MINIT MESYUARAT JAWATANKUASA KERJA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
MS ISO/IEC 27001:2013 KALI KEDUA

TARIKH	**:**	**16 JUN 2016 (KHAMIS)**
MASA	**:**	**9.00 PAGI**
TEMPAT	**:**	**BILIK ANGSANA PUTRA 1, ARAS 2, BANGUNAN CANSELORI PUTRA, UNIVERSITI PUTRA MALAYSIA**
KEHADIRAN	**:**	**LAMPIRAN A**

MINIT	AGENDA	TINDAKAN/ MAKLUMAN
2.1	**ALUAN PENGERUSI** Pengerusi: 2.1.1. mengalu-alukan kehadiran ahli ke Mesyuarat Jawatankuasa Kerja Sistem Pengurusan Keselamatan Maklumat Kali Kedua; 2.1.2 memaklumkan Struktur Jawatankuasa ISMS beserta terma rujukan jawatankuasa adalah seperti pada **Lampiran 1**; 2.1.3 mencadangkan supaya Encik Hashim Md Shari dilantik sebagai Penasihat Jawatankuasa Kerja ISMS yang baharu. Mesyuarat dimaklumkan 2 orang Penasihat Jawatankuasa Kerja ISMS sediaada adalah Tuan Haji Rosdi Wah dan Encik Rosmi Othman; 2.1.4 memaklumkan mengenai skop persijilan ISMS iaitu: a) Sistem Pengurusan Keselamatan Maklumat hanya melibatkan proses Pendaftaran Pelajar Baharu Prasiswazah semasa Minggu Perkasa Putra; b) Sistem Pengurusan Keselamatan Maklumat untuk	**Makluman** **Makluman** **Sekretariat Pusat Jaminan Kualiti** **Makluman**

MINIT	AGENDA	TINDAKAN/ MAKLUMAN
	Pengoperasian Pusat Data bagi proses Pendaftaran Pelajar Baharu Prasiswazah; dan c) Sistem Pengurusan Keselamatan Maklumat untuk Pengoperasian Pusat Pemulihan Bencana bagi proses Pendaftaran Pelajar Baharu Prasiswazah.	
2.2	**PENGESAHAN MINIT MESYUARAT JAWATANKUASA KERJA SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS) MS ISO/IEC 27001:2013 KALI PERTAMA** Minit Mesyuarat Jawatankuasa Kerja Sistem Pengurusan Keselamatan Maklumat (ISMS) MS ISO/IEC 27001:2013 Kali Pertama yang diadakan pada 6 November 2016 disahkan tanpa sebarang pindaan.	**Makluman**
2.3	**PERKARA-PERKARA BERBANGKIT** 2.3.1 Mesyuarat meneliti perkara-perkara berbangkit hasil Mesyuarat Jawatankuasa Kerja Sistem Pengurusan Keselamatan Maklumat (ISMS) MS ISO/IEC 27001:2013 Kali Pertama adalah seperti pada **Lampiran 2.** 2.3.2 Mesyuarat seterusnya mengambil perhatian terhadap perkara berikut, iaitu: a) **<u>Minit 1.2.2 (ii)</u>** - meminta supaya Pengukuran Objektif ISMS dibuat dengan merujuk kepada Garis Panduan Pemantauan Pengukuran Analisis & Penilaian (UPM/ISMS/OPR/DC/GP07/SECURITY/METRICS) yang telah dikuatkuasakan pada 16 November 2015. b) **<u>Minit 1.3.2.3</u>** - mengambil maklum status pelaksanaan tiga (3) latihan ISMS yang telah diluluskan oleh Mesyuarat Jawatankuasa Latihan Universiti Putra Malaysia (JKLU) Kali Ke-11 adalah seperti berikut: i) Latihan Pengukuhan Penggunaan *The Malaysian Public Sector Information Security Risk Assessment System* (MyRAM App 2.0) telah dilaksanakan pada 2 Februari 2016 kepada semua peneraju Proses ISMS.	**Makluman** **Peneraju ISMS Berkenaan** **Makluman**

MINIT	AGENDA	TINDAKAN/ MAKLUMAN
	ii) Kursus Audit Dalaman Sistem Pengurusan Keselamatan Maklumat yang dirancang pada 6 hingga 7 April 2016 akan dijadualkan semula sekitar bulan Ogos 2016 dengan sasaran peserta iaitu pegawai yang berpotensi untuk dilantik sebagai Juruaudit Dalaman ISMS, wakil PTJ yang terlibat dengan proses ISMS dan juga peneraju proses ISMS.	**Sekretariat Pusat Jaminan Kualiti**
	iii) Kursus Perluasan Skop Sistem Pengurusan Keselamatan Maklumat yang dijadual pada 25 hingga 26 Oktober 2016 perlu melibatkan Peneraju Sediaada iaitu Peneraju Skop Pendaftaran Pelajar Baharu serta Peneraju Baharu yang terlibat dengan aktiviti perluasan skop dan entiti iaitu Pusat Pembangunan Akademik, *Putra Science Park* dan Universiti Putra Malaysia Kampus Bintulu.	**Sekretariat Pusat Jaminan Kualiti**
2.4	**LAPORAN PENILAIAN RISIKO SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS) MS ISO/IEC 27001:2013 (SEMAKAN JUN 2016)**	
	2.4.1 Mesyuarat mengambil maklum berkaitan laporan penilaian risiko berdasarkan *The Malaysian Public Sector Information Security Risk Assessment System* (MyRAM) adalah seperti pada **Lampiran 3.**	**Makluman**
	2.4.2 Mesyuarat mengambil maklum terdapat sebanyak 527 aset telah dinilai dan hasil penilaian mendapati empat (4) aset dikategorikan berisiko tinggi (dengan 13 ancaman) dan 254 aset berisiko sederhana dan 260 aset berisiko rendah.	**Makluman**
	2.4.3 Mesyuarat meneliti dan bersetuju meluluskan laporan penilaian risiko (semakan Jun 2016) sepertimana yang telah dibentang dengan beberapa penambahbaikan yang dicadangkan semasa mesyuarat.	**Jawatankuasa Penilaian Risiko/ Peneraju Proses ISMS**
	2.4.4 Mesyuarat meminta satu mesyuarat khas diadakan 2 minggu sebelum tarikh audit pihak ketiga bagi meluluskan semula laporan penilaian risiko mengambilkira beberapa perubahan yang berlaku dalam proses pendaftaran pelajar baharu prasiswazah (pendaftaran mengikut zon) serta pengemaskinian maklumat terkini daripada setiap peneraju proses.	**Sekretariat Pusat Jaminan Kualiti/ Jawatankuasa Penilaian Risiko/ Peneraju Proses ISMS**

MINIT	AGENDA	TINDAKAN/ MAKLUMAN
2.5	**LAPORAN PELAN PEMULIHAN RISIKO SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS) MS ISO/IEC 27001:2013**	
	2.5.1 Mesyuarat meneliti laporan pemulihan risiko Sistem Pengurusan Keselamatan Maklumat (ISMS) berdasarkan laporan penilaian risiko (semakan Jun 2016) sepertimana pada **Lampiran 3.**	**Makluman**
	2.5.2 Mesyuarat meminta supaya laporan pelan pemulihan risiko bagi aset yang berisiko tinggi yang melibatkan projek sistem sokongan (Pusat Data) dikemaskini dengan memasukkan maklumat kawalan melalui pemeriksaan bangunan selamat diduduki dan melaksanakan mitigasi (mitigation) untuk mengelak banjir di kawasan persekitaran Pusat Data bagi membolehkan Pusat Data beroperasi di lokasi sedia ada manakala bagi projek pembayaran yuran pelajar baharu prasiswazah dengan menambah kawalan pemulihan risiko melalui kaedah Kempen 'Jom Pay'.	**Jawatankuasa Penilaian Risiko/ Peneraju Terlibat**
2.6	**LAPORAN *STATEMENT OF APPLICABILITY* (SOA)**	
	2.6.1 Mesyuarat meneliti Laporan *Statement of Applicability (SoA)* Sistem Pengurusan Keselamatan Maklumat (ISMS) (UPM/ISMS/OPR/SoA) adalah seperti pada **Lampiran 4**.	**Makluman**
	2.6.2 Mesyuarat meneliti perubahan terhadap Kawalan A.6.2.2 *(Teleworking)* yang telah dibuat berdasarkan penambahbaikan proses kawalan capaian ke sistem oleh pentadbir proses.	**Makluman**
	2.6.3 Mesyuarat bersetuju meluluskan cadangan perubahan *Statement of Applicability (SoA)* untuk dikuatkuasakan pada 1 Julai 2016.	**Sekretariat Pusat Jaminan Kualiti/ Timbalan Pegawai Kawalan Dokumen iDEC**

MINIT	AGENDA	TINDAKAN/ MAKLUMAN
2.7	**OBJEKTIF KESELAMATAN SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS) MS ISO/IEC 27001:2013 TAHUN 2016** Mesyuarat- 2.7.1 mengambil maklum laporan pencapaian objektif keselamatan ISMS ISO/IEC 27001:2013 tahun 2016 adalah sepertimana pada **Lampiran 5.** 2.7.2 turut mengambil maklum 2 objektif keselamatan ISMS telah mencapai sasaran yang ditetapkan manakala 3 lagi objektif hanya dapat diukur pada sesi kemasukan 2016/2017. 2.7.3 mencadangkan supaya perkataan 'setiap semester' digugurkan daripada penyataan objektif 'Memastikan 95% sokongan ICT (rangkaian, sistem aplikasi dan pangkalan data) terhadap proses pendaftaran pelajar baharu bebas dari gangguan setiap semester' dan dikemaskini dalam Manual ISMS.	**Makluman** **Peneraju HEPA/Kolej/ BKU** **Sekretariat Pusat Jaminan Kualiti/ Timbalan Pegawai Kawalan Dokumen iDEC**
2.8	**<u>CADANGAN PINDAAN DOKUMEN (CPD)</u>** Mesyuarat- 2.8.1 maklum laporan cadangan pindaan dokumen Sistem Pengurusan Keselamatan Maklumat (ISMS) MS ISO/IEC 27001:2013 yang dibentangkan oleh Timbalan Pegawai Kawalan Dokumen (TPKD) adalah sepertimana pada **Lampiran 6.** Sebanyak 48 dokumen dipinda, 2 dokumen baharu diwujudkan dan 9 dokumen digugurkan. 2.8.2 meneliti dan bersetuju meluluskan kesemua 59 cadangan pindaan dokumen yang dikemukakan dengan beberapa penambahbaikan yang dicadangkan semasa mesyuarat dan akan dikuatkuasakan pada tarikh 01 Julai 2016.	**Makluman** **Sekretariat Pusat Jaminan Kualiti/ Timbalan Pegawai Kawalan Dokumen (TPKD) iDEC**

MINIT	AGENDA	TINDAKAN/ MAKLUMAN
	2.8.3 meminta Peneraju Pasukan Pusat Data mengadakan taklimat kesedaran kepada semua ahli pasukan bagi memastikan maklumat perubahan dokumen dapat disampaikan dengan berkesan kepada pegawai yang terlibat.	**Peneraju Pasukan Pusat Data**
2.9	**LAPORAN PELAKSANAAN ISMS SETIAP PASUKAN** **2.9.1 Pasukan Pusat Data** Mesyuarat meneliti dan mengambil maklum laporan pelaksanaan ISMS di Pusat Data yang merangkumi laporan dokumentasi, kawalan akses, aset dan Infrastruktur dan kawalan. Perincian mengenai pelaporan adalah sepertimana pada **Lampiran 7.** **2.9.2 Pasukan Pendaftaran Pelajar Baharu Prasiswazah** Mesyuarat meminta supaya laporan pelaksanaan ISMS oleh pasukan pendaftaran pelajar baharu prasiswazah dibentangkan dalam mesyuarat akan datang mengambilkira perubahan yang berlaku dalam proses pendaftaran pelajar baharu prasiswazah di UPM.	**Makluman** **Peneraju Pasukan Pendaftaran Pelajar Baharu Prasiswazah**
2.10	**HAL- HAL LAIN** **2.10.1 Laporan Penemuan Audit Dalaman ISMS Tahun 2016** Mesyuarat meneliti laporan penemuan Audit Dalaman ISMS Tahun 2016 yang telah dijalankan pada 3 hingga 5 Mei 2016. Sebanyak 16 laporan ketakakuran (NCR) dan 20 peluang penambahbaikan (OFI) dicatatkan sepanjang proses audit dilaksanakan. Perincian mengenai laporan penemuan audit dalaman ISMS tahun 2016 adalah seperti di **Lampiran 8.** **2.10.2 Perancangan Soal Selidik Pendaftaran Pelajar Baharu Prasiswazah** a) Mesyuarat mengambil maklum mengenai cadangan untuk mengadakan kajian soal selidik secara atas talian semasa hari pendaftaran pelajar baharu prasiswazah sesi kemasukan 2016/2017 yang dijadualkan pada 31 Ogos 2016 adalah seperti di **Lampiran 9.**	**Makluman** **Makluman**

MINIT	AGENDA	TINDAKAN/ MAKLUMAN
	b) Mesyuarat bersetuju supaya Peneraju Pasukan Pendaftaran Pelajar Baharu Prasiswazah diberi tanggungjawab untuk menyelaras pelaksanaan soal selidik ini dengan bantuan pihak Pusat Pembangunan Maklumat dan Komunikasi (iDEC) untuk penyediaan aplikasi bagi kajian ini.	**Peneraju Pendaftaran Pelajar Baharu Prasiswazah (Bahagian Hal Ehwal Pelajar)**
	c) Mesyuarat bersetuju setiap kolej kediaman menyediakan 1 kaunter khas bagi menempatkan 1 unit komputer yang akan dibekalkan oleh pihak iDEC untuk pelajar menjawab soal selidik secara atas talian.	**Bahagian Hal Ehwal Pelajar/Kolej Kediaman**
	2.10.3 Status Penutupan Peluang Penambahbaikan (OFI) Audit Pensijilan Semula SIRIM ISMS Tahun 2015	
	a) Mesyuarat mengambil maklum laporan status penutupan peluang penambahbaikan (OFI) Audit Pensijilan Semula SIRIM ISMS Tahun 2015 adalah sepertimana di **Lampiran 10.** Daripada 10 OFI yang diterima, sebanyak 6 OFI telah ditutup manakala baki 4 lagi OFI belum ditutup.	**Makluman**
	b) Mesyuarat meminta semakan semula dibuat bagi penghantaran bukti tindakan OFI No. 9 oleh peneraju Pasukan Penilaian Risiko dan meminta supaya memajukan surat peringatan kepada peneraju yang terlibat dengan OFI No. 1, 3 dan 5 yang masih belum memberi sebarang maklumbalas berkaitan penutupan OFI SIRIM.	**Sekretariat Pusat Jaminan Kualiti**
	2.10.4 Input Soalan Kaji Selidik Pemegang Taruh	
	a) Mesyuarat meneliti dan bersetuju dengan cadangan draf soalan kaji selidik pemegang taruh ISMS sepertimana di **Lampiran 11.**	**Makluman**
	b) Mesyuarat meminta supaya draf soalan kaji selidik ini dikemukakan kepada pihak iDEC untuk tujuan pembangunan aplikasi bagi soal selidik secara atas talian kepada pelajar baharu prasiswazah bagi sesi kemasukan 2016/2017.	**Sekretariat Pusat Jaminan Kualiti**

MINIT	AGENDA	TINDAKAN/ MAKLUMAN
2.11	**PENANGGUHAN MESYUARAT** Mesyuarat ditangguhkan pada jam 12.00 tengahari dengan ucapan terima kasih daripada Pengerusi.	

