controls**
Clause	**Sec**	**Control Objective/Control**					
	A.18.2.3	**Technical compliance review** Information systems shall be regularly reviewed for compliance with the organization's information security security policies and standards.	Seksyen Keselamatan	YES	YES	memastikan sistem maklumat hendaklah dikaji semula secara berkala untuk mematuhi dasar dan standard keselamatan keselamatan maklumat organisasi.	• Mesyuarat Jawatankuasa Kerja ISMS • Audit Dalaman ISMS • Laporan Pentest

LAMPIRAN 7

<table>
<tr><th colspan="2">Huraian Pindaan Dokumen</th><th rowspan="2">Tambahan (T) / ~~Pemotongan~~ (P)</th></tr>
<tr><th>Asal</th><th>Pindaan</th></tr>
<tr><td>Nama Dokumen: GARIS PANDUAN ~~PENGUKURAN KEBERKESANAN KAWALAN ISMS~~
Kod Dokumen: UPM/ISMS/OPR/DC/GP07/SECURITY METRICS
No. Isu: 01, No. Semakan: 02, Tarikh Kuatkuasa: 05/06/2015</td><td>Nama Dokumen: GARIS PANDUAN PEMANTAUAN, PENGUKURAN, ANALISIS DAN PENILAIAN
Kod Dokumen: UPM/ISMS/OPR/DC/GP07/SECURITY METRICS
No. Isu: 01, No. Semakan: 03,</td><td>P</td></tr>
<tr><td>2.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Lampiran 1 : ~~Security Metrics~~</td></tr></table></td><td>2.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Lampiran 1 : Borang Perincian</td></tr></table></td><td></td></tr>
<tr><td>4.0 PENGUKURAN KEBERKESANAN KAWALAN ISMS

Kawalan yang bersesuaian perlu dikenalpasti bagi mengukur keberkesanan ISMS. Kriteriakriteria berikut perlu diberi perhatian dalam dalam mengukur keberkesanan:-

~~i. Tujuan yang spesifik~~
~~ii. Mudah difahami~~
~~iii. Boleh diukur~~
~~iv. Ada peluang untuk penambahbaikan~~
~~v. Tahap ukuran yang boleh dicapai~~
~~vi. Maklumat mudah diperolehi~~
~~vii. Kekerapan pengukuran~~

~~Security Metrics~~ yang telah dibangunkan perlu dilaksanakan secara berkala bagi memantau keberkesanan kawalan yang</td><td>4.0 PENGUKURAN KEBERKESANAN KAWALAN ISMS

Kawalan yang bersesuaian perlu dikenalpasti bagi mengukur keberkesanan ISMS. Kriteria-kriteria berikut perlu diberi perhatian dalam dalam mengukur keberkesanan:-

a. Perkara yang perlu dipantau dan diukur, termasuk proses dan kawalan ke atas keselamatan maklumat melibatkan:
i. Petunjuk prestasi
ii. Pengukuran keberkesanan
b. Kaedah untuk pemantauan, pengukuran, analisis dan penilaian yang berkenaan untuk memastikan hasil yang sah dan tepat;
c. Masa pelaksanaan pemantauan dan pengukuran;
d. Staf yang terlibat dalam pemantauan dan pengukuran;</td><td></td></tr>
</table>

telah dilaksanakan dan semua maklumat perlu direkodkan.	e. Proses analisis dan penilaian terhadap keputusan pemantauan dan pengukuran; dan f. Staf yang telibat dalam membuat analisis dan penilaian terhadap keputusan pemantauan dan pengukuran. Pengukuran yang telah dibangunkan perlu dilaksanakan secara berkala bagi memantau keberkesanan kawalan yang telah dilaksanakan dan semua maklumat perlu direkodkan.	

UPM UNIVERSITI PUTRA MALAYSIA	**PENGURUSAN** Kod Dokumen: PGR/BR04/AD 02
	BORANG JADUAL AUDIT DALAMAN

Ketua Juruaudit Dalaman : Encik Krishnan Mariappan

Kumpulan : B

Ketua Kumpulan : Tuan Sayid Mohamad Nazari Sayid Ismail

Tarikh Audit : 18-19 November 2015

Masa : 8.30 pagi hingga 5.00 petang

Proses Yang Akan Diaudit : Penilaian dan Rawatan Risiko

Program Audit :

Sub. Kumpulan	PTJ Diaudit	Juruaudit UPM	Dari	Juruaudit PTJ Diaudit	Skop Audit
Tiada	Jawatankuasa Penilaian Risiko	• Tuan Sayid Mohamad Nazari Sayid Ismail • Puan Rosliza Ibrahim • Puan Noraihan Noordin	• iDEC • iDEC • BPQ	Tiada	Klausa : 6.1 8.2 8.3 Annex : A.16 A.17

Disediakan oleh:

Tandatangan Penyelaras Audit

Nama: NORAIHAN NOORDIN

Tarikh: 30/10/2015

Disahkan Oleh:

Tandatangan Wakil Pengurusan

Nama: DATO' WAN AZMAN WAN OMAR

Tarikh: 30/10/2015

	PENGURUSAN
	Kod Dokumen: PGR/BR04/AD 02
	BORANG JADUAL AUDIT DALAMAN

Ketua Juruaudit Dalaman : Encik Krishnan Mariappan

Kumpulan : A

Ketua Kumpulan : Encik Mat Razi Abdullah

Tarikh Audit : 18-19 November 2015

Masa : 8.30 pagi hingga 5.00 petang

Proses Yang Akan Diaudit : Pengurusan

Program Audit :

Sub. Kumpulan	PTJ Diaudit	Juruaudit UPM	Dari	Juruaudit PTJ Diaudit	Skop Audit
Tiada	• Bahagian Pengurusan Kualiti • Bahagian Pembangunan Sumber Manusia • Pusat Pembangunan Maklumat dan Komunikasi	• Encik Mat Razi Abdullah • Encik Krishnan Mariappan • Puan Juraidah Mohamad Amin • Puan Hajjah Faridah Abu Aman	• BPQ • iDEC • iDEC • iDEC	Tiada	Klausa : 4.1 4.2 4.3 4.4 5.1 5.2 5.3 6.2 9.1 9.2 9.3 10.1 10.2 Annex: A.5 A.6 A.7

Disediakan oleh:

Tandatangan Penyelaras Audit

Nama: NORAIHAN NOORDIN

Tarikh: 30/10/2015

Disahkan Oleh:

Tandatangan Wakil Pengurusan

Nama: DATO' WAN AZMAN WAN OMAR

Tarikh: 30/10/2015

UPM UNIVERSITI PUTRA MALAYSIA	**PENGURUSAN** Kod Dokumen: PGR/BR04/AD 02
	BORANG JADUAL AUDIT DALAMAN

Ketua Juruaudit Dalaman : Encik Krishnan Mariappan

Kumpulan : C

Ketua Kumpulan : Puan Hashimah Amat Sejani

Tarikh Audit : 18-19 November 2015

Masa : 8.30 pagi hingga 5.00 petang

Proses Yang Akan Diaudit : Pelaksanaan ISMS

Progran Audit :

Sub. Kumpulan	PTJ Diaudit	Juruaudit UPM	Dari	Juruaudit PTJ Diaudit	Skop Audit
Tiada	• Kolej • Pejabat Bursar • Pusat Kesihatan Universiti • Bahagian Keselamatan Universiti • Pejabat Penasihat Undang-Undang • Pusat Pembangunan Maklumat dan Komunikasi • Bahagian Kemasukan Akademik • Perpustakaan Sultan Samad • Bahagian Pengurusan Sumber Manusia • Bahagian Perkhidmatan Sumber Manusia	• Puan Hashimah Amat Sejani • Encik Shahril Iskandar Amir • Encik Ahmad Faisal Abd Ghaffar • Puan Zurayawati Sulaiman • Puan Haryati Abdullah • Encik Hasidin Abdul Rashid • Tuan Haji Rusli Ahmad • Encik Mohd Zul Mohd Yusoff • Puan Hamidah Meseran	• iDEC • iDEC • iDEC • iDEC • iDEC • iDEC • iDEC • iDEC • iDEC	Tiada	Klausa : 7.1 7.2 7.3 7.4 7.5 8.2 8.3 Annex : A.8 A.9 A.10 A.11 A.12 A.13 A.14 A.15 A.16 A.17 A.18

Disediakan oleh:

Tandatangan Penyelaras Audit

Nama: NORAIHAN NOORDIN

Tarikh: 30/10/2015

Disahkan Oleh:

Tandatangan Wakil Pengurusan

Nama: DATO' WAN AZMAN WAN OMAR

Tarikh: 30/10/2015

UPM UNIVERSITI PUTRA MALAYSIA	**PENGURUSAN** Kod Dokumen: PGR/BR04/AD 02
	BORANG JADUAL AUDIT DALAMAN

Ketua Juruaudit Dalaman : Encik Krishnan Mariappan

Kumpulan : B

Ketua Kumpulan : Tuan Sayid Mohamad Nazari Sayid Ismail

Tarikh Audit : 18-19 November 2015

Masa : 8.30 pagi hingga 5.00 petang

Proses Yang Akan Diaudit : Penilaian dan Rawatan Risiko

Program Audit :