LAMPIRAN A

SENARAI KEHADIRAN MESYUARAT JAWATANKUASA KERJA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
MS ISO/IEC 27001:2013 KALI KEDUA

HADIR

1. Encik Mohd Faizal Daud - Pengerusi
2. Encik Rosmi Othman (Penasihat Jawatankuasa Kerja ISMS)
3. Encik Shahril Iskandar Amir
   (Pengerusi, Pasukan Pusat Data - Jawatankuasa Kerja ISMS)
4. Puan Shamriza Shari - Setiausaha

TURUT HADIR

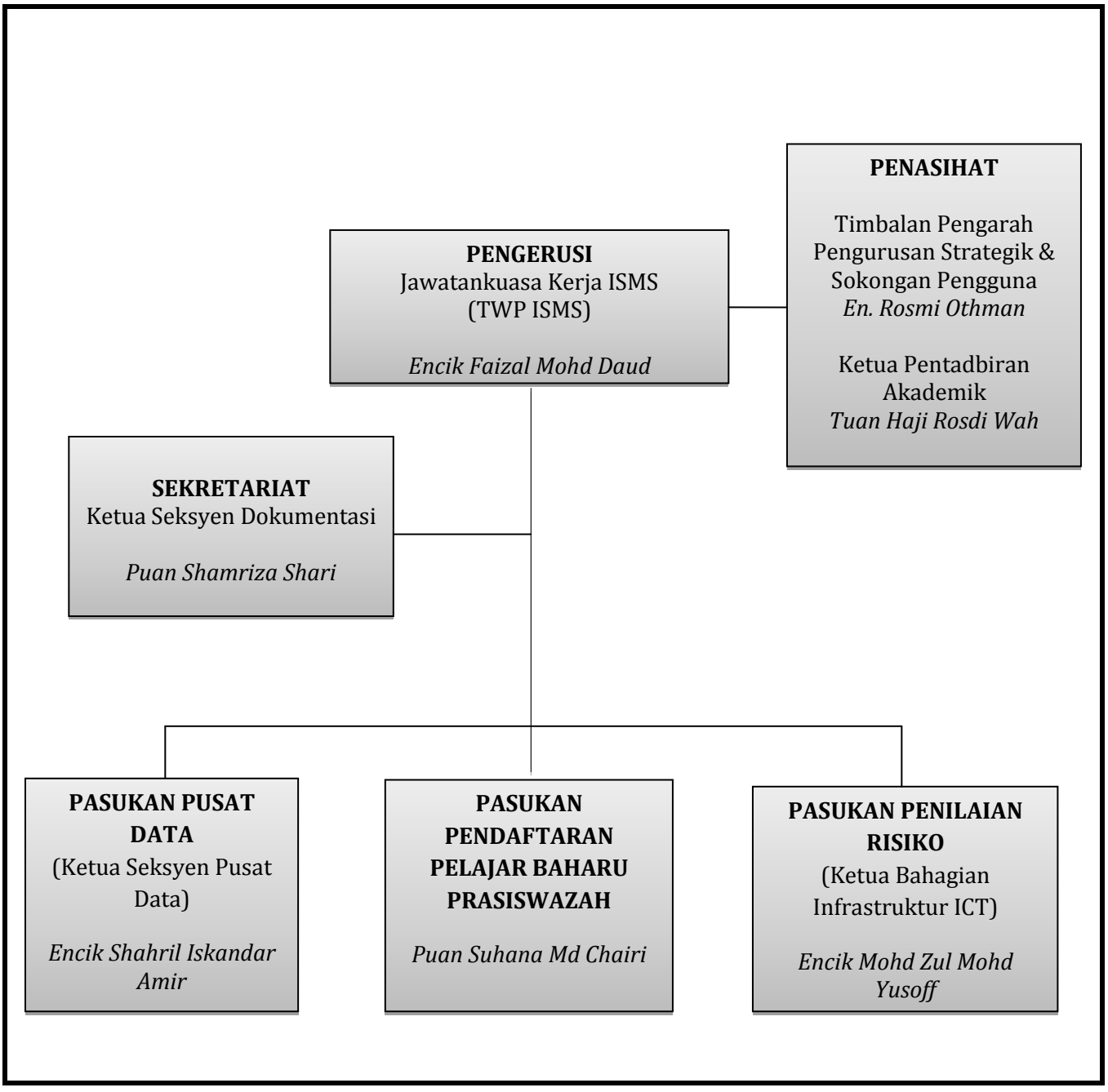
1. Tuan Haji Hashim Md. Shari
2. Puan Lailawati Bakar (Wakil Tuan Haji Rosdi Wah)
3. Puan Noraida Ahmad (Wakil Puan Suhana Md. Chairi)
4. Dr. Suhaila Abd. Hamid (Wakil Dr. Suhyna Mohamad Sulaiman)
5. Puan Salmah Uzairi
6. Tuan Haji Mokhtar Dahari
7. Puan Hashimah Amat Sejani (Wakil Pengerusi Pasukan Penilaian Risiko)
8. Puan Nurul Fatihah Md Marham (Timbalan Pegawai Kawalan Dokumen iDEC)

TIDAK HADIR DENGAN KENYATAAN

1. Tuan Haji Rosdi Wah (Penasihat Jawatankuasa Kerja ISMS)
2. Puan Suhana Md Chairi
   (Pengerusi, Pasukan Pendaftaran Pelajar Baharu Prasiswazah - Jawatankuasa Kerja ISMS)
3. Encik Mohd Zul Mohd Yusoff
   (Pengerusi, Pasukan Penilaian Risiko - Jawatankuasa Kerja ISMS)
4. Dr. Suhyna Mohamad Sulaiman
5. Puan Mazitah Ahmad
6. Dr. Haji Latif Anwar

LAMPIRAN 1

STRUKTUR JAWATANKUASA KERJA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)



TANGGUNGJAWAB JAWATANKUASA KERJA ISMS

1. Memantau keberkesanan pelaksanaan ISMS;
2. Memantau pencapaian objektif kualiti;
3. Melaksanakan penambahbaikan terhadap dokumentasi, proses dan perkhidmatan;
4. Menyediakan laporan keberkesanan pelaksanaan Sistem Pengurusan Keselamatan Maklumat;
5. Memantau dan menyemak carta perbatuan ISMS;
6. Membangunkan kriteria penerimaan risiko, tahap risiko dan *risk treatment plan;*
7. Melaksanakan keputusan dan tindakan hasil Mesyuarat Kajian Semula Pengurusan ISMS;
8. Membangun dan menyelenggara pengurusan dokumen dan rekod pelaksanaan ISMS; dan
9. Mengambil tindakan ke atas tindakan pembetulan, pencegahan dan peluang penambahbaikan.

LAMPIRAN 2

TINDAKAN SUSULAN BAGI PERKARA BERBANGKIT
MESYUARAT JAWATANKUASA KERJA SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS),
KALI PERTAMA PADA 06 NOVEMBER 2015

BIL	MINIT	AGENDA	TINDAKAN	STATUS PELAKSANAAN TINDAKAN
1.	**1.2**	1.2.2 **Objektif ISMS** ii. bersetuju agar, objektif ISMS seperti pada **Lampiran 3** diukur dan dibuat analisis mengikut format yang akan dikeluarkan oleh sekretariat.	Pusat Jaminan Kualiti	Format pengukuran dan analisis Objektif ISMS adalah dengan merujuk kepada Garis Panduan Pemantauan Pengukuran Analisis &Penilaian (UPM/ISMS/OPR/DC/GP07/SECURITY METRICS) yang telah dikuatkuasakan pada 16 November 2015.
2.	**1.3**	**KUATKUASA DOKUMENTASI** Mesyuarat bersetuju untuk meluluskan pindaan dokumen yang akan kuatkuasa pada 16 November 2015. Dokumen yang dipinda adalah seperti berikut: 1.3.1 Penilaian Risiko Sistem Pengurusan Keselamatan Maklumat (ISMS) (UPM/ISMS/OPR/RA) 1.3.1.2 bersetuju pada penilaian risiko bagi kad pelajar jumlah *people* adalah 7 orang ini kerana mengira hari pendaftaran di kolej-kolej.	Timbalan Kawalan Dokumen Jawatankuasa Penilaian Risiko	Telah dikemaskini dalam Sistem MyRAM mengambilkira jumlah *people* bagi penilaian risiko kad pelajar adalah seramai 8 orang.

BIL	MINIT	AGENDA	TINDAKAN	STATUS PELAKSANAAN TINDAKAN
		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	Semakan SOA telah dilaksanakan dan dikuatkuasakan pada 7 Disember 2015.
		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	Mesyuarat dengan Pejabat Bursar telah diadakan pada November 2015 dan mesyuarat bersetuju bahawa keperluan berkaitan keselamatan maklumat hanya melibatkan kontrak perolehan yang terlibat di Perpustakaan Sultan Abdul Samad.
		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	Maklumat keperluan latihan ISMS telah dihantar kepada pihak Seksyen Latihan, Pejabat Pendaftar dan telah dimasukkan dalam Takwim Latihan UPM yang telah diluluskan oleh Mesyuarat Jawatankuasa Latihan Universiti Putra Malaysia (JKLU) Kali Ke 11 pada 20 Januari 2016.
		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	Garis Panduan Pemantauan Pengukuran Analisis & Penilaian (UPM/ISMS/OPR/DC/GP07/SECURITY METRICS) telah dikuatkuasakan pada 16 November 2015.

LAMPIRAN 3

HASIL PENILAIAN RISIKO DAN STATUS PELAN PEMULIHAN RISIKO

Keperluan penilaian risiko dalam pelaksanaan ISMS adalah berdasarkan kepada Standard MS ISO/IEC 27001:2013, iaitu:

Klausa 6.1 : *Actions to address risk and opportunities*
Klausa 8.2 : *Information security risk assessment*
Klausa 8.3 : *Information security risk treatment*

Bil	Output penilaian risiko Jumlah aset :	Projek	Punca dominan	Pelan pemulihan	Tanggungjawab
1.	Aset berisiko tinggi = 13	Sistem Sokongan (Pusat Data)	**Bangunan iDEC Beta** 1. *Lightning* 2. *Fire* 3. *Water* 4. *Catastrophes in the environment* 5. *Failure of the IT system* **Bangunan iDEC Epsilon** 1. *Lightning* 2. *Fire* 3. *Water* 4. *Power failure* 5. *Catastrophes in the environment* 6. *Failure of the IT system*	Permohonan bangunan IDEC baru dalam RMK-11 Peringkat Pengurusan Universiti	Pusat Pembangunan Maklumat dan Komunikasi
		Pengesahan Laporan Pemeriksaan Kesihatan Pelajar Baharu Prasiswazah	**Laporan Pemeriksaan Kesihatan** - *Loss of data confidentiality/ integrity as a result of IT user error*	Semua pemeriksaan akan dilakukan di PKU UPM dan data akan disimpan didalam format digital	Pusat Kesihatan Universiti
		Pembayaran Yuran Pelajar Baharu Prasiswazah	***Cash Box*** - *Problems caused by big public events*	1. *90% cashless* 2. *100% Internet Banking*	Pejabat Bursar

Bil	Output penilaian risiko Jumlah aset :	Projek	Punca dominan	Pelan pemulihan	Tanggungjawab
2	Aset berisiko sederhana	Sistem Sokongan (Rangkaian)	*Cisco Catalyst 6509* *1. Hardware malfunctions* *2. Failure of a local area network or wide area network (LAN and WAN)* *Ruijie Switch S12006* *1. Hardware malfunctions* *2. Failure of a local area network or wide area network (LAN and WAN)* *Cisco Nexus 5000* *1. Hardware malfunctions* *2. Failure of a local area network or wide area network (LAN and WAN)* *LAN* - *Failure of a local area network or wide area network (LAN and WAN)* *WAN* - *Failure of a local area network or wide area network (LAN and WAN)*	1. Perjanjian perkhidmatan dengan pihak berkaitan 2. Penyelenggaraan berkala oleh pihak vendor *3. Monitoring* 4. Penyelenggaraan dan pemantauan berkala 5. Penyelenggaraan dan pemantauan berkala 6. Mewujudkan SOP penyelenggaraan LAN/WAN 7. Naiktaraf infrastruktur rangkaian	Pusat Pembangunan Maklumat dan Komunikasi

Bil	Output penilaian risiko Jumlah aset :	Projek	Punca dominan	Pelan pemulihan	Tanggungjawab
	Aset berisiko sederhana	Sistem Sokongan (Pusat Data)	I. *SERVER DNS* II. *Desktop Console* III. *Storage Infortrend EonNAS 3016* 1. *Power failure* 2. *Failure of the IT system* 3. *Threat posed by internal staff during maintenance or administration work* 4. *Personnel is not competent* 5. *Non-compliant with IT security measures, standards and policy* 6. *Hardware malfunctions* 7. *Disruption of power supply* I. Timbalan Pengarah Perkhidmatan ICT II. Ketua Bahagian Infrastruktur ICT III. Ketua Seksyen Pusat Data Penolong Pegawai Teknologi Maklumat Seksyen Pusat Data	1. Penyelenggaraan berkala Genset dan UPS 2. Pelaksanaan DRP ICT dan Pelan Kesinambungan Perkhidmatan UPM (PKP UPM) 3. Penyelenggaraan Berkala 4. Prosedur Pengoperasian Pengurusan Pusat Data 5. Program Kesedaraan pelaksanaan ISMS 6. Latihan berkaitan 7. Pemahaman kepada Standard, prosedur garis panduan dan, dokumen ISMS 8. Perjanjian perkhidmatan dengan pihak berkaitan	Pusat Pembangunan Maklumat dan Komunikasi

Bil	Output penilaian risiko Jumlah aset :	Projek	Punca dominan	Pelan pemulihan	Tanggungjawab
	Aset berisiko sederhana	Sistem Sokongan (Pusat Data)	IV. Juruteknik Seksyen Pusat Data 1. *Social engineering* Pegawai Teknologi Maklumat Seksyen Pusat Data 1. *Misuse of user & administrator rights* 2. *Social engineering* I. Fail Pendaftaran Pelawat II. Fail Pemantauan Capaian ke Sistem di Pusat Data III. Fail Pendaftaran Pembekal IV. Fail Pemantauan Operasi Pusat Data V. Fail Peralatan ICT Persendirian VI. Fail Pengukuran Keberkesanan ISMS VII. Fail Akses Staf ke Pusat Data - *Loss of confidentiality of classified information* *I. DR Standby Genset* *II. DR Centralised UPS* - *Hardware malfunctions* - *DR Centralised UPS*		

Bil	Output penilaian risiko Jumlah aset :	Projek	Punca dominan	Pelan pemulihan	Tanggungjawab
3	Aset Berisiko Rendah	Kad Pelajar Baharu Prasiswazah	*1.Preface* *2.Card Personalize* *Personnel is not competent* *Software malfunction*	Latihan dari pembekal perisian Penyelenggaraan Berkala	Bhg.Keselamatan
			1.Bahagian Keselamatan 2. Pembantu tadbir (Kolej) *Loss of Personnel* *Personnel is not competent*	Proses Latihan kepada staf lain kepada Proses Kerja Permohonan Kad Pintar UPM/OPR/BKU/AK01/ Kad Pintar -Latihan kesedaran ISMS - Latihan Prosedur Pendaftaran	
			1.Borang Permohonan Kad Pelajar *Inadvertant manipulation of data*	Arahan Kerja Permohonan Kad Pintar	
			1.Bilik Kad Pintar *Fire*	Penyelenggaraan alat Pemadam Api	
			1.Komputer Kad Pelajar *Power failure*	GPKTMK Perkara 11.1 (h): Perkhidmatan Sokongan	

Bil	Output penilaian risiko Jumlah aset :	Projek	Punca dominan	Pelan pemulihan	Tanggungjawab
	Aset Berisiko Rendah	Pengesahan Laporan Pemeriksaan Kesihatan Pelajar Baharu Prasiswazah	*1.CCTV* *Power failure* *Hardware malfunction* *Failure of LAN and WAN*		Pusat Kesihatan Universiti
			1. Paramedik 2. Staf Sokongan 3. Doktor Perubatan *Loss of Personnel* *Negligence in handling information and operating the IT System.*	1.Backup staf 2.Buku Panduan perkhidmatan kesihatan PKU 3.Pemantauan yang berterusan ke atas data.	
			1. Filem X-ray *Loss of data confidentility, Integrity*	Dimasukkan ke dalam sampul x-ray dan dimasukkan kedalam bekas khas	
			1. Rak Penyimpanan filem x-ray dan laporan pemeriksaan kesihatan *Loss of confidentiality of classified information*	Bilik simpanan berkunci CCTV di luar bilik simpanan	

Bil	Output penilaian risiko Jumlah aset :	Projek	Punca dominan	Pelan pemulihan	Tanggungjawab
	Aset Berisiko Rendah	Pengesahan Pendaftaran pelajar Baharu Prasiswazah di Kolej Kediaman	1. Staf Kolej Kediaman *negligence in handling information and operating the IT system*	Semakan semula data sekiranya terdapat ralat / kecuaian	Kolej Kediaman
			1. Borang Maklumat Peribadi Pelaja *negligence in handling information and operating the IT system*	Menggunapakai Prosedur Kawalan Rekod	
			1.Pendaftaran Kolej *Disruption of power supply*	Pendaftaran kehadiran pelajar secara manua	
			1. Semakan Tawaran *negligence in handling information and operating the IT system*	Kursus Fasilitator Minggu Putra Perkasa	

LAMPIRAN 4

MESYUARAT JAWATANKUASA KERJA KEDUA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
MS ISO/IEC/27001:2013

LAPORAN *STATEMENT OF APPLICABILITY* (SoA)

1. TUJUAN

Kertas ini adalah untuk mendapat pengesahan dan makluman Mesyuarat Jawatankuasa Kerja Sistem Pengurusan Keselamatan Maklumat (ISMS) Universiti Putra Malaysia (UPM) berkaitan laporan *Statement of Applicability* (SoA).

2. LATARBELAKANG

Statement of Applicability (SoA) adalah dokumen utama dalam pelaksanaan ISMS di mana dokumen SoA ini menjelaskan justifikasi kawalan dan dokumen rujukan dalam melindungi keselamatan aset ICT di dalam skop isms. Pemilihan kawalan dalan SoA adalah hasil pemulihan risiko dan peraturan-peraturan perlindungan aset ICT dalam Kaedah-Kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) dan Garis Panduan Keselamatan Teknologi Maklumat Komunikasi (GPKTMK).

3. LAPORAN

Terdapat 14 seksyen dan 114 kontrol yang terdapat di dalam dokumen SoA ini. Terdapat 1 kawalan yang disenarai pendek sebagai "NO" atau tidak diguna pakai di peringkat UPM atas justifikasi yang telah dipersetujui bersama pihak peneraju-peneraju proses. Rujuk jadual di bawah:

Seksyen	A.6.1.5
Kawalan	Information security in project management information security shall be addressed in project management, regardless of the type of the project
Justifikasi	Tiada sebarang pengurusan projek terlibat dalam pelaksanaan ISMS di bawah skop pensijilan

Semakan terhadap dokumen SoA telah dilaksanakan dan pindaan terhadap kawalan A.6.2.2 telah dibuat berdasarkan penambahbaikan terhadap proses kawalan capaian ke sistem oleh pentadbir proses. Perubahan kawalan boleh dirujuk pada Lampiran 1.

Cadangan pindaan dokumen bagi dokumen SoA bagi kawalan A.6.2.2 boleh dirujuk pada Lampiran 2.

4. SYOR

Mesyuarat diminta untuk mengambil maklum dan membuat keputusan berkaitan Cadangan pindaan dokumen *Statement of Applicability* (SoA) seperti yang dinyatakan pada Lampiran 2.

ISO/IEC 27001:2013 Controls			Owner	Applicable (Yes/No)	Implemented (Yes/Partial/No)	Justification	Current Controls
Clause	**Sec**	**Control Objective/Control**					
A.6 ORGANIZATION OF INFORMATION	A.6.2	**Mobile devices and teleworking** To ensure the security of teleworking and use of mobile devices.					
	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 Pembangunan Maklumat & Komunikasi (iDEC)	YES	YES	Pentadbir Sistem dibenarkan untuk akses dari luar UPMNET. , Akses dari UPMNET hanya dibenarkan dari workstation Pentadbir Sistem yang terkawal	• Garis Panduan Pemantauan Capaian ke Sistem (UPM/ISMS/OPR/GP06/ PEMANTAUAN CAPAIAN) Perkara 4.0 Pemantauan Capaian

No. CPD	Pemilik Proses	Huraian Pindaan Dokumen *		Tambahan (T) / ~~Pemotongan~~ (P)
		Asal	**Pindaan**	
ISMS (IDEC): 31/2016	**iDEC**	Nama Dokumen: STATEMENT OF APPLICABILITY (SoA) Kod Dokumen:UPM/ISMS/OPR/SOA No. Isu:_01_, No. Semakan:_08_, Tarikh Kuatkuasa: 07/12/2015	Nama Dokumen: STATEMENT OF APPLICABILITY (SoA) Kod Dokumen:UPM/ISMS/OPR/SOA No. Isu:_01_, No. Semakan: 09_, Tarikh Kuatkuasa: 01/07/2016	
		2.1 PENYEDIAAN SoA **c)** Membentangkan cadangan awal SoA dalam ~~mesyuarat pengurusan ISMS~~; dan	**3.1 PENYEDIAAN SoA** **c)** Membentangkan cadangan awal SoA dalam Mesyuarat Jawatankuasa Kerja ISMS; dan	**P**
		3.2 PELAKSANAAN SoA d) Melaporkan penemuan di para c) dalam ~~mesyuarat pengurusan ISMS~~ untuk pertimbangan dan kelulusan.	**3.2 PELAKSANAAN SoA** d) Melaporkan penemuan di para c) dalam Mesyuarat Jawatankuasa Kerja ISMS untuk pertimbangan dan kelulusan.	**P**
		Sec : A.5.1.2 **Current Control :** • 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	Sec : A.5.1.2 **Current Control :** • Kaedah-Kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi 2014) Bahagian B : Pelaksanaan dan Pindaan Dasar 4 (1) oleh LPU • GPKTMK 5.1 (c) Penyelenggaraan Perkara iv oleh iDEC	**P**
		Sec : A.6.2.2 Control Objective : **Teleworking** A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites. ~~Applicable = NO~~ ~~Implemented : NO~~	Sec : A.6.2.2 Control Objective : **Teleworking** A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites. Applicable = YES Implemented : YES	

		~~Justification :~~ ~~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~~	Justification : Pentadbir Sistem dibenarkan untuk akses dari luar UPMNET. , Akses dari UPMNET hanya dibenarkan dari workstation Pentadbir Sistem yang terkawal **Current Control :** • Garis Panduan Pemantauan Capaian ke Sistem (UPM/ISMS/OPR/GP06/ PEMANTAUAN CAPAIAN) Perkara 4.0 Pemantauan Capaian	
		Sec : A.9.1.1 **Current Control :** • 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)	Sec : A.9.1.1 **Current Control :** • GPKTMK Perkara 9.1 : Dasar Kawalan Capaian • Garis Panduan Kawalan Akses Ke Pusat Data (UPM/ISMS/OPR/GP03/KAWALAN AKSES) • Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/GP06/ PEMANTAUAN CAPAIAN)	**P**
		Sec : A.9.1.2 **Current Control :** • GPKTMK Perkara 13.2 : Kawalan Akses Rangkaian • Garis Panduan Pengurusan Pengagihan Rangkaian (UPM/ISMS/OPR/~~NET~~/GP13/AGIHAN RANGKAIAN)	Sec : A.9.1.2 **Current Control :** • GPKTMK Perkara 13.2 : Kawalan Akses Rangkaian • Garis Panduan Pengurusan Pengagihan Rangkaian (UPM/ISMS/OPR/GP13/AGIHAN RANGKAIAN)	**P**
		Sec : A.9.2.1 **Current Control :** • 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)	Sec : A.9.2.1 **Current Control :** • GPKTMK Perkara 9.2 : Pengurusan Capaian Pengguna • Prosedur Kawalan dan Pemantauan Capaian ke Sistem (UPM/ISMS/OPR/P003) • Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/GP06/PEMANTAUAN CAPAIAN)	**P**
		Sec : A.9.2.2 **Current Control :** • GPKTMK Perkara 9.2 : Pengurusan Capaian Pengguna • Garis Panduan Pemantauan Capaian Ke Sistem ~~Di Pusat~~	Sec : A.9.2.2 **Current Control :** • GPKTMK Perkara 9.2 : Pengurusan Capaian Pengguna • Garis Panduan Pemantauan Capaian Ke Sistem	**P**

		~~Data~~ (UPM/ISMS/OPR/~~DC~~/GP06/PEMANTAUAN CAPAIAN)	(UPM/ISMS/OPR/GP06/ PEMANTAUAN CAPAIAN)	
		Sec : A.9.2.3 **Current Control :** • GPKTMK Perkara 9.2 : Pengurusan Capaian Pengguna • Garis Panduan Pemantauan Capaian Ke Sistem ~~Di Pusat Data~~ (UPM/ISMS/OPR/~~DC~~/GP06/PEMANTAUAN CAPAIAN)	Sec : A.9.2.3 **Current Control :** • GPKTMK Perkara 9.2 : Pengurusan Capaian Pengguna • Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/GP06/ PEMANTAUAN CAPAIAN)	**P**
		Sec : A.9.2.4 **Current Control :** • GPKTMK Perkara 10.0 : Kawalan Kriptografi • Garis Panduan Pengurusan UPM-ID (UPM/ISMS/OPR/~~PD~~/GP16/UPM-ID)	Sec : A.9.2.4 **Current Control :** • GPKTMK Perkara 10.0 : Kawalan Kriptografi • Garis Panduan Pengurusan UPM-ID (UPM/ISMS/OPR /GP16/UPM-ID)	**P**
		Sec : A.9.2.5 **Current Control :** • Garis Panduan Pemantauan Capaian Ke Sistem ~~Di Pusat Data~~ (UPM/ISMS/OPR/~~DC~~/GP06/PEMANTAUAN CAPAIAN)	Sec : A.9.2.5 **Current Control :** • Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/GP06/PEMANTAUAN CAPAIAN)	**P**
		Sec : A.9.2.6 **Current Control :** • 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)	Sec : A.9.2.6 **Current Control :** • GPKTMK Perkara 9.2 : Pengurusan Capaian Pengguna • Prosedur Kawalan dan Pemantauan Capaian ke Sistem (UPM/ISMS/OPR/DC/P003) • Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/DC/GP06/PEMANTAUAN CAPAIAN)	**P**
		Sec : A.9.4.1 **Current Control :** • 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)	Sec : A.9.4.1 **Current Control :** • GPKTMK Perkara 9.1 : Dasar Kawalan Capaian • Prosedur Kawalan dan Pemantauan Capaian ke Sistem (UPM/ISMS/OPR//P003) • Garis Panduan Kawalan Akses Ke Pusat Data (UPM/ISMS/OPR//GP03/KAWALAN AKSES)	**P**

		• 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)	• Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR//GP06/PEMANTAUAN CAPAIAN) • Garis Panduan Pengendalian Maklumat (UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT)	
		Sec : A.9.4.2 **Current Control :** • GPKTMK Perkara 9.3 : Kawalan Akses Sistem Pengoperasian Server • Prosedur Kawalan dan Pemantauan Capaian ke Sistem ~~di Pusat Data~~ (UPM/ISMS/OPR/~~DC~~/P003)	Sec : A.9.4.2 **Current Control :** • GPKTMK Perkara 9.3 : Kawalan Akses Sistem Pengoperasian Server • Prosedur Kawalan dan Pemantauan Capaian ke Sistem (UPM/ISMS/OPR/P003)	**P**
		Sec : A.9.4.4 **Current Control :** • 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)	Sec : A.9.4.4 **Current Control :** • Prosedur Kawalan dan Pemantauan Capaian ke Sistem (UPM/ISMS/OPR/P003) • Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/GP06/PEMANTAUAN CAPAIAN)	**P**
		Sec : A.11.2.3 **Current Control :** • 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)	Sec : A.11.2.3 **Current Control :** • 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/GP12/PEMASANGAN KABEL)	**P**
		Sec : A.11.2.4 **Current Control :** • 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)	Sec : A.11.2.4 **Current Control :** • Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan komunikasi 2014) Bhgn D, 10 • GPKTMK Perkara 11.3 (e) : Penyelenggaraan Peralatan • Prosedur Penyelenggaraan ICT (UPM/OPR/IDEC/P003) • Prosedur Baik Pulih ICT (UPM/OPR/IDEC/P004) • Garis Panduan Penyelenggaraan Berkala (PPPA) (UPM/SOK/PYG/GP02)	**P**

		• Prosedur Penyelenggaraan Baik Pulih (PPPA) (UPM/SOK/PYG/P001)	• Prosedur Penyelenggaraan Baik Pulih (PPPA) (UPM/SOK/PYG/P001)	
		Sec : A.11.2.5 **Current Control :** • 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)	Sec : A.11.2.5 **Current Control :** • 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/OPR/IDEC/P004) • Prosedur Penyelenggaraan Baik Pulih (PPPA) (UPM/SOK/PYG/P001)	**P**
		Sec : A.11.2.6 **Current Control :** • 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)	Sec : A.11.2.6 **Current Control :** • UPM/SOK/KEW-AST/P012 : Prosedur Pengurusan Aset • GPKTMK Perkara 11.3 (f) : Peralatan Di Luar Premis • Prosedur Baik Pulih ICT (UPM/OPR/IDEC/P004) • Prosedur Penyelenggaraan Baik Pulih (PPPA) (UPM/SOK/PYG/P001)	**P**
		Sec : A.12.3.1 **Current Control :** • 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)	Sec : A.12.3.1 **Current Control :** • GPKTMK Perkara 12.3 (a) : Backup • Garis Panduan Pengurusan Backup Pangkalan Data (UPM/ISMS/OPR/GP14/BACKUP) • Garis Panduan Penggunaan Data Pengujian (UPM/ISMS/OPR/GP15/DATA PENGUJIAN)	**P**
		Sec : A.12.4.3 **Current Control :** • Prosedur Kawalan dan Pemantauan Capaian ke Sistem ~~di Pusat Data~~ (UPM/ISMS/OPR/~~DC~~/P003) • Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI)	Sec : A.12.4.3 **Current Control :** • Prosedur Kawalan dan Pemantauan Capaian ke Sistem (UPM/ISMS/OPR/P003) • Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI)	**P**

		Sec : A.12.6.1 **Current Control :** • 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	Sec : A.12.6.1 **Current Control :** • GPKTMK Perkara 12.6: Pengurusan Kerentanan Teknikal • Garis Panduan Penilaian Tahap Keselamatan (UPM/ISMS/OPR/GP09/TAHAP KESELAMATAN) • MyRAM Step 5, 6, 7 & 8	**P**
		Sec : A.12.7.1 **Current Control :** • 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	Sec : A.12.7.1 **Current Control :** • GPKTMK Perkara 12.7(a) : Kawalan Audit Sistem Maklumat • Garis Panduan Penilaian Tahap Keselamatan ICT (UPM/ISMS/OPR/GP09/TAHAP KESELAMATAN) • Badan Pensijilan SIRIM • Audit Dalaman ISMS	**P**
		Sec : A.13.1.1 **Current Control :** • 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)	Sec : A.13.1.1 **Current Control :** • GPKTMK Perkara 13.2 : Kawalan Akses Rangkaian • Garis Panduan Pengurusan Pengagihan Rangkaian (UPM/ISMS/OPR/GP13/AGIHAN RANGKAIAN) • ID & Password Staf • Private network (SMP) - network conceptual diagram)	**P**
		Sec : A.13.1.3 **Current Control :** • Garis Panduan Pengurusan Pengagihan Rangkaian (UPM/ISMS/OPR/~~NET~~/GP13/AGIHAN RANGKAIAN) • VLAN USPOT • VLAN Kolej/Fakulti/Institut • VLAN Pusat Data	Sec : A.13.1.3 **Current Control :** • Garis Panduan Pengurusan Pengagihan Rangkaian (UPM/ISMS/OPR/GP13/AGIHAN RANGKAIAN) • VLAN USPOT • VLAN Kolej/Fakulti/Institut • VLAN Pusat Data	**P**
		Sec : A.14.2.8 **Current Control :** • Garis Panduan Penilaian Tahap Keselamatan (UPM/ISMS/OPR/~~KES~~/GP09/TAHAP KESELAMATAN)	Sec : A.14.2.8 **Current Control :** • Garis Panduan Penilaian Tahap Keselamatan (UPM/ISMS/OPR/GP09/TAHAP KESELAMATAN)	**P**
		Sec : A.15.1.1 **Current Control :** • Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan komunikasi 2014) Bhgn F, 16 (c)	Sec : A.15.1.1 **Current Control :** • Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan komunikasi 2014) Bhgn F, 16 (c)	**P**

		• GPKTMK Perkara 15.1 : Pihak Ketiga • Prosedur Pengoperasian Pengurusan Pusat Data (UPM/ISMS/OPR/~~DC~~/P001)	• GPKTMK Perkara 15.1 : Pihak Ketiga • Prosedur Pengoperasian Pengurusan Pusat Data (UPM/ISMS/OPR/P001)	
		Sec : A.16.1.1 **Current Control :** • Pelan Kesinambungan Perkhidmatan (PKP) • ~~Prosedur Pengendalian Insiden ICT (UPM/ISMS/OPR/KES/P004)~~	Sec : A.16.1.1 **Current Control :** • Pelan Kesinambungan Perkhidmatan (PKP) • Garis Panduan Pengendalian Insiden ICT (UPM/ISMS/OPR/GP18/PENGENDALIAN INSIDEN)	**P**
		Sec : A.16.1.2 **Current Control :** • Pelan Kesinambungan Perkhidmatan (PKP) • ~~Prosedur Pengendalian Insiden ICT (UPM/ISMS/OPR/KES/P004)~~	Sec : A.16.1.2 **Current Control :** • Pelan Kesinambungan Perkhidmatan (PKP) • Garis Panduan Pengendalian Insiden ICT (UPM/ISMS/OPR/GP18/PENGENDALIAN INSIDEN)	**p**
		Sec : A.16.1.3 **Current Control :** • Pelan Kesinambungan Perkhidmatan (PKP) • ~~Prosedur Pengendalian Insiden ICT (UPM/ISMS/OPR/KES/P004)~~	Sec : A.16.1.3 **Current Control :** • Pelan Kesinambungan Perkhidmatan (PKP) • Garis Panduan Pengendalian Insiden ICT (UPM/ISMS/OPR/GP18/PENGENDALIAN INSIDEN)	**P**
		Sec : A.16.1.4 **Current Control :** • Pelan Kesinambungan Perkhidmatan (PKP) • ~~Prosedur Pengendalian Insiden ICT (UPM/ISMS/OPR/KES/P004)~~	Sec : A.16.1.4 **Current Control :** • Pelan Kesinambungan Perkhidmatan (PKP) • Garis Panduan Pengendalian Insiden ICT (UPM/ISMS/OPR/GP18/PENGENDALIAN INSIDEN)	**P**
		Sec : A.16.1.5 **Current Control :** • Pelan Kesinambungan Perkhidmatan (PKP) • ~~Prosedur Pengendalian Insiden ICT (UPM/ISMS/OPR/KES/P004)~~	Sec : A.16.1.5 **Current Control :** • Pelan Kesinambungan Perkhidmatan (PKP) • Garis Panduan Pengendalian Insiden ICT (UPM/ISMS/OPR/GP18/PENGENDALIAN INSIDEN)	**P**

		Sec : A.16.1.6 **Current Control :** • Pelan Kesinambungan Perkhidmatan (PKP) • ~~Prosedur Pengendalian Insiden ICT (UPM/ISMS/OPR/KES/P004)~~	Sec : A.16.1.6 **Current Control :** • Pelan Kesinambungan Perkhidmatan (PKP) • Garis Panduan Pengendalian Insiden ICT (UPM/ISMS/OPR/GP18/PENGENDALIAN INSIDEN)	**P**
		Sec : A.16.1.7 **Current Control :** • Pelan Kesinambungan Perkhidmatan (PKP) • ~~Prosedur Pengendalian Insiden ICT (UPM/ISMS/OPR/KES/P004)~~	Sec : A.16.1.7 **Current Control :** • Pelan Kesinambungan Perkhidmatan (PKP) • Garis Panduan Pengendalian Insiden ICT (UPM/ISMS/OPR/GP18/PENGENDALIAN INSIDEN)	**P**

LAMPIRAN 5

LAPORAN PENCAPAIAN OBJEKTIF SISTEM PENGURUSAN KESELAMATAN MAKLUMAT 2016

BIL.	OBJEKTIF	PETUNJUK PRESTASI	PENCAPAIAN	CATATAN
1.	Memastikan semakan penilaian risiko dan pelan pemulihan risiko dilaksanakan	sekurang-kurangnya sekali setahun	Semakan penilaian risiko dan pelan pemulihan risiko tahun 2016 telah dilaksanakan dan akan diluluskan pada 16 Jun 2016	
2.	Menjalankan ujian simulasi pelan pemulihan bencana ICT	sekurang-kurangnya 1 kali setahun;	Ujian simulasi pelan pemulihan bencana ICT telah dilaksanakan pada 3 Jun 2016	
3.	Memastikan sokongan ICT (rangkaian, sistem aplikasi dan pangkalan data) terhadap proses pendaftaran pelajar baharu bebas dari gangguan setiap semester;	95%	Pengukuran dilaksanakan pada sesi kemasukan 2016/2017	
4.	Memastikan pelajar yang berdaftar adalah pelajar yang mendapat tawaran; dan	100%	Pengukuran dilaksanakan pada sesi kemasukan 2016/2017	
5.	Memastikan borang permohonan kad pelajar yang diterima diisi dengan lengkap.	100%	Pengukuran dilaksanakan pada sesi kemasukan 2016/2017	

LAMPIRAN 6

MESYUARAT JAWATANKUASA KERJA KEDUA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
MS ISO/IEC/27001:2013

CADANGAN PINDAAN DOKUMEN (CPD)

1. TUJUAN

Kertas ini adalah untuk mendapat pengesahan dan kelulusan Mesyuarat Jawatankuasa Kerja Sistem Pengurusan Keselamatan Maklumat (ISMS) Universiti Putra Malaysia (UPM) berkaitan cadangan pindaan dokumen ISMS.

2. LATARBELAKANG

Dokumentasi ISMS telah dilaksanakan sejak dari mula pelaksanaan ISMS di Universiti Putra Malaysia (UPM) iaitu pada tahun 2012 dan sehingga kini proses penambahbaikan telah dibuat dari tahun ke tahun berdasarkan keperluan dan hasil penemuan audit.

3. LAPORAN

Semakan ke atas semua dokumen ISMS yang terlibat telah dilaksanakan dan terdapat beberapa cadangan pindaan dokumen telah diusulkan. Rujuk statistik perubahan dokumen di bawah:

Bil.	Kategori Dokumen ISO	Bilangan Dokumen Terlibat			Jumlah
		Pinda	Baru/tambah	Gugur	
1.	Prosedur	5	0	1	6
2.	Arahan Kerja	5	1	4	10
3.	Garis Panduan	19	1	0	20
4.	Borang	8	0	3	11
5.	Log	10	0	1	11
6.	Dokumen rujukan	1	0	0	1
Jumlah Keseluruhan		**48**	**2**	**9**	**59**

Perubahan menyeluruh kepada kod dokumen di mana kod dokumen diselaraskan sebagai langkah kepada penyatuan dokumen ISO.

Senarai penuh huraian pindaan boleh dirujuk pada Lampiran 1.

4. SYOR

Mesyuarat diminta untuk mengambil maklum dan membuat keputusan berkaitan Cadangan pindaan dokumen ISMS seperti yang dinyatakan pada Lampiran 1.

HURAIAN PINDAAN DOKUMEN ISO UPM

<table>
<tr><th rowspan="2">No. CPD</th><th rowspan="2">Pemilik Proses</th><th colspan="2">Huraian Pindaan Dokumen *</th><th rowspan="2"><u>Tambahan</u> (T) / ~~Pemotongan~~ (P)</th></tr>
<tr><th>Asal</th><th>Pindaan</th></tr>
<tr><td>ISMS (IDEC): 1/2016</td><td>iDEC</td><td>Nama Dokumen: PROSEDUR PERTUKARAN MAKLUMAT
Kod Dokumen:UPM/ISMS/SOK/P002
No. Isu:_01_, No. Semakan:_00_, Tarikh Kuatkuasa: 01/06/2012</td><td>Nama Dokumen: PROSEDUR PERTUKARAN MAKLUMAT
Kod Dokumen:UPM/ISMS/SOK/P002
No. Isu:_01_, No. Semakan:_01_, Tarikh Kuatkuasa: 01/07/2016</td><td></td></tr>
<tr><td></td><td></td><td>3.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>UPM/ISMS/ PGR/MP</td><td>Manual Sistem Pengurusan Keselamatan Maklumat</td></tr><tr><td>MS ISO/IEC 27001:~~2007~~</td><td>Information Technology – Security Techniques – Information Security Management Systems – Requirements</td></tr><tr><td>-</td><td>Arahan Keselamatan Kerajaan Malaysia</td></tr></table></td><td>4.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>UPM/ISMS/ PGR/MP</td><td>Manual Sistem Pengurusan Keselamatan Maklumat</td></tr><tr><td>MS ISO/IEC 27001:<u>2013</u></td><td>Information Technology – Security Techniques – Information Security Management Systems – Requirements</td></tr><tr><td>-</td><td>Arahan Keselamatan Kerajaan Malaysia</td></tr></table></td><td>P</td></tr>
<tr><td></td><td></td><td>4.0 TERMINOLOGI DAN SINGKATAN
PKD ISMS : Pegawai Kawalan Dokumen ISMS
Ketua Unit : Pegawai yang berhak untuk menyemak
PYB : Pegawai yang bertanggungjawab</td><td>5.0 TERMINOLOGI DAN SINGKATAN
PKD ISMS : Pegawai Kawalan Dokumen ISMS
Ketua <u>Bahagian/ Seksyen/</u>Unit : Pegawai yang berhak untuk menyemak
PYB : Pegawai yang bertanggungjawab</td><td>P/T</td></tr>
<tr><td></td><td></td><td>5.0 ~~TANGGUNGJAWAB~~</td><td>3.0 <u>TANGGUNGJAWAB</u></td><td>P</td></tr>
<tr><td></td><td></td><td>6.0 ~~CARTA ALIR~~
Rujuk lampiran 1</td><td>6.0 <u>PROSES TERPERINCI</u>
Rujuk lampiran 1</td><td>P</td></tr>
</table>

<table>
<tr><td></td><td>iDEC</td><td><s>8.0 REKOD ISMS</s></td><td>7.0 REKOD ISMS</td><td></td></tr>
<tr><td></td><td></td><td><s>9.0 SEJARAH SEMAKAN</s></td><td><u>8.0 SEJARAH SEMAKAN</u></td><td>P</td></tr>
<tr><td>ISMS (IDEC): 2/2016</td><td></td><td>Nama Dokumen: GARIS PANDUAN PENGENDALIAN MAKLUMAT
Kod Dokumen:UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT
No. Isu:_01_, No. Semakan:_00_, Tarikh Kuatkuasa: 30/11/2012</td><td>Nama Dokumen: GARIS PANDUAN PENGENDALIAN MAKLUMAT
Kod Dokumen:UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT
No. Isu:_01_, No. Semakan:_01_, Tarikh Kuatkuasa: 01/07/2016</td><td></td></tr>
<tr><td></td><td></td><td>3.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Arahan Keselamatan Kerajaan Malaysia</td></tr><tr><td>-</td><td><s>Garis Panduan Keselamatan Teknologi Maklumat & Komunikasi (GPKTMK)</s></td></tr></table></td><td>3.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Arahan Keselamatan Kerajaan Malaysia</td></tr><tr><td>-</td><td><s>Garis Panduan Keselamatan Teknologi Maklumat & Komunikasi (GPKTMK)</s></td></tr><tr><td><u>-</u></td><td><u>Panduan pengurusan Fail dan Rekod Universiti</u></td></tr></table></td><td>P</td></tr>
<tr><td>ISMS (IDEC): 3/2016</td><td>iDEC</td><td>Nama Dokumen: GARIS PANDUAN ENKRIPSI FAIL
Kod Dokumen:UPM/ISMS/SOK/GP04/ENKRIPSI
No. Isu:_01_, No. Semakan:_00_, Tarikh Kuatkuasa: 24/10/2014</td><td>Nama Dokumen: GARIS PANDUAN ENKRIPSI FAIL
Kod Dokumen:UPM/ISMS/SOK/GP04/ENKRIPSI
No. Isu:_01_, No. Semakan:_01_, Tarikh Kuatkuasa: 01/07/2016</td><td>p</td></tr>
<tr><td></td><td></td><td>4.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Kaedah-kaedah UPM (Teknologi Maklumat dan Komunikasi)</td></tr></table></td><td>4.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Kaedah-kaedah UPM (Teknologi Maklumat dan Komunikasi)</td></tr><tr><td>-</td><td><u>Garis Panduan Keselamatan Teknologi</u></td></tr></table></td><td>P</td></tr>
</table>

<table>
<tr><td></td><td></td><td><table><tr><td>-</td><td><s>Garis Panduan Teknologi Maklumat Komunikasi</s></td></tr></table></td><td><table><tr><td></td><td>Maklumat & Komunikasi (GPKTMK)</td></tr></table></td><td></td></tr>
<tr><td>ISMS (IDEC): 4/2016</td><td>iDEC</td><td>Nama Dokumen: GARIS PANDUAN KESELAMATAN PERALATAN MUDAH ALIH
Kod Dokumen:UPM/ISMS/SOK/GP05/PERALATAN MUDAH ALIH
No. Isu:_01_, No. Semakan:_00_, Tarikh Kuatkuasa: 24/10/2014</td><td>Nama Dokumen: GARIS PANDUAN KESELAMATAN PERALATAN MUDAH ALIH
Kod Dokumen:UPM/ISMS/SOK/GP05/PERALATAN MUDAH ALIH
No. Isu:_01_, No. Semakan:_01_, Tarikh Kuatkuasa: 01/07/2016</td><td></td></tr>
<tr><td></td><td></td><td>2.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Kaedah-kaedah UPM (Teknologi Maklumat dan Komunikasi)</td></tr><tr><td>-</td><td><s>Garis Panduan Teknologi Maklumat Komunikasi</s></td></tr></table></td><td>2.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Kaedah-kaedah UPM (Teknologi Maklumat dan Komunikasi)</td></tr><tr><td>-</td><td>Garis Panduan Keselamatan Teknologi Maklumat & Komunikasi (GPKTMK)</td></tr></table></td><td>P</td></tr>
<tr><td>ISMS (IDEC): 5/2016</td><td>iDEC</td><td>Nama Dokumen: GARIS PANDUAN PENGURUSAN IDENTITI
Kod Dokumen:UPM/ISMS/SOK/GP07/IDENTITI
No. Isu:_01_, No. Semakan:_00_, Tarikh Kuatkuasa: 05/06/2016</td><td>Nama Dokumen: GARIS PANDUAN PENGURUSAN IDENTITI
Kod Dokumen:UPM/ISMS/SOK/GP07/IDENTITI
No. Isu:_01_, No. Semakan:_01_, Tarikh Kuatkuasa: 01/07/2016</td><td></td></tr>
<tr><td></td><td></td><td>3.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Kaedah-kaedah UPM (Teknologi Maklumat dan Komunikasi)</td></tr><tr><td>-</td><td><s>Garis Panduan Teknologi Maklumat Komunikasi</s></td></tr></table></td><td>3.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Kaedah-kaedah UPM (Teknologi Maklumat dan Komunikasi)</td></tr><tr><td>-</td><td>Garis Panduan Keselamatan Teknologi Maklumat & Komunikasi (GPKTMK)</td></tr></table></td><td>`
P</td></tr>
</table>

		4.2 PENGESAHAN (*AUTHENTICATION*)	**4.2 PENGESAHAN (*AUTHENTICATION*)** viii. Aplikasi akan log keluar secara automatik sekiranyan tiada sebarang aktiviti atau tidak aktif selepas tempoh 15 minit (mengikut kesesuaian sistem).	
		4.3 KEIZINAN (*AUTHORIZATION*)	**4.3 KEIZINAN (*AUTHORIZATION*)** viii. ID pengguna dan kata laluan sistem aplikasi perlu ditarik balik serta merta sekiranya pengguna telah bertukar atau bersara.	
			4.4 PENGURUSAN ID BERPUSAT Pengurusan ID berpusat adalah perkhidmatan direktori pengenalan tunggal atau "*shared authentication database*" yang dibangunkan bagi mengatasi masalah berbilang id pengguna dan kata laluan. Semua sistem dan aplikasi UPM termasuk capaian ke rangkaian, emel akan menggunakan satu ID pengguna dan katalaluan yang sama. Perkhidmatan operasi ID berpusat merangkumi aspek berikut: i. Pendaftaran dan pengeluaran pelajar a. Rekod staf dan pelajar baharu perlu diaktifkan secara automatik ke dalam sistem ID berpusat. b. Penamatan dan penghapusan rekod staf dan pelajar perlu dilaksanakan dari sistem ID berpusat sekiranya telah tamat perkhidmatan/belajar atau tidak aktif. ii. Pengaktifan dan penjagaan kata laluan a. Pengaktifan dan penjagaan kata laluan dilaksanakan oleh pengguna sendiri tetapi dikawal selia oleh sistem ID berpusat. iii. *Single Sign On* (SSO) a. Membenarkan pengguna untuk log masuk ke sistem hanya menggunakan satu set ID pengguna dan kata laluan.	

<table>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>ISMS (IDEC): 6/2016</td><td>iDEC</td><td>Nama Dokumen: PROSEDUR PENGOPERASIAN PENGURUSAN PUSAT DATA
Kod Dokumen:UPM/ISMS/OPR/<s>DC</s>/P001
No. Isu:_01_, No. Semakan:_03_, Tarikh Kuatkuasa: 24/10/2014</td><td>Nama Dokumen: PROSEDUR PENGOPERASIAN PENGURUSAN PUSAT DATA
Kod Dokumen:UPM/ISMS/OPR/P001
No. Isu:_01_, No. Semakan:_04_, Tarikh Kuatkuasa: 01/07/2016</td><td></td></tr>
<tr><td></td><td></td><td>7.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Garis Panduan Keselamatan Teknologi Maklumat & Komunikasi (GPKTMK)</td></tr><tr><td>UPM/ISMS/OPR/<s>DC</s>/ GP01/ PENYELENGGARAAN OPERASI</td><td>Garis Panduan Penyelenggaraan Operasi Pusat Data</td></tr><tr><td>UPM/ISMS/OPR/<s>DC</s>/ GP02/PENYEDIAAN SERVER</td><td>Garis Panduan Penyediaan Server di Pusat Data</td></tr><tr><td>UPM/ISMS/OPR/<s>DC</s>/ GP03/KAWALAN AKSES</td><td>Garis Panduan Kawalan Akses ke Pusat Data</td></tr><tr><td>UPM/ISMS/SOK/GP05/PERALATAN MUDAH ALIH</td><td>Garis Panduan keselamatan peralatan mudah alih</td></tr><tr><td>UPM/ISMS/OPR/<s>PD</s>/ GP14/BACKUP</td><td>Garis Panduan Pengurusan Backup Pangkalan Data</td></tr></table></td><td>4.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Garis Panduan Keselamatan Teknologi Maklumat & Komunikasi (GPKTMK)</td></tr><tr><td>UPM/ISMS/OPR/GP01/ PENYELENGGARAAN OPERASI</td><td>Garis Panduan Penyelenggaraan Operasi Pusat Data</td></tr><tr><td>UPM/ISMS/OPR/GP02/ PENYEDIAAN SERVER</td><td>Garis Panduan Penyediaan Server di Pusat Data</td></tr><tr><td>UPM/ISMS/OPR/GP03/ KAWALAN AKSES</td><td>Garis Panduan Kawalan Akses ke Pusat Data</td></tr><tr><td>UPM/ISMS/SOK/GP05/ PERALATAN MUDAH ALIH</td><td>Garis Panduan keselamatan peralatan mudah alih</td></tr><tr><td>UPM/ISMS/OPR/GP14/ BACKUP</td><td>Garis Panduan Pengurusan Backup Pangkalan Data</td></tr></table></td><td>P</td></tr>
<tr><td></td><td></td><td>8.0 TERMINOLOGI/SINGKATAN
PYB : Pegawai yang bertanggungjawab
K(UDC) : Ketua <s>Unit</s> Pusat Data
TP (<s>BPI</s>) : Timbalan Pengarah <s>Bahagian</s></td><td>5.0 TERMINOLOGI DAN SINGKATAN
PYB : Pegawai yang bertanggungjawab
K(SDC) : Ketua Seksyen Pusat Data
TPPICT : Timbalan Pengarah Perkhidmatan ICT</td><td>P/T</td></tr>
</table>

		Perkhidmatan ~~Infrastruktur~~ ICT Pembekal : Pembekal sah yang dilantik oleh iDEC untuk kerja-kerja perkhidmatan dan penyelenggaraan BPI : Bahagian ~~Perkhidmatan~~ Infrastruktur ICT iDEC : Pusat Pembangunan Maklumat dan Komunikasi PTJ : Pusat Tanggungjawab ~~U~~DC : ~~Unit~~ Pusat Data	Pembekal : Pembekal sah yang dilantik oleh iDEC untuk kerja-kerja perkhidmatan dan penyelenggaraan BICT : Bahagian Infrastruktur ICT iDEC : Pusat Pembangunan Maklumat dan Komunikasi PTJ : Pusat Tanggungjawab SDC : Seksyen Pusat Data	
		9.0 ~~TANGGUNGJAWAB~~	**4.0 TANGGUNGJAWAB**	**P**
		10.0 ~~CARTA ALIR~~ Rujuk lampiran 2	**7.0 PROSES TERPERINCI** Rujuk lampiran 2	**P**
		~~8.0 REKOD ISMS~~	**7.0 REKOD ISMS**	**P**
		~~9.0 SEJARAH SEMAKAN~~	**8.0 SEJARAH SEMAKAN**	**P**
ISMS (IDEC): 7/2016	**iDEC**	Nama Dokumen: PROSEDUR PEMANTAUAN OPERASI PUSAT DATA Kod Dokumen:UPM/ISMS/OPR/~~DC~~/P002 No. Isu:_01_, No. Semakan:_01_, Tarikh Kuatkuasa: 24/10/2014	Nama Dokumen: PROSEDUR PEMANTAUAN OPERASI PUSAT DATA Kod Dokumen:UPM/ISMS/OPR/P002 No. Isu:_01_, No. Semakan:_02_, Tarikh Kuatkuasa: 01/07/2016	
		3.0 DOKUMEN RUJUKAN	**4.0 DOKUMEN RUJUKAN**	**P**

Kod Dokumen	Tajuk Dokumen
-	Garis Panduan Keselamatan Teknologi Maklumat & Komunikasi (GPKTMK)
UPM/ISMS/OPR/~~DC~~/ GP05/	Garis Panduan Pemantauan Operasi Pusat Data

Kod Dokumen	Tajuk Dokumen
-	Garis Panduan Keselamatan Teknologi Maklumat & Komunikasi (GPKTMK)
UPM/ISMS/OPR/GP05/PEMANTAUAN	Garis Panduan Pemantauan Operasi Pusat Data

		PEMANTAUAN OPERASI UPM/ISMS/OPR/~~DC~~/GP08/MAKLUMAT LOG — Garis Panduan Perlindungan Maklumat Log Server	OPERASI UPM/ISMS/OPRGP08/MAKLUMAT LOG — Garis Panduan Perlindungan Maklumat Log Server	
		4.0 TERMINOLOGI/SINGKATAN PYB : Pegawai yang bertanggungjawab K(UDC) : Ketua ~~Unit~~ Pusat Data TP (~~BPI~~) : Timbalan Pengarah ~~Bahagian~~ Perkhidmatan ~~Infrastruktur~~ ICT iDEC : Pusat Pembangunan Maklumat dan Komunikasi PTJ : Pusat Tanggungjawab	**5.0 TERMINOLOGI DAN SINGKATAN** PYB : Pegawai yang bertanggungjawab K(SDC) : Ketua Seksyen Pusat Data TPPICT : Timbalan Pengarah Perkhidmatan ICT iDEC : Pusat Pembangunan Maklumat dan Komunikasi PTJ : Pusat Tanggungjawab	**P/T**
		5.0 ~~TANGGUNGJAWAB~~	**3.0 TANGGUNGJAWAB**	**P**
		6.0 ~~CARTA ALIR~~ Rujuk lampiran 3	**6.0 PROSES TERPERINCI** Rujuk lampiran 3	**P**
		~~8.0 REKOD ISMS~~	**7.0 REKOD ISMS**	**P**
		~~9.0 SEJARAH SEMAKAN~~	**8.0 SEJARAH SEMAKAN**	**P**
ISMS (IDEC): 8/2016	**iDEC**	Nama Dokumen: PROSEDUR KAWALAN DAN PEMANTAUAN CAPAIAN KE SISTEM SI PUSAT DATA Kod Dokumen:UPM/ISMS/OPR/~~DC~~/P003 No. Isu:_01_, No. Semakan:_02_, Tarikh Kuatkuasa: 24/10/2014	Nama Dokumen: PROSEDUR KAWALAN DAN PEMANTAUAN CAPAIAN KE SISTEM SI PUSAT DATA Kod Dokumen:UPM/ISMS/OPR/P003 No. Isu:_01_, No. Semakan:_03_, Tarikh Kuatkuasa: 01/07/2016	
		3.0 DOKUMEN RUJUKAN **Kod Dokumen** — **Tajuk Dokumen** - — Garis Panduan Keselamatan Teknologi Maklumat & Komunikasi (GPKTMK)	**4.0 DOKUMEN RUJUKAN** **Kod Dokumen** — **Tajuk Dokumen** - — Garis Panduan Keselamatan Teknologi Maklumat & Komunikasi (GPKTMK)	**P**

		UPM/SOK/ICT/P001 — Garis Panduan Penyelenggaraan ICT UPM/ISMS/OPR/~~DC~~/GP06/PEMANTAUAN CAPAIAN — Garis Panduan Pemantauan Capaian ke Sistem di Pusat Data	UPM/OPR/IDEC/P003 — Garis Panduan Penyelenggaraan ICT UPM/ISMS/OPR/GP06/PEMANTAUAN CAPAIAN — Garis Panduan Pemantauan Capaian ke Sistem di Pusat Data	
		4.0 TERMINOLOGI/SINGKATAN PYB : Pegawai yang bertanggungjawab K(UDC) : Ketua ~~Unit~~ Pusat Data TP (~~BPI~~) : Timbalan Pengarah ~~Bahagian~~ Perkhidmatan ~~Infrastruktur~~ ICT iDEC : Pusat Pembangunan Maklumat dan Komunikasi PTJ : Pusat Tanggungjawab	**5.0 TERMINOLOGI DAN SINGKATAN** PYB : Pegawai yang bertanggungjawab K(SDC) : Ketua Seksyen Pusat Data TPPICT : Timbalan Pengarah Perkhidmatan ICT iDEC : Pusat Pembangunan Maklumat dan Komunikasi PTJ : Pusat Tanggungjawab	**P/T**
		5.0 ~~TANGGUNGJAWAB~~	**3.0 TANGGUNGJAWAB**	**P**
		6.0 ~~CARTA ALIR~~ Rujuk lampiran 4	**6.0 PROSES TERPERINCI** Rujuk lampiran 4	**P**
		~~8.0 REKOD ISMS~~	**7.0 REKOD ISMS**	**P**
ISMS (IDEC): 9/ 2016	**iDEC**	Nama Dokumen: PROSEDUR PELAN TINDAK BALAS INSIDEN ICT Kod Dokumen:UPM/ISMS/SOK/P001 No. Isu:_01_, No. Semakan:_00_, Tarikh Kuatkuasa: 30/11/2012	Nama Dokumen: PROSEDUR PELAN TINDAK BALAS INSIDEN ICT Kod Dokumen:UPM/ISMS/SOK/P001 No. Isu:_01_, No. Semakan:_01_, Tarikh Kuatkuasa: 01/07/2016	
		4.0 DOKUMEN RUJUKAN **Kod Dokumen** — **Tajuk Dokumen** UPM/ISMS/OPR/~~KES~~/P004 — Prosedur Pengendalian Insiden Bilangan 4 Tahun 2006 — Surat Pekeliling Am Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan	**4.0 DOKUMEN RUJUKAN** **Kod Dokumen** — **Tajuk Dokumen** UPM/ISMS/OPR/GP18/PENGENDALIAN INSIDEN — Garis Panduan Pengendalian Insiden DRP-ICT UPM (3.0) — PELAN PEMULIHAN BENCANA ICT UPM	**P/T**

<table>
<tr>
<td></td>
<td></td>
<td>
<table>
<tr><td></td><td>Komunikasi Sektor Awam.</td></tr>
<tr><td>Bilangan 1 Tahun 2001</td><td>Pekeliling Am Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi</td></tr>
</table>
</td>
<td>
<table>
<tr><td>Bilangan 4 Tahun 2006</td><td>Surat Pekeliling Am Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.</td></tr>
<tr><td>Bilangan 1 Tahun 2001</td><td>Pekeliling Am Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi</td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>
6.0 PELAN TINDAK BALAS INSIDEN KESELAMATAN ICT
<table>
<tr><th>Proses</th><th>Aktiviti</th><th>Masa</th><th>Tindakan</th></tr>
<tr><td>Pembaikan</td><td>c. Tindakan pemulihan ke atas bencana berkaitan ICT hendaklah merujuk kepada manual:
~~- DRP Data Center~~
~~- DRP Sistem Sumber Manusia~~
~~- DRP Sistem Kewangan~~
~~- DRP Laman Web~~
~~- DRP Sistem Maklumat Pelajar~~</td><td>Mengikut masa yang ditetapkan</td><td>Pentadbir Sistem

Pentadbir Sistem

Pengarah iDEC</td></tr>
<tr><td>Pemantauan</td><td>d.Menyediakan laporan insiden dan makluman kepada ~~Pengurusan Universiti~~</td><td></td><td></td></tr>
</table>
</td>
<td>
6.0 PELAN TINDAK BALAS INSIDEN KESELAMATAN ICT
<table>
<tr><th>Proses</th><th>Aktiviti</th><th>Masa</th><th>Tindakan</th></tr>
<tr><td>Pembaikan</td><td>c. Tindakan pemulihan ke atas bencana berkaitan ICT hendaklah merujuk kepada manual:
- Pelan Pemulihan Bencana ICT UPM</td><td>Mengikut masa yang ditetapkan</td><td>Pentadbir Sistem

Pentadbir Sistem

Pengarah iDEC</td></tr>
<tr><td>Pemantauan</td><td>d.Menyediakan laporan insiden dan makluman kepada Jawatankuasa Keselamatan Teknologi Maklumat dan Komunikasi UPM</td><td></td><td></td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td>ISMS (IDEC): 10/ 2016</td>
<td>iDEC</td>
<td>Nama Dokumen: GARIS PANDUAN PENILAIAN RISIKO ASET
Kod Dokumen:UPM/ISMS/SOK/GP02/RISK ASSESSMENT
No. Isu:_01_, No. Semakan:_04_, Tarikh Kuatkuasa: 05/06/2015</td>
<td>Nama Dokumen: GARIS PANDUAN PENILAIAN RISIKO ASET
Kod Dokumen:UPM/ISMS/SOK/GP02/RISK ASSESSMENT
No. Isu:_01_, No. Semakan:_05_, Tarikh Kuatkuasa: 01/07/2016</td>
<td></td>
</tr>
</table>

<table>
<tr>
<td></td>
<td></td>
<td>1.TUJUAN
Garis panduan ini disediakan untuk menilai tahap risiko ~~aset ICT~~ supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan pelindungan dan kawalan ke atas aset ICT UPM.</td>
<td>1. TUJUAN
Garis panduan ini disediakan untuk menilai tahap risiko keselamatan maklumat ~~a~~supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas keselamatan maklumat UPM.</td>
<td>P/T</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.DEFINISI
<table>
<tr><th>Bil.</th><th>Terma</th><th>Deskripsi</th></tr>
<tr><td>1</td><td>Aset</td><td>Sesuatu yang bernilai yang boleh menyebabkan kerugian sekiranya hilang atau berubah. Berdasarkan MyRAM aset-aset tergolong kepada data/maklumat, perkhidmatan, perisian, perkakasan dan manusia. ~~Sila rujuk seksyen 8, Deskripsi langkah-langkah penilaian risiko: Pengenalpastian Aset (StepS3) untuk maklumat lanjut.~~</td></tr>
<tr><td>2</td><td>Aset Yang bersandar</td><td>Subjek yang dinyatakan ketika kejadian sesuatu peristiwa. Bermakna aset lain diperlukan untuknya berfungsi. ~~Sila rujuk seksyen 8, Deskripsi langkah-langkah penilaian risiko: Penilaian asset-aset dan penentuan kebergantungan antara asset-aset (Step S4)) untuk maklumat lanjut.~~</td></tr>
<tr><td>3</td><td>~~Pentadbir Proses (Owner)~~</td><td>Pentadbir Proses ~~juga sebagai pemilik risiko yang ebrtanggung terhadap risiko untuk sesuatu asset atau proses.~~</td></tr>
<tr><td>4</td><td>~~Pentadbir Sistem (Custodian)~~</td><td>Kakitangan Teknikal ICT yang memelihara keselamatan, menyelenggara, atau mengawal sesuatu aset.</td></tr>
<tr><td>5</td><td>Risiko</td><td>Secara umum ia adalah kemungkinan berhadapan dengan bahaya atau menyebabkan mudarat atau kerugian, terutamanya dari kurang penjagaan yang sesuai.</td></tr>
</table></td>
<td>3. DEFINISI
<table>
<tr><th>Bil.</th><th>Terma</th><th>Deskripsi</th></tr>
<tr><td>1</td><td>Aset</td><td>Sesuatu yang bernilai yang boleh menyebabkan kerugian sekiranya hilang atau berubah. Berdasarkan MyRAM aset-aset tergolong kepada data/maklumat, perkhidmatan, perisian, perkakasan dan manusia.</td></tr>
<tr><td>2</td><td>Aset Yang bersandar</td><td>Subjek yang dinyatakan ketika kejadian sesuatu peristiwa. Bermakna aset lain diperlukan untuknya berfungsi</td></tr>
<tr><td>3</td><td>Owner/Pentadbir Proses /Pemilik Risiko</td><td>Pentadbir Proses yang bertanggungjawab terhadap risiko untuk sesuatu aset atau proses.</td></tr>
<tr><td>4</td><td>Custodian/ Pentadbir Sistem</td><td>Kakitangan Teknikal ICT yang memelihara keselamatan, menyelenggara, atau mengawal sesuatu aset.</td></tr>
<tr><td>5</td><td>Risiko</td><td>Secara umum ia adalah kemungkinan berhadapan dengan bahaya atau menyebabkan mudarat atau kerugian, terutamanya dari kurang penjagaan yang sesuai.</td></tr>
<tr><td>6</td><td>Penilaian Risiko</td><td>Penilaian bagi kemungkinan-kemungkinan bahaya atau mudarat atau kerugian/kehilangan aset</td></tr>
<tr><td>7</td><td>Ancaman</td><td>sebarang kejadian atau perbuatan yang boleh menyebabkan satu atau lebih daripada perkara berikut berlaku:</td></tr>
</table></td>
<td>P/T</td>
</tr>
</table>

		6	Penilaian Risiko	Penilaian bagi kemungkinan-kemungkinan bahaya atau mudarat atau kerugian/kehilangan aset			
		7	*Ancaman*	~~Mengenalpasti potensi~~ sebarang kejadian atau perbuatan yang boleh menyebabkan satu atau lebih daripada perkara berikut berlaku: pendedahan yang tidak diluluskan, kemusnahan, penyingkiran, pengubahsuaian atau gangguan maklumat sensitive atau kritikal, asset-aset atau perkhidmatan. Sesuatu ancaman boleh berlaku dengan semulajadi, sengaja atau tidak sengaja.			
							pendedahan yang tidak diluluskan, kemusnahan, penyingkiran, pengubahsuaian atau gangguan maklumat sensitif atau kritikal, aset-aset atau perkhidmatan. Sesuatu ancaman boleh berlaku dengan semula jadi, sengaja atau tidak sengaja.	
		5.0 METODOLOGI PENILAIAN RISIKO ASET ICT ~~Semua agensi Kerajaan tertakluk untuk melaksanakan penilaian risiko aset ICT 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.~~ ~~Sepuluh (11) langkah utama dalam MyRAM adalah seperti berikut:~~ ~~1. Menubuhkan pasukan penilaian risiko~~ ~~2. Menetapkan sempadan aset~~ ~~3. Mengenal pasti Aset~~ ~~4. Mengenal pasti Pentadbir Proses dan Pentadbir Sistem;~~ ~~5. Menilai Aset~~ ~~6. Menilai Ancaman~~ ~~7. Menilai Kelemahan~~ ~~8. Mengenal pasti Kawalan~~ ~~9. Menganalisa Impak~~ ~~10. Menganalisa Kemungkinan~~ ~~11. Pengiraan Risiko~~ ~~Agensi hendaklah melaksanakan penilaian risiko berasaskan 10 langkah utama seperti di atas. Setiap~~		**5.0 METODOLOGI PENILAIAN RISIKO ASET ICT** Penilaian risiko ialah satu kaedah untuk menentukan apakah ancaman-ancaman yang wujud untuk sesuatu aset dan tahap risiko yang berkaitan dengan ancaman tersebut. Penentuan tahap risiko menyediakan organisasi dengan maklumat yang diperlukan untuk memilih perlindungan-perlindungan dan langkah kawalan yang bersesuaian untuk mengurangkan risiko kepada satu tahap yang boleh diterima. MAMPU telah membangunkan Malaysian Public Sector Information Security Risk Assessment Methodology atau MyRAM bagi membantu organisasi sektor awam dalam mengenalpasti dan menguruskan risiko keselamatan Maklumat. MAMPU akan menggunakan MyRAM untuk memastikan kesahihan maklumat dan aset Kerajaan dalam menyediakan perkhidmatan yang efektif dan efisien bagi semua pelanggan. Kami juga telah mengambil ISO/IEC 27005 sebagai contoh. **5.1 Kriteria Penilaian Risiko**: Kriteria bagi penilaian risiko UPM adalah seperti berikut: i. Semua risiko yang dinilaikan sebagai taraf "RENDAH" akan dianggap Sebagai boleh diterima kepada pengurusan.	**P/T**

		~~langkah MyRAM saling bergantungan dengan menghasilkan satu atau lebih dokumen yang merupakan input kepada satu atau lebih langkah utama MyRAM.~~ ~~Sebarang pengemaskinian terhadap maklumat aset di dalam sistem MyRAM dilaksanakan apabila berlaku perubahan atau penambahan aset di dalam skop ISMS yang terlibat.~~	ii. Risiko-risiko yang tidak menjejaskan Visi, Misi and Nilai-nilai UPM mungkin boleh dipertimbangkan untuk penerimaan. iii. Risiko-risiko yang tidak mempunyai impak ke atas reputasi, penjenamaan dan imej UPM mungkin boleh dipertimbangkan untuk penerimaan. iv. Risiko-risiko yang tidak mempunyai impak ke atas pematuhan perundangan mungkin boleh dipertimbangkan untuk penerimaan. v. Risiko-risiko yang mempunyai sedikit impak atau tiada kepada pengguna akhir, mungkin boleh dipertimbangkan untuk penerimaan.	
		~~**6.0 CADANGAN PERINGKAT TINGGI**~~ ~~Keputusan bagaimana untuk mengendalikan risiko dan atribut yang perlu dipertimbangkan sebelum membuat keputusan dianalisis dan ditentukan. Cadangan peringkat tinggi akan dibentangkan oleh pasukan penilaian risiko kepada pihak pengurusan dalam laporan yang dijana oleh MYRAM.~~	**6.0 KEPERLUAN UNTUK PENILAIAN RISIKO** Penilaian risiko akan dilakukan untuk: i. Mengambilkira perubahan pada struktur organisasi dan aset baru; ii. Mempertimbangkan ancaman baru dan kelemahan; dan iii. Mengesahkan bahawa kawalan tetap efektif dan bersesuaian. iv. Mengesahkan risiko yang masih ada setelah kawalan untuk rawatan risiko dilaksanakan; v. Mengesahkan kriteria penilaian risiko oleh pihak pengurusan atasan.	**P/T**
		~~**7.0 KEPUTUSAN MENGENAI PILIHAN**~~ ~~Pada "Keputusan Pilihan", pasukan Risk Assessment akan mencadangkan kepada pihak pengurusan sama ada untuk menerima, mengurangkan, memindahkan, atau mengelakkan tahap risiko ancaman tertentu yang wujud di dalam aset tertentu. Penerangan bagi setiap pilihan keputusan adalah seperti berikut:~~	**7.0 PROSES PENILAIAN RISIKO** Pendekatan yang diambil adalah mengikut garis panduan proses penilaian risiko dalam dokumen MyRAM, bermula dari langkah Penubuhan Ahli Kumpulan sehingga Langkah 10, yang merupakan Pengiraan Risiko. Langkah-langkah ini berkaitan antara satu sama lain kerana input untuk satu aktiviti penilaian risiko boleh diambil daripada output langkah- langkah terdahulu. Jadual 1 dibawah, menunjukkan sepuluh (10) langkah latihan penilaian risiko.	**P/T**
		8.0	**8.0 PERANAN DAN TANGGUNGJAWAB AHLI KUMPULAN PENILAIAN RISIKO** i. Memberi nasihat kepakaran untuk aktiviti penilaian risiko ii. Mengurus aktiviti penilaian risiko	**T**

			iii. Memastikan selesai tepat pada masa; dan iv. Melakukan semakan semula untuk semua output dan dokumen sebelum dibentangkan kepada penasihat projek v. Sentiasa menentukan progres kerja; vi. Menilai keputusan-keputusan, jurang dan memberi maklum balas; dan vii. Melakukan semua tugasan yang disebut dalam langkah-langkah penilaian risiko	
		9.0	**9.0 TARAF NILAI ASET** Berdasarkan Jadual 1 dibawah, kumpulan penilaian risiko perlu mewujudkan taraf nilai untuk keperluan Keselamatan Maklumat, iaitu Kerahsiaan/*Confidentiality* (C), Kesahihan/*Integrity* (I) dan Ketersediaan/*Availability* (A). Tahap-tahap *Low* (Rendah), *Medium* (Pertengahan)dan *High* (Tinggi) di Jadual 1 adalah berpandukan huraian yang diberi mengikut setiap skor. Dalam menilai sensitiviti setiap aset, Pasukan Penilaian Risiko akan menggunakan garis-garis panduan berikut: a) **Kerahsiaan (*Confidentiality*)** Kesan pendedahan maklumat rahsia/sulit yang tidak diluluskan boleh mengakibatkan kehilangan keyakinan pemegang saham dan mengaibkan. b) **Kesahihan (*Integrity*)** Kesan kepada sistem yang disebabkan dari pengubahsuaian aset secara sengaja, tanpa mendapat kelulusan atau tidak sengaja. c) **Ketersediaan (*Availability*)** Ini ialah kesan daripada penafian pengunaan aset secara sengaja atau kebetulan. Setiap aset mesti dinilai menurut tahap Confidentiality (Rahsia), Integrity (Kesahihan) dan Availability (Ketersediaan) masing-masing. **9.1 Kaedah Skor Untuk Risiko**	**T** **T**

			Menggunakan Jadual 1 di bawah, selepas mengira nilai-nilai CIA dan nilai aset, sekarang kita perlu menghitung tahap risiko yang terdedah kepada aset-aset tersebut. Risiko-risiko wujud disebabkan kewujudan **Ancaman** kepada aset dan **Kelemahan** aset-aset itu sendiri 9.2 **Kebarangkalian & Impak** Dalam persekitaran sebenar, risiko yang dikenalpasti berdasarkan ancaman-ancaman dan kelemahan-kelemahan mungkin boleh berlaku atau tidak. Kemungkinan "peluang" risiko terjadi boleh bergantung kepada situasi. Oleh itu penilaian risiko adalah berdasarkan kepada "KebarangkalianTerjadi" dan "Impak" disebabkan sesuatu kejadian. Impak diukur kepada aset secara langsung, begitu juga impak kepada bisnes. Kebarangkalian dan Impak boleh dipilih berdasarkan Jadual 1 di bawah dan ditarafkan dari 3-1 berdasarkan huraian dalam Jadual.	
		10.0	**10.0 GARIS PANDUAN UNTUK KEPUTUSAN BAGI RISIKO YANG DIKENALPASTI** Output proses penilaian risiko adalah input bagi proses membuat keputusan yang menetapkan sama ada menerima, mengurangkan, memindahkan atau mengelakkan risiko yang sudah dikenalpasti. Ini akan dilakukan dalam Selection of Controls (Pemilihan Kawalan) dan ditunjukkan dalam Risk Treatment Plan (RTP) (Pelan Rawatan Risiko). Pasukan Penilaian Risiko akan menubuhkan High-Level-Recommendation untuk memperoleh kelulusan bertulis atau pengakuan daripada Jawatankuasa Kerja ISMS yang akan menentukan di dalam RTP apa yang mesti dilakukan selepas mendapat tahap risiko untuk semua aset-aset yang dikenalpasti. Di peringkat ini, keputusan sama ada menerima, mengurangkan, memindahkan, atau mengelakkan risiko yang telah kenalpasti mestilah dibuat hanya setelah latihan penilaian risiko selesai. Perlu mendapat pengesahan muktamad Timbalan Wakil Pengurusan ISMS. Secara asasnya membuat keputusan sama ada menerima, mengurangkan, memindahkan, atau mengelakkan tahap risiko adalah berdasarkan faktor-faktor masa, wang, tenaga kerja	**T**

			dan peralatan. Ketentuan pilihan untuk mengendali risiko boleh dilakukan dengan mengikuti langkah-langkah dalam Rajah 2 di bawah. Seperti yang digambarkan dalam Rajah 2 di atas, langkah pertama untuk membuat cadangan-cadangan High-Level ialah dengan mendapatkan keputusan tahap risiko-risiko dari Langkah 10. Kemudian tentukan apakah tahap risiko yang boleh diterima oleh Pasukan Penilaian Risiko. Rujuk Seksyen 4: Kriteria untuk menerima Risiko-risiko. Untuk Cadangan High-Level, terdapat dua (2) output iaitu: a) Keputusan atas pilihan; dan b) Strategi Perlindungan 10.1 **Keputusan atas Pilihan** Dalam Keputusan atas Pilihan, Kumpulan Penilaian Risiko akan mencadangkan kepada JawatanKuas Kerja ISMS sama ada untuk menerima, mengurangkan, memindahkan, atau mengelak tahap risiko ancaman yang wujud dalam sesuatu aset. Huraian-huraian untuk setiap pilihan keputusan ialah seperti berikut: a. **Menerima**: untuk menerima risiko-risiko berkaitan dengan aset-aset tanpa melaksanakan sebarang perlindungan atau kawalan b. **Mengurangkan**: melaksanakan kawalan untuk mengurangkan risiko. Mengurangkan tahap risiko adalah perlu apabila risiko tinggi. c. **Pemindahan**: Memindahkan risiko kepada entiti yang lain. d. **Mengelakkan**: untuk mengelak risiko-risiko apabila tiada pilihan lain. Pasukan Penilaian Risiko akan menerima, mengurangkan, memindahkan atau mengelakkan	

			risiko bagi kriteria berikut: a. Memeriksa dan menilai sama ada risiko dapat diterima atau tidak. Kumpulan Penilaian Risiko boleh mencadangkan kepada pengurusan untuk menerima semua aset dengan tahap risiko Low (Rendah) dan tiada tindakan serta-merta diambil bagi melindungi aset; dan b. Jika risiko-risiko tidak boleh diterima, maka semak dan nilaikan sama ada ianya patut dikurangkan, dipindahkan atau dielakkan; c. Jika implikasi risiko-risiko membawa kepada bencana dan kritikal (High), risiko-risiko tersebut patut dikurangkan. Pengurangan Risiko akan dicapai melalui pelaksanaan komponen-komponen berikut: operasi, prosedur, fizikal, Kakitangan dan keselamatan teknikal untuk memastikan bahawa operasi kritikal tidak terjejas. dan d. Jika implikasi risiko-risiko adalah sederhana kritikal (Medium), risiko-risiko tersebut boleh juga dipindahkan berdasarkan syarat-syarat berikut. i. Risiko-risiko mesti dipindahkan dengan adil. Risiko boleh dikongsi oleh pemilik-pemilik aset dan pihak ketiga. Misalnya, talian komunikasi bermasalah, dan Service Level Agreement (SLA) dengan penyedia talian menyatakan bahawa talian boleh didapati dalam 24 jam; bencana yang tidak dapat diketahui yang mungkin dialami pihak ketiga merupakan satu risiko yang dikongsi bersama dimana agensi bersediauntuk terima; dan ii. Risiko-risiko sepatutnya dielakkan sama sekali sekiranya tiada	

			kawalan munasabah yang boleh dilaksanakan untuk mengurangkan risiko. Contoh, mengelak risiko-risiko ialah dengan memutuskan sistem. Pasukan Penilaian Risiko perlu membangunkan pelan perlindungan "*Risk Treatment Plan*" untuk dibentangkan kepada pengurusan. Bagi *Risk Treatment Plan,* kumpulan Penilaian Risiko perlu melihat samada kawalan yang sedia ada adalah cukup untuk melindungi aset-aset atau tidak. Jika kawalan yang sedia ada tidak mencukupi, kumpulan yang terbabit atau kumpulan pemilik risiko akan memilih objektif-objektif kawalan sesuai dan kawalan boleh didapati dalam *Annex A, ISO / IEC 27001:2005 ISMS Requirements*. Ini boleh didapati dalam *Statement of Applicability* atau Dokumen SOA.	
		11.0	**11.0 KELULUSAN PENGURUSAN** a) Dokumen yang dibentangkan kepada Jawatankuasa Kerja ISMS untuk kelulusan maklumat analisis risiko mempunyai perkara-perkara berikut: b) Sebarang syarat dan konsep-konsep yang baru atau berbeza – misalnya, aset-aset, ancaman-ancaman, risiko dan profil risiko - perlu dijelaskan. c) Maklumat ancaman, risiko dan kelemahan untuk setiap asset kritikal; d) Komposit, analisa keputusan-keputusan analisis risiko. Maklumat tersebut perlu dikemukakan dalam bentuk jadual atau grafik yang mudah dibaca. Implikasi mesti turut dijelaskan pada setiap tahap risiko yang sudah dikenal pasti; e) Amalan-amalan strategi perlindungan dan kelemahan-kelemahan organisasi dikumpulkan mengikut bidang amalan;	**T**

			dan f) Justifikasi untuk rancangan pelindungan g) Pengurusan tertinggi telah memutuskan bahawa semua risiko berbaki (risiko yang tinggal selepas menggunakan kawalan yang sesuai) hendaklah disifatkan sebagai 'Diterima' oleh pihak pengurusan.	
ISMS (IDEC): 11/ 2016	**iDEC**	Nama Dokumen: ARAHAN KERJA PENGURUSAN DNS Kod Dokumen:UPM/ISMS/OPR/~~DC~~/AK08 No. Isu:_01_, No. Semakan:_00_, Tarikh Kuatkuasa: 24/10/2014	Nama Dokumen: ARAHAN KERJA PENGURUSAN DNS Kod Dokumen:UPM/ISMS/OPR/AK08 No. Isu:_01_, No. Semakan:_01_, Tarikh Kuatkuasa: 01/07/2016	**P**
		3.0 ARAHAN KERJA ARAHAN TERPERINCI Terima permohonan DNS melalui Borang ~~Sokongan Perkhidmatan ICT (OPR/UDC/SOK/BR03)~~ Wujudkan atau kemaskini DNS menggunakan langkah-langkah berikut: 1. Gunakan SSH untuk akses ke server DNS1 / DNS2. 2. Login ID dan Password. 3. Pastikan anda berada dalam folder /opt/named 4. Taip command untuk semak dns atau IP address grep -/ <dns / ip address> 5. Edit guna vi untuk tambah atau kemaskini DNS dan ip address 6. vi upm.edu.my.zone 7. <hostname/dns> IN A IP ADDRESS alias IN A CNAME <hostname/dns>. <hostname/dns> IN A MX 0 <IP ADDRESS> 8. Tambah nombor terakhir pada serial number (Contoh 100 kepada 101) dan save file. 9. Refresh zone file dengan menaip command %rndc reload upm.edu.my.zone	**3.0 ARAHAN KERJA** ARAHAN TERPERINCI Terima permohonan DNS melalui Borang Permohonan Perkhidmatan Sokongan ICT (OPR/IDEC/BR03/SOKONGAN ICT) Wujudkan atau kemaskini DNS menggunakan langkah-langkah berikut: 1. Gunakan SSH untuk akses ke server DNS1 / DNS2. 2. Login ID dan Password. 3. Pastikan anda berada dalam folder /opt/named 4. Taip command untuk semak dns atau IP address grep -/ <dns / ip address> 5. Edit guna vi untuk tambah atau kemaskini DNS dan ip address 6. vi upm.edu.my.zone 7. <hostname/dns> IN A IP ADDRESS alias IN A CNAME <hostname/dns>. <hostname/dns> IN A MX 0 <IP ADDRESS> 8. Tambah nombor terakhir pada serial number (Contoh 100 kepada 101) dan save file. 9. Refresh zone file dengan menaip command %rndc reload upm.edu.my.zone	**P**

		Maklumkan DNS telah diwujudkan atau dikemaskini kepada pemohon melalui emel.	Maklumkan DNS telah diwujudkan atau dikemaskini kepada pemohon melalui emel.	
ISMS (IDEC): 12/ 2016	**iDEC**	Nama Dokumen: ARAHAN KERJA PENGURUSAN VIRTUAL HOST Kod Dokumen:UPM/ISMS/OPR/~~DC~~/AK09 No. Isu:_01_, No. Semakan:_00_, Tarikh Kuatkuasa: 24/10/2014	Nama Dokumen: ARAHAN KERJA PENGURUSAN VIRTUAL HOST Kod Dokumen:UPM/ISMS/OPR/AK09 No. Isu:_01_, No. Semakan:_01_, Tarikh Kuatkuasa: 01/07/2016	**P**
		3.0 ARAHAN KERJA ARAHAN TERPERINCI Terima permohonan DNS melalui Borang ~~Sokongan Perkhidmatan ICT (OPR/UDC/SOK/BR03)~~ Pastikan DNS / Hostname telah diwujudkan didalam server DNS1 atau DNS dengan capaian (luar/dalam UPM). Wujudkan Virtual Host : 1. Gunakan SSH untuk akses ke server webptj/webpstn/webkolej/webptj2. 2. Wujudkan ID dan Password 3. Untuk sistem Operasi Centos / RHELL, edit /tc/httpd/conf/httpd.conf 4. Untuk Sistem Operasi Ubuntu. Pastikan anda berada dalam folder /etc/apache2/sites-available dan copy file dengan menggunakan cp example.com.conf test.com.conf 5. Edit file test.com.conf menggunakan command vi /etc/apache2/sites-available/test.com.conf <VirtualHost *:so> ServerAdmin admin@test.com ServerName test.com ServerAlias www.test.com DocumentRoot /var/www/test.com/public_html ErrorLog ${APACHE_LOG_DIR}/error.log CustomLog &{APACHE_LOG_DIR}/access.log	**3.0 ARAHAN KERJA** ARAHAN TERPERINCI Terima permohonan Virtual Host melalui Borang Permohonan Perkhidmatan Sokongan ICT (OPR/IDEC/BR03/SOKONGAN ICT) Pastikan DNS / Hostname telah diwujudkan didalam server DNS1 atau DNS dengan capaian (luar/dalam UPM). Wujudkan Virtual Host : 1. Gunakan SSH untuk akses ke server webptj/webpstn/webkolej/webptj2. 2. Wujudkan ID dan Password 3. Untuk sistem Operasi Centos / RHELL, edit /tc/httpd/conf/httpd.conf 4. Untuk Sistem Operasi Ubuntu. Pastikan anda berada dalam folder /etc/apache2/sites-available dan copy file dengan menggunakan cp example.com.conf test.com.conf 5. Edit file test.com.conf menggunakan command vi /etc/apache2/sites-available/test.com.conf <VirtualHost *:so> ServerAdmin admin@test.com ServerName test.com ServerAlias www.test.com DocumentRoot /var/www/test.com/public_html ErrorLog ${APACHE_LOG_DIR}/error.log CustomLog &{APACHE_LOG_DIR}/access.log	**P**

		combined </VirtualHost> 6. Untuk Ubuntu; a2ensite example.com.conf a2ensite test.com.conf 7. Restart Apache; Service apache2 restart Maklumkan kepada pemohon melalui emel bahawa Virtual Host telah diwujudkan.	combined </VirtualHost> 6. Untuk Ubuntu; a2ensite example.com.conf a2ensite test.com.conf 7. Restart Apache; Service apache2 restart Maklumkan kepada pemohon melalui emel bahawa Virtual Host telah diwujudkan.	
ISMS (IDEC): 13/ 2016	**iDEC**	Nama Dokumen: ARAHAN KERJA PENGURUSAN ID VPN Kod Dokumen:UPM/ISMS/OPR/~~DC~~/AK10 No. Isu:_01_, No. Semakan:_00_, Tarikh Kuatkuasa: 23/01/2015	Nama Dokumen: ARAHAN KERJA PENGURUSAN ID VPN Kod Dokumen:UPM/ISMS/OPR/AK10 No. Isu:_01_, No. Semakan:_01_, Tarikh Kuatkuasa: 01/07/2016	**P**
		3.0 ARAHAN KERJA ARAHAN TERPERINCI Terima permohonan DNS melalui Borang ~~Sokongan Perkhidmatan ICT (OPR/UDC/SOK/BR03)~~ Menetapkan syarat pengaktifan maksimum tiga (3) bulan selepas tarikh kelulusan pendaftaran.	**3.0 ARAHAN KERJA** ARAHAN TERPERINCI Terima permohonan DNS melalui Borang Permohonan Perkhidmatan Sokongan ICT (OPR/IDEC/BR03/SOKONGAN ICT) Menetapkan syarat pengaktifan maksimum tiga (3) bulan selepas tarikh kelulusan pendaftaran.	**P**
ISMS (IDEC): 14/ 2016	**iDEC**	Nama Dokumen: ARAHAN KERJA PENGURUSAN BACKUP Kod Dokumen:UPM/ISMS/OPR/~~PD~~/AK02 No. Isu:_01_, No. Semakan:_02_, Tarikh Kuatkuasa: 23/01/2015	Nama Dokumen: ARAHAN KERJA PENGURUSAN BACKUP Kod Dokumen:UPM/ISMS/OPR/AK02 No. Isu:_01_, No. Semakan:_03_, Tarikh Kuatkuasa: 01/07/2016	
		2.0 DOKUMEN RUJUKAN **Kod Dokumen** / **Tajuk Dokumen** UPM/ISMS/~~PD~~/GP14 /BACKUP / Garis Panduan pengurusan Backup Pangkalan Data	**2.0 DOKUMEN RUJUKAN** **Kod Dokumen** / **Tajuk Dokumen** UPM/ISMS/GP14/BA CKUP / Garis Panduan pengurusan Backup Pangkalan Data	**P**
		3.0 ARAHAN KERJA ARAHAN TERPERINCI	**3.0 ARAHAN KERJA** ARAHAN TERPERINCI	**P**

<table>
<tr><td></td><td></td><td>Rancang jadual backup penyelenggaraan pangkalan data dengan merujuk Prosedur Penyelenggaraan ICT (~~UPM/SOK/ICT/P001).~~</td><td>Rancang jadual backup penyelenggaraan pangkalan data dengan merujuk Prosedur Penyelenggaraan ICT (UPM/OPR/IDEC/P003).</td><td></td></tr>
<tr><td>ISMS (IDEC): 15/ 2016</td><td>iDEC</td><td>Nama Dokumen: ARAHAN KERJA PELUPUSAN PITA BACKUP
Kod Dokumen:UPM/ISMS/OPR/~~PD~~/AK07
No. Isu:_01_, No. Semakan:_01_, Tarikh Kuatkuasa: 23/01/2015</td><td>Nama Dokumen: ARAHAN KERJA PELUPUSAN PITA BACKUP
Kod Dokumen:UPM/ISMS/OPR/AK07
No. Isu:_01_, No. Semakan:_02_, Tarikh Kuatkuasa: 01/07/2016</td><td></td></tr>
<tr><td></td><td></td><td>3.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>UPM/ISMS/~~PD~~/GP14 /BACKUP</td><td>Garis Panduan pengurusan Backup Pangkalan Data</td></tr></table></td><td>3.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>UPM/ISMS/GP14/BA CKUP</td><td>Garis Panduan pengurusan Backup Pangkalan Data</td></tr></table></td><td>P</td></tr>
<tr><td>ISMS (IDEC): 16/ 2016</td><td>iDEC</td><td>Nama Dokumen: GARIS PANDUAN PENYELENGGARAAN OPERASI PUSAT DATA
Kod Dokumen:UPM/ISMS/OPR/~~DC/~~GP01/PENYELENGGARAAN OPERASI
No. Isu:_01_, No. Semakan:_00_, Tarikh Kuatkuasa: 01/06/2012</td><td>Nama Dokumen: GARIS PANDUAN PENYELENGGARAAN OPERASI PUSAT DATA
Kod Dokumen:UPM/ISMS/OPR/GP01/PENYELENGGARAAN OPERASI
No. Isu:_01_, No. Semakan:_01_, Tarikh Kuatkuasa: 01/07/2016</td><td></td></tr>
<tr><td></td><td></td><td>3.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>~~UPM/SOK/ICT/P001~~</td><td>Prosedur Penyelenggaraan ICT</td></tr></table></td><td>3.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>UPM/OPR/IDEC/P003</td><td>Prosedur Penyelenggaraan ICT</td></tr></table></td><td>P</td></tr>
<tr><td>ISMS (IDEC): 17/ 2016</td><td>iDEC</td><td>Nama Dokumen: GARIS PANDUAN PENYEDIAAN SERVER DI PUSAT DATA
Kod Dokumen:UPM/ISMS/OPR/~~DC/~~GP02/PENYEDIAAN SERVER
No. Isu:_01_, No. Semakan:_02_, Tarikh Kuatkuasa: 12/08/2013</td><td>Nama Dokumen: GARIS PANDUAN PENYEDIAAN SERVER DI PUSAT DATA
Kod Dokumen:UPM/ISMS/OPR/GP02/PENYEDIAAN SERVER
No. Isu:_01_, No. Semakan:_03_, Tarikh Kuatkuasa: 01/07/2016</td><td></td></tr>
<tr><td></td><td></td><td>2.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>~~UPM/ISMS/OPR/DC/ AK01~~</td><td>~~Arahan Kerja Konfigurasi *Session Time-Out*~~</td></tr></table></td><td>2.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>UPM/ISMS/OPR/ AK11</td><td>Arahan Kerja Konfigurasi Server</td></tr></table></td><td>P</td></tr>
</table>

<table>
<tr><td></td><td></td><td><table><tr><td>~~UPM/ISMS/OPR/DC/AK05~~</td><td>~~Arahan Kerja Pemasangan Perisian Server~~</td></tr><tr><td>~~UPM/ISMS/OPR/DC/AK06~~</td><td>~~Arahan Kerja Kemaskini *Patches*~~</td></tr></table></td><td></td><td></td></tr>
<tr><td></td><td></td><td>4.0 PROSES PENYEDIAAN SERVER
3.0 Rujuk Arahan Kerja ~~Pemasangan Perisian Server (UPM/ISMS/OPR/AK05) untuk kerja-kerja pemasangan perisian pada server.~~ ..</td><td>4.0 PROSES PENYEDIAAN SERVER
3.0 Rujuk Arahan Kerja konfigurasi server (UPM/ISMS/OPR/AK11) untuk kerja-kerja pemasangan perisian pada server.</td><td>P</td></tr>
<tr><td></td><td></td><td>5.0 KESELAMATAN SERVER
Pastikan keselamatan server adalah ditahap yang sepatutnya dengan memastikan server dan storan telah pun diimbas dan ~~dilabelkan sebagai ‘SECURED’ oleh Unit~~ Keselamatan ICT UPM sebelum dibenarkan untuk beroperasi sepenuhnya di Pusat Data.</td><td>5.0 KESELAMATAN SERVER
Pastikan keselamatan server adalah ditahap yang sepatutnya dengan memastikan server dan storan telah pun diimbas dan selamat dari ancaman siber oleh Seksyen Keselamatan ICT UPM sebelum dibenarkan untuk beroperasi sepenuhnya di Pusat Data.</td><td>P</td></tr>
<tr><td></td><td></td><td>7.0 PENETAPAN KONFIGURASI SESSION-TIME-OUT
Pastikan penetapan konfigurasi session time-out dibuat pada server dengan merujuk Arahan Kerja ~~Konfigurasi *Session Time-Out* (UPM/ISMS/OPR/DC/AK01~~)...</td><td>7.0 PENETAPAN KONFIGURASI SESSION-TIME-OUT
Pastikan penetapan konfigurasi session time-out dibuat pada server dengan merujuk Arahan Kerja konfigurasi server (UPM/ISMS/OPR/AK11) untuk kerja-kerja pemasangan perisian pada server.</td><td>P</td></tr>
<tr><td>ISMS (IDEC): 18/2016</td><td>iDEC</td><td>Nama Dokumen: GARIS PANDUAN KAWALAN AKSES KE PUSAT DATA
Kod Dokumen:UPM/ISMS/OPR/~~DC/~~GP03/KAWALAN AKSES
No. Isu:_01_, No. Semakan:_03_, Tarikh Kuatkuasa: 23/01/2015</td><td>Nama Dokumen: GARIS PANDUAN KAWALAN AKSES KE PUSAT DATA
Kod Dokumen:UPM/ISMS/OPR/GP03/KAWALAN AKSES
No. Isu:_01_, No. Semakan:_04_, Tarikh Kuatkuasa: 01/07/2016</td><td>P</td></tr>
<tr><td></td><td></td><td>3.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Garis Panduan Teknologi Maklumat & Komunikasi (GPTMK)</td></tr><tr><td>UPM/ISMS/OPR/~~DC~~/P001</td><td>Prosedur Pengoperasian Pengurusan Pusat Data</td></tr></table></td><td>3.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Garis Panduan Teknologi Maklumat & Komunikasi (GPTMK)</td></tr><tr><td>UPM/ISMS/OPR/P001</td><td>Prosedur Pengoperasian Pengurusan Pusat Data</td></tr></table></td><td>p</td></tr>
</table>

		4.1 KAWALAN AKSES KE PUSAT DATA **1. Ruang Pusat Data** Ruang Pusat Data adalah merujuk kepada ~~Lokasi skop pensijilan ISMS di Manual Sistem Keselamatan Maklumat.~~	**4.1 KAWALAN AKSES KE PUSAT DATA** **1. Ruang Pusat Data** Ruang Pusat Data adalah merujuk kepada ruang server utama termasuk bilik konsol dan bilik penyediaan server (*Staging room*). **5. Pendaftaran Pelawat Atas Talian** Sistem pendaftaran pelawat secara atas talian dilaksanakan dan boleh diakses melalui url xxxxx	**P/T**
		4.2 KATEGORI PENGGUNA **1. STAF** Terdapat 3 kategori staf iaitu : **a. Staf Pengurus Pusat Data** Adalah merupakan staf yang bertanggungjawab mengurus Pusat Data seperti staf Unit Pusat Data, Unit Rangkaian, Unit Pentadbiran Data dan Unit Keselamatan ICT sahaja. **2. PELAWAT** Berikut adalah kategori pengguna yang diletakkan dibawah kategori pelawat: **a. PELANGGAN/PEMBEKAL PENYELENGGARAAN DAN PERKHIDMATAN** i. Pembekal yang mempunyai kontrak penyelenggaraan dan bertanggungjawab untuk melaksanakan kerja-kerja penyelenggaraan secara berkala seperti yang tercatat di dalam Perjanjian yang telah dibuat antara pihak Pusat Data dan juga Pembekal.	**4.2 KATEGORI PENGGUNA** **1. STAF** Terdapat 3 kategori staf iaitu : **b. Staf Pengurus Pusat Data** Adalah merupakan staf yang bertanggungjawab mengurus Pusat Data melibatkan pengurusan server, pangkalan data, rangkaian dan keselamatan di Pusat Data. **2. PELAWAT** Berikut adalah kategori pengguna yang diletakkan dibawah kategori pelawat: **a. PELANGGAN/PEMBEKAL PENYELENGGARAAN DAN PERKHIDMATAN** i. Pembekal yang mempunyai kontrak penyelenggaraan dan bertanggungjawab untuk melaksanakan kerja-kerja penyelenggaraan secara berkala seperti yang tercatat di dalam Perjanjian yang telah dibuat antara pihak Pusat Data dan juga Pembekal. ii. Perlu melengkapkan Borang Pendaftaran Pembekal (UPM/ISMS/OPR/BR04/PENDAFTARAN PEMBEKAL) dan perlu disahkan oleh pihak syarikat. iii. Pihak Pembekal perlu mengisi dan	**P** **P**

		ii. Perlu melengkapkan Borang Pendaftaran Pembekal (UPM/ISMS/OPR/~~DC~~/BR04/PENDAFTARAN PEMBEKAL) dan perlu disahkan oleh pihak syarikat. iii. Pihak Pembekal perlu mengisi dan menandatangani Surat Aku Janji Pihak luar. iv. Kehadiran pihak pembekal mesti bersama sekurang-kurangnya seorang yang telah didaftar atau disenaraikan di dalam Borang Pendaftaran Pembekal. v. Perlu mengisi Borang Pendaftaran Pelawat (UPM/ISMS/OPR/~~DC~~/BR01/PENDAFTARAN PELAWAT) dan perlu mendapat pengesahan dari Pemilik Sistem/Aplikasi/~~UDC~~ yang berkaitan sebelum dibenarkan untuk masuk ke Pusat Data. **b. PELAWAT RASMI** i. Pelawat adalah merupakan kategori pengguna yang datang untuk melawat Pusat Data atas tujuan pembelajaran, penyelidikan atau lawatan tapak. ii. Perlu mendapat kebenaran awal daripada Ketua ~~Unit~~ Pusat Data. iii. Makluman untuk lawatan ke Pusat Data perlulah dibuat dalam tempoh sekurang-kurangnya 1 hari lebih awal bagi tujuan kelulusan dan perancangan. iv. Perlu mengisi Borang Pendaftaran Pelawat (UPM/ISMS/OPR/~~DC~~/BR01/PENDAFTARAN PELAWAT) dan perlu mendapat pengesahan dari Pemilik Sistem/Aplikasi yang berkaitan.	menandatangani Surat Aku Janji Pihak luar. iv. Kehadiran pihak pembekal mesti bersama sekurang-kurangnya seorang yang telah didaftar atau disenaraikan di dalam Borang Pendaftaran Pembekal. v. Perlu mengisi Borang Pendaftaran Pelawat (UPM/ISMS/OPR/BR01/PENDAFTARAN PELAWAT) dan perlu mendapat pengesahan dari Pemilik Sistem/Aplikasi/Pengiring yang berkaitan sebelum dibenarkan untuk masuk ke Pusat Data. **b. PELAWAT RASMI** i. Pelawat adalah merupakan kategori pengguna yang datang untuk melawat Pusat Data atas tujuan pembelajaran, penyelidikan atau lawatan tapak. ii. Perlu mendapat kebenaran awal daripada Ketua Pusat Data. iii. Makluman untuk lawatan ke Pusat Data perlulah dibuat dalam tempoh sekurang-kurangnya 1 hari lebih awal bagi tujuan kelulusan dan perancangan. iv. Perlu mengisi Borang Pendaftaran Pelawat (UPM/ISMS/OPR/BR01/PENDAFTARAN PELAWAT) dan perlu mendapat pengesahan dari Pemilik Sistem/Aplikasi yang berkaitan.	**P**
		5.0 PROSES KAWALAN AKSES KE PUSAT DATA **5.1 KATEGORI STAF**	**5.0 PROSES KAWALAN AKSES KE PUSAT DATA** **5.1 KATEGORI STAF**	**P**

		1. Memastikan staf yang ingin akses ke Pusat Data telah mendapat kebenaran oleh Staf Pusat Data. 2. Mengisi maklumat staf yang diperlukan ke dalam Log Keluar Masuk Pusat Data (Staf) (UPM/ISMS/OPR/~~DC~~/BL01/AKSES STAF). 3. Memastikan staf berkenaan sentiasa memakai dan mempamerkan kad staf sepanjang berada di pusat data. 4. Mengemaskini waktu keluar di dalam Log Keluar Masuk Pusat Data (Staf) (UPM/ISMS/OPR/~~DC~~/BL01/AKSES STAF). **5.2 KATEGORI PELAWAT** 1. Meminta pelawat untuk mengisi Borang Pendaftaran Pelawat (UPM/ISMS/OPR/~~DC~~/BR01/PENDAFTARAN PELAWAT) 2. Memastikan borang lengkap diisi oleh pelawat. 3. Memastikan Borang Pendaftaran Pelawat (UPM/ISMS/OPR/~~DC~~/BR01/PENDAFTARAN PELAWAT) telah pun disahkan oleh Pemilik Sistem/Aplikasi yang berkaitan. 4. Mengisi maklumat pelawat ke dalam Log Keluar Masuk Pusat Data (Pelawat) (UPM/ISMS/OPR/~~DC~~/BL02/AKSES PELAWAT). 5. Menyerahkan pas pelawat kepada pelawat . 6. Staf Pusat Data / staf dari unit berkaitan mestilah memantau sebarang aktiviti pelawat sepanjang berada di Pusat Data. 7. Memastikan pelawat sentiasa memakai dan mempamerkan pas pelawat sepanjang berada di pusat data. 8. Memastikan pelawat memulangkan kembali pas kepada petugas kaunter sebaik sahaja aktiviti selesai 9. Mengemaskini waktu keluar di dalam Log	1. Memastikan staf yang ingin akses ke Pusat Data telah mendapat kebenaran oleh Staf Pusat Data. 2. Mengisi maklumat staf yang diperlukan ke dalam Log Keluar Masuk Pusat Data (Staf) (UPM/ISMS/OPR/BL01/AKSES STAF). 3. Memastikan staf berkenaan sentiasa memakai dan mempamerkan kad staf sepanjang berada di pusat data. 4. Mengemaskini waktu keluar di dalam Log Keluar Masuk Pusat Data (Staf) (UPM/ISMS/OPR/BL01/AKSES STAF). **5.2 KATEGORI PELAWAT** 1. Meminta pelawat untuk mengisi Borang Pendaftaran Pelawat (UPM/ISMS/OPR/BR01/PENDAFTARAN PELAWAT) 2. Memastikan borang lengkap diisi oleh pelawat. 3. Memastikan Borang Pendaftaran Pelawat (UPM/ISMS/OPR/BR01/PENDAFTARAN PELAWAT) telah pun disahkan oleh Pemilik Sistem/Aplikasi yang berkaitan. 4. Mengisi maklumat pelawat ke dalam Log Keluar Masuk Pusat Data (Pelawat) (UPM/ISMS/OPR/BL02/AKSES PELAWAT). 5. Menyerahkan pas pelawat kepada pelawat . 6. Staf Pusat Data / staf dari unit berkaitan mestilah memantau sebarang aktiviti pelawat sepanjang berada di Pusat Data. 7. Memastikan pelawat sentiasa memakai dan mempamerkan pas pelawat sepanjang berada di pusat data. 8. Memastikan pelawat memulangkan kembali pas kepada petugas kaunter sebaik sahaja aktiviti selesai 9. Mengemaskini waktu keluar di dalam Log Keluar Masuk Pusat Data (Pelawat) (UPM/ISMS/OPR/BL02/AKSES PELAWAT). 10. Menyimpan borang pendaftaran pelawat yang telah lengkap ke dalam fail yang berkaitan.	

<table>
<tr><td></td><td></td><td>Keluar Masuk Pusat Data (Pelawat) (UPM/ISMS/OPR/~~DC~~/BL02/AKSES PELAWAT).
10. Menyimpan borang pendaftaran pelawat yang telah lengkap ke dalam fail yang berkaitan.</td><td></td><td></td></tr>
<tr><td>ISMS (IDEC): 19/2016</td><td>iDEC</td><td>Nama Dokumen: GARIS PANDUAN PEMANTAUAN OPERASI PUSAT DATA
Kod Dokumen:UPM/ISMS/OPR/~~DC/~~GP05/PEMANTAUAN OPERASI
No. Isu:_01_, No. Semakan:_00_, Tarikh Kuatkuasa: 01/06/2012</td><td>Nama Dokumen: GARIS PANDUAN PEMANTAUAN OPERASI PUSAT DATA
Kod Dokumen:UPM/ISMS/OPR/GP05/PEMANTAUAN OPERASI
No. Isu:_01_, No. Semakan: 01_, Tarikh Kuatkuasa: 01/07/2016</td><td></td></tr>
<tr><td></td><td></td><td>3.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Garis Panduan Teknologi Maklumat & Komunikasi (GPTMK)</td></tr><tr><td>UPM/ISMS/ OPR/~~DC~~/P001</td><td>Prosedur Pengoperasian Pengurusan Pusat Data</td></tr></table></td><td>3.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Garis Panduan Teknologi Maklumat & Komunikasi (GPTMK)</td></tr><tr><td>UPM/ISMS/ OPR/P001</td><td>Prosedur Pengoperasian Pengurusan Pusat Data</td></tr></table></td><td>P</td></tr>
<tr><td></td><td></td><td>4.1 OPERASI SERVER
4.1.1 PANTAU OPERASI SERVER
4. Pastikan fail Server ini akan disemak dan dipantau oleh ~~Ketua Unit Pusat data~~ dari semasa ke semasa.</td><td>4.1 OPERASI SERVER
4.1.1 PANTAU OPERASI SERVER
4. Pastikan fail Server ini akan disemak dan dipantau oleh Ketua Seskyen Pusat Data dari semasa ke semasa.</td><td>P</td></tr>
<tr><td></td><td></td><td>4.2 OPERASI INFRASTRUKTUR DAN KEMUDAHAN
4.2.1 CATAT AKTIVITI PEMANTAUAN KE DALAM LOG PEMANTAUAN
1. Rekod aktiviti pemantauan ke dalam Log Pemantauan Operasi Pusat Data (UPM/ISMS/OPR/~~DC~~/BL05/PEMANTAUAN OPERASI) secara berkala.</td><td>4.2 OPERASI INFRASTRUKTUR DAN KEMUDAHAN
4.2.1 CATAT AKTIVITI PEMANTAUAN KE DALAM LOG PEMANTAUAN
2. Rekod aktiviti pemantauan ke dalam Log Pemantauan Operasi Pusat Data (UPM/ISMS/OPR/BL05/PEMANTAUAN OPERASI) secara berkala.</td><td>P</td></tr>
</table>

<table>
<tr>
<td>ISMS (IDEC): 20/2016</td>
<td>iDEC</td>
<td>Nama Dokumen: GARIS PANDUAN PEMANTAUAN CAPAIAN KE SISTEM DI PUSAT DATA
Kod Dokumen:UPM/ISMS/OPR/<s>DC/</s>GP06/PEMANTAUAN CAPAIAN
No. Isu:_01_, No. Semakan:_01_, Tarikh Kuatkuasa: 12/08/2013</td>
<td>Nama Dokumen: GARIS PANDUAN PEMANTAUAN CAPAIAN KE SISTEM
Kod Dokumen:UPM/ISMS/OPR/GP05/PEMANTAUAN CAPAIAN
No. Isu:_01_, No. Semakan: 02_, Tarikh Kuatkuasa: 01/07/2016</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.0 DOKUMEN RUJUKAN
<table>
<tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr>
<tr><td>-</td><td>Garis Panduan Teknologi Maklumat & Komunikasi (GPTMK)</td></tr>
<tr><td>UPM/ISMS/ OPR/<s>DC</s>/P001</td><td>Prosedur Pengoperasian Pengurusan Pusat Data</td></tr>
<tr><td>UPM/ISMS/O PR/<s>DC</s>/P003</td><td>Prosedur Kawalan dan Pemantauan Capaian ke Sistem Di Pusat Data</td></tr>
<tr><td>UPM/OPR/iDE C/P002</td><td>Prosedur Perkhidmatan Sokongan ICT</td></tr>
<tr><td><s>UPM/ISMS/S OK/GP01/KAT A LALUAN</s></td><td><s>Garis Panduan pengurusan Kata Laluan</s></td></tr>
</table></td>
<td>3.0 DOKUMEN RUJUKAN
<table>
<tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr>
<tr><td>-</td><td>Garis Panduan Teknologi Maklumat & Komunikasi (GPTMK)</td></tr>
<tr><td>UPM/ISMS/ OPR/P001</td><td>Prosedur Pengoperasian Pengurusan Pusat Data</td></tr>
<tr><td>UPM/ISMS/O PR/P003</td><td>Prosedur Kawalan dan Pemantauan Capaian ke Sistem</td></tr>
<tr><td>UPM/OPR/iDE C/P002</td><td>Prosedur Perkhidmatan Sokongan ICT</td></tr>
<tr><td>UPM/ISMS/S OK/GP07/IDE NTITI</td><td>Garis Panduan Pengurusan Identiti</td></tr>
</table></td>
<td>P</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.0 PEMANTAUAN CAPAIAN
3. Berikut adalah <s>ketegori</s> hak capaian yang dibenarkan:
<s>a. Maksimum</s>
i. Pengguna yang diberi akses sebagai Admin atau yang setara dengannya.
ii. Pengguna boleh mewujud, menyimpan, mengemaskini, mengubah dan membatalkan maklumat.
iii. Pengguna yang diberi hak maksimum adalah pengguna yang merupakan staf</td>
<td>4.1 PEMANTAUAN CAPAIAN
3. Berikut adalah hak capaian yang dibenarkan:
i. Pengguna yang diberi akses sebagai Admin atau yang setara dengannya.
ii. Pengguna boleh mewujud, menyimpan, mengemaskini, mengubah dan membatalkan maklumat.
iii. Pengguna yang diberi hak maksimum adalah pengguna yang merupakan staf pusat data yang telah dipertanggungjawabkan sepenuhnya oleh Ketua Seskyen Pusat Data untuk mengawal dan menjaga</td>
<td>P/T</td>
</tr>
</table>

		pusat data yang telah dipertanggungjawabkan sepenuhnya oleh Ketua ~~Unit~~ Pusat Data untuk mengawal dan menjaga server. iv. Pengguna yang diberi hak capaian maksimum adalah pengguna yang merupakan staf IT UPM yang telah diberi kebenaran oleh ~~pemilik sistem/server~~ untuk memiliki ID yang bertaraf Admin. b. ~~Minimum~~ ~~i. Pengguna yang ditentukan oleh pemilik sistem, hanya boleh membaca dan melihat maklumat.~~ ~~ii. Pengguna yang diberi akses secara terhad sebagaimana yang telah ditentukan oleh pemilik sistem/server.~~ ~~iii. Pengguna yang diberi hak capaian minimum adalah pengguna yang merupakan staf UPM yang telah diberi kebenaran oleh pemilik sistem untuk memiliki ID yang terhad (minima) penggunaannya.~~ **c.** ~~Memerlukan kelulusan~~ ~~Pengguna yang hanya layak diberi hak capaian minimum tetapi memerlukan capaian maksimum perlu mendapat kelulusan dari pemilik sistem atau Pengarah iDEC.~~	server. iv. Pengguna yang diberi hak capaian maksimum adalah pengguna yang merupakan staf IT UPM yang telah diberi kebenaran oleh Pentadbir Proses atau Pengarah untuk memiliki ID yang bertaraf Admin. v. Capaian ke sistem dari luar Pusat Data oleh Pentadbir sistem hanya dibenarkan melalui kaedah dan kawalan berikut: i. Pengguna merupakan authorized user yang berdaftar dan proses login perlu melalui sistem authentication User ID server yang hendak dicapai; dan ii. Bagi capaian dalam rangkaian setempat (LAN), maklumat IP dan MAC address komputer/workstation pengguna perlu berdaftar dan diberi hak akses oleh server berkenaan. Sebagai contoh maklumat workstation berkenaan didaftarkan dalam konfigurasi hosts.allow bagi server UNIX; atau iii. Bagi capaian melalui rangkaian Internet , pengguna perlu mendaftar untuk menggunakan sistem keselamatan Virtual Private Network (VPN).	
		4.1 PEMILIKAN ID DAN KATALALUAN i. Pemilikan ID dan katalaluan 'Root' hanya diberikan kepada ~~Unit~~ Pusat Data.	**4.1 PEMILIKAN ID DAN KATALALUAN** i. Pemilikan ID dan katalaluan 'Root' hanya diberikan kepada Seksyen Pusat Data.	**P**

		ii. Pentadbir server diberikan ID capaian bertaraf 'System Administrator' sepenuhnya dengan kebenaran Ketua ~~Unit~~ Pusat Data.	**ii.** Pentadbir server diberikan ID capaian bertaraf 'System Administrator' sepenuhnya dengan kebenaran Ketua Seskyen Pusat Data.	
		4.2 PENGGUNA AKTIF/BARU Pengguna yang aktif adalah pengguna yang diberi hak capaian ke sistem dan boleh membuat capaian ke sistem sama ada secara kerap atau tidak dan capaian ke sistem menggunakan Root password hanya boleh dilakukan dengan menggunakan console yang telah disediakan sahaja. Hanya pengguna sah yang tersenarai di dalam Log Senarai Pengguna Sah Pusat Data (UPM/ISMS/OPR/~~DC~~/BL06/PENGGUNA SAH) sahaja yang dibenarkan untuk remote access ke server menggunakan ID pengguna dan katalaluan yang telah ditetapkan.	**4.2 PENGGUNA AKTIF/BARU** Pengguna yang aktif adalah pengguna yang diberi hak capaian ke sistem dan boleh membuat capaian ke sistem sama ada secara kerap atau tidak dan capaian ke sistem menggunakan Root password hanya boleh dilakukan dengan menggunakan console yang telah disediakan sahaja. Hanya pengguna sah yang tersenarai di dalam Log Senarai Pengguna Sah Pusat Data (UPM/ISMS/OPR /BL06/PENGGUNA SAH) sahaja yang dibenarkan untuk remote access ke server menggunakan ID pengguna dan katalaluan yang telah ditetapkan.	**P**
		1. ID PENGGUNA a. Terima Borang Permohonan Perkhidmatan Sokongan ICT (OPR/iDEC/BR03/Sokongan ICT) daripada pengguna yang ingin memohon ID Pengguna dan katalaluan. b. Wujudkan satu pengenalan diri (ID Pengguna) yang unik untuk setiap pengguna berdasarkan pengkhususan tugas dalam senarai tugas pengguna tersebut dan hanya boleh digunakan oleh pengguna tersebut sahaja. ~~c.~~ Cara mewujudkan ID pengguna yang akan didaftarkan haruslah merujuk kepada ~~Garis Panduan Pengurusan Kata Laluan (UPM/ISMS/SOK/GP01/KATA LALUAN).~~ d. Rekod maklumat pengguna ke dalam Log Senarai Pengguna Sah Pusat Data (UPM/ISMS/OPR/~~DC~~/BL06/PENGGUNA SAH). e. Serah ID pengguna yang telah didaftarkan kepada	**1. ID PENGGUNA** a. Terima Borang Permohonan Perkhidmatan Sokongan ICT (OPR/iDEC/BR03/Sokongan ICT) daripada pengguna yang ingin memohon ID Pengguna dan katalaluan. b. Wujudkan satu pengenalan diri (ID Pengguna) yang unik untuk setiap pengguna berdasarkan pengkhususan tugas dalam senarai tugas pengguna tersebut dan hanya boleh digunakan oleh pengguna tersebut sahaja. c. Cara mewujudkan ID pengguna yang akan didaftarkan haruslah merujuk kepada Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI) d. Rekod maklumat pengguna ke dalam Log Senarai Pengguna Sah Pusat Data (UPM/ISMS/OPR/BL06/PENGGUNA SAH). e. Serah ID pengguna yang telah didaftarkan kepada pemohon mestilah melalui serahan tangan sahaja dan ianya perlu mendapat pengesahan penerimaan dari pemohon.	**P**

		pemohon mestilah melalui serahan tangan sahaja dan ianya perlu mendapat pengesahan penerimaan dari pemohon.		
		4.3 PENGGUNA BERTUKAR/TAMAT PERKHIDMATAN Berikut adalah beberapa kategori pengguna yang diklasifikasikan di bawah kategori pengguna yang bertukar/tamat perkhidmatan **1. KATEGORI PENGGUNA BERTUKAR** a. Staf yang dipindahkan dari ~~unit~~ pusat data ke ~~unit~~ yang lain. **b.** Staf yang dipindahkan dari satu ~~unit~~ ke satu ~~unit~~ yang lain.	**4.3 PENGGUNA BERTUKAR/TAMAT PERKHIDMATAN** Berikut adalah beberapa kategori pengguna yang diklasifikasikan di bawah kategori pengguna yang bertukar/tamat perkhidmatan 1. **KATEGORI PENGGUNA BERTUKAR** a. Staf yang dipindahkan dari seksyen pusat data ke seksyen yang lain. b. Staf yang dipindahkan dari satu seskyen ke satu seskyen yang lain.	**P**
		4.3.1 MAKLUMAT PENGGUNA BERTUKAR/TAMAT PERKHIDMATAN **a.** Terima maklumat pengguna bertukar/tamat perkhidmatan **b.** Semak maklumat pengguna dalam Log Senarai Pengguna Sah Pusat Data (UPM/ISMS/OPR/~~DC~~/BL06/PENGGUNA SAH).	**4.3.1 MAKLUMAT PENGGUNA BERTUKAR/TAMAT PERKHIDMATAN** **a.** Terima maklumat pengguna bertukar/tamat perkhidmatan **b.** Semak maklumat pengguna dalam Log Senarai Pengguna Sah Pusat Data (UPM/ISMS/OPR /BL06/PENGGUNA SAH).	**P**
		4.3.3 SENARAI PENGGUNA PUSAT DATA a. Kemaskini Log Senarai Pengguna Sah Pusat Data (UPM/ISMS/OPR/~~DC~~/BL06/PENGGUNA SAH). b. Rekodkan nama pengguna tersebut kedalam Log Senarai Pengguna Bertukar/tamat perkhidmatan (UPM/ISMS/OPR/~~DC~~/BL07/PENGGUNA TAMAT PERKHIDMATAN).	**4.3.3 SENARAI PENGGUNA PUSAT DATA** c. Kemaskini Log Senarai Pengguna Sah Pusat Data (UPM/ISMS/OPR/BL06/PENGGUNA SAH). d. Rekodkan nama pengguna tersebut kedalam Log Senarai Pengguna Bertukar/tamat perkhidmatan (UPM/ISMS/OPR/BL07/PENGGUNA TAMAT PERKHIDMATAN).	**P**
ISMS (IDEC): 21/2016	**iDEC**	Nama Dokumen: GARIS PANDUAN PEMANTAUAN, PENGUKURAN, ANALISIS DAN PENILAIAN Kod Dokumen:UPM/ISMS/OPR/~~DC/~~GP07/SECURITY METRICS No. Isu:_01_, No. Semakan:_03_, Tarikh Kuatkuasa: 16/11/2015	Nama Dokumen: GARIS PANDUAN PEMANTAUAN, PENGUKURAN, ANALISIS DAN PENILAIAN Kod Dokumen:UPM/ISMS/OPR/~~DC/~~GP07/SECURITY METRICS No. Isu:_01_, No. Semakan: 04_, Tarikh Kuatkuasa: 01/07/2016	**P**

<table>
<tr>
<td></td>
<td></td>
<td>2.0 DOKUMEN RUJUKAN
<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Lampiran 1</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>P</td>
</tr>
<tr>
<td>ISMS (IDEC): 22/2016</td>
<td>iDEC</td>
<td>Nama Dokumen: GARIS PANDUAN PERLINDUNGAN MAKLUMAT LOG SERVER
Kod Dokumen:UPM/ISMS/OPR/~~DC/~~GP08/MAKLUMAT LOG
No. Isu:_01_, No. Semakan:_00_, Tarikh Kuatkuasa: 09/11/2012</td>
<td>Nama Dokumen: GARIS PANDUAN PERLINDUNGAN MAKLUMAT LOG SERVER
Kod Dokumen:UPM/ISMS/OPR/GP08/MAKLUMAT LOG
No. Isu:_01_, No. Semakan: 01_, Tarikh Kuatkuasa: 01/07/2016</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.0 DOKUMEN RUJUKAN
<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Garis Panduan Teknologi Maklumat & Komunikasi (GPTMK)</td></tr><tr><td>UPM/ISMS/ OPR/~~DC~~/P003</td><td>Prosedur Pemantauan Capaian ke Sistem</td></tr></table></td>
<td>3.0 DOKUMEN RUJUKAN
<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Garis Panduan Teknologi Maklumat & Komunikasi (GPTMK)</td></tr><tr><td>UPM/ISMS/ OPR/P001</td><td>Prosedur Pemantauan Capaian ke Sistem</td></tr></table></td>
<td>P</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.0 SKOP
Garis panduan ini digunapakai untuk memastikan maklumat log yang terdapat pada server di Pusat Data UPM dilindungi.</td>
<td>2.0 SKOP
Garis panduan ini digunapakai untuk memastikan maklumat log yang terdapat pada server di Pusat Data UPM dilindungi.</td>
<td></td>
</tr>
<tr>
<td>ISMS (IDEC): 23/2016</td>
<td>iDEC</td>
<td>Nama Dokumen: GARIS PANDUAN PENILAIAN TAHAP KESELAMATAN
Kod Dokumen:UPM/ISMS/OPR/~~DC/~~GP09/TAHAP KESELAMATAN
No. Isu:_01_, No. Semakan:_01_, Tarikh Kuatkuasa: 12/08/2013</td>
<td>Nama Dokumen: GARIS PANDUAN PENILAIAN TAHAP KESELAMATAN
Kod Dokumen:UPM/ISMS/OPR/~~DC/~~GP09/TAHAP KESELAMATAN
No. Isu:_01_, No. Semakan: 02_, Tarikh Kuatkuasa: 01/07/2016</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.0 TUJUAN

Garis panduan ini disediakan untuk rujukan staf ~~Unit~~ Keselamatan ICT yang terlibat dalam melaksanakan imbasan terhadap server yang terlibat dalam skop ISMS. Ia juga digunakan untuk menghindarkan sistem ICT dari serangan penceroboh (hackers), mengelakkan data hilang atau dicuri oleh penceroboh (hackers),</td>
<td>1.0 TUJUAN

Garis panduan ini disediakan untuk rujukan staf Seksyen Keselamatan ICT yang terlibat dalam melaksanakan imbasan terhadap server yang terlibat dalam skop ISMS. Ia juga digunakan untuk menghindarkan sistem ICT dari serangan penceroboh (hackers), mengelakkan data hilang atau dicuri oleh penceroboh (hackers), memastikan integriti data di</td>
<td>P</td>
</tr>
</table>

<table>
<tr>
<td></td><td></td>
<td>memastikan integriti data di dalam sistem ICT sentiasa terpelihara, dan meningkatkan keyakinan pengguna terhadap tahap keselamatan sistem aplikasi yang digunakan.</td>
<td>dalam sistem ICT sentiasa terpelihara, dan meningkatkan keyakinan pengguna terhadap tahap keselamatan sistem aplikasi yang digunakan.</td>
<td></td>
</tr>
<tr>
<td></td><td></td>
<td><s>3.0</s> SKOP

1. Semua sistem ICT yang mempunyai sambungan Rangkaian UPMNet.
2. Semua Sistem Aplikasi Web UPM merangkumi:-
a. Semua Sistem Aplikasi Web Baru yang dibangunkan secara dalaman atau outsource
b. Semua Sistem Aplikasi Web Baru yang dicapai secara Intranet sahaja atau Internet sahaja atau kedua-duanya sekali.</td>
<td><u>2.0</u> SKOP

1. Semua sistem ICT yang mempunyai sambungan Rangkaian UPMNet.
2. Semua Sistem Aplikasi Web UPM merangkumi:-
a. Semua Sistem Aplikasi Web Baru yang dibangunkan secara dalaman atau outsource
b. Semua Sistem Aplikasi Web Baru yang dicapai secara Intranet sahaja atau Internet sahaja atau kedua-duanya sekali.</td>
<td></td>
</tr>
<tr>
<td></td><td></td>
<td>2.0 DOKUMEN RUJUKAN
<table>
<tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr>
<tr><td>UPM/OPR/iDEC/P002</td><td>Prosedur Perkhidmatan Sokongan ICT</td></tr>
<tr><td>UPM/ISMS/OPR/KES/P004</td><td>Prosedur Pengendalian Insiden</td></tr>
</table>
</td>
<td>3.0 DOKUMEN RUJUKAN
<table>
<tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr>
<tr><td>UPM/OPR/iDEC/P002</td><td>Prosedur Perkhidmatan Sokongan ICT</td></tr>
<tr><td>UPM/ISMS/OPR/GP