Sub. Kumpulan	PTJ Diaudit	Juruaudit UPM	Dari	Juruaudit PTJ Diaudit	Skop Audit
Tiada	Jawatankuasa Penilaian Risiko	• Tuan Sayid Mohamad Nazari Sayid Ismail • Puan Rosliza Ibrahim • Puan Noraihan Noordin	• iDEC • iDEC • BPQ	Tiada	Klausa : 6.1 8.2 8.3 Annex : A.16 A.17

Disediakan oleh:

Tandatangan Penyelaras Audit

Nama: NORAIHAN NOORDIN

Tarikh: 30/10/2015

Disahkan Oleh:

Tandatangan Wakil Pengurusan

Nama: DATO' WAN AZMAN WAN OMAR

Tarikh: 30/10/2015

	PENGURUSAN
	Kod Dokumen: PGR/BR04/AD 02
	BORANG JADUAL AUDIT DALAMAN

Ketua Juruaudit Dalaman : Encik Krishnan Mariappan

Kumpulan : A

Ketua Kumpulan : Encik Mat Razi Abdullah

Tarikh Audit : 18-19 November 2015

Masa : 8.30 pagi hingga 5.00 petang

Proses Yang Akan Diaudit : Pengurusan

Program Audit :

Sub. Kumpulan	PTJ Diaudit	Juruaudit UPM	Dari	Juruaudit PTJ Diaudit	Skop Audit
Tiada	• Bahagian Pengurusan Kualiti • Bahagian Pembangunan Sumber Manusia • Pusat Pembangunan Maklumat dan Komunikasi	• Encik Mat Razi Abdullah • Encik Krishnan Mariappan • Puan Juraidah Mohamad Amin • Puan Hajjah Faridah Abu Aman	• BPQ • iDEC • iDEC • iDEC	Tiada	Klausa : 4.1 4.2 4.3 4.4 5.1 5.2 5.3 6.2 9.1 9.2 9.3 10.1 10.2 Annex: A.5 A.6 A.7

Disediakan oleh:

Tandatangan Penyelaras Audit

Nama: NORAIHAN NOORDIN

Tarikh: 30/10/2015

Disahkan Oleh:

Tandatangan Wakil Pengurusan

Nama: DATO' WAN AZMAN WAN OMAR

Tarikh: 30/10/2015

UPM UNIVERSITI PUTRA MALAYSIA	**PENGURUSAN** Kod Dokumen: PGR/BR04/AD 02
	BORANG JADUAL AUDIT DALAMAN

Ketua Juruaudit Dalaman : Encik Krishnan Mariappan

Kumpulan : C

Ketua Kumpulan : Puan Hashimah Amat Sejani

Tarikh Audit : 18-19 November 2015

Masa : 8.30 pagi hingga 5.00 petang

Proses Yang Akan Diaudit : Pelaksanaan ISMS

Progran Audit :

Sub. Kumpulan	PTJ Diaudit	Juruaudit UPM	Dari	Juruaudit PTJ Diaudit	Skop Audit
Tiada	• Kolej • Pejabat Bursar • Pusat Kesihatan Universiti • Bahagian Keselamatan Universiti • Pejabat Penasihat Undang-Undang • Pusat Pembangunan Maklumat dan Komunikasi • Bahagian Kemasukan Akademik • Perpustakaan Sultan Samad • Bahagian Pengurusan Sumber Manusia • Bahagian Perkhidmatan Sumber Manusia	• Puan Hashimah Amat Sejani • Encik Shahril Iskandar Amir • Encik Ahmad Faisal Abd Ghaffar • Puan Zurayawati Sulaiman • Puan Haryati Abdullah • Encik Hasidin Abdul Rashid • Tuan Haji Rusli Ahmad • Encik Mohd Zul Mohd Yusoff • Puan Hamidah Meseran	• iDEC • iDEC • iDEC • iDEC • iDEC • iDEC • iDEC • iDEC • iDEC	Tiada	Klausa : 7.1 7.2 7.3 7.4 7.5 8.2 8.3 Annex : A.8 A.9 A.10 A.11 A.12 A.13 A.14 A.15 A.16 A.17 A.18

Disediakan oleh:

Tandatangan Penyelaras Audit

Nama: NORAIHAN NOORDIN

Tarikh: 30/10/2015

Disahkan Oleh:

Tandatangan Wakil Pengurusan

Nama: DATO' WAN AZMAN WAN OMAR

Tarikh: 30/10/2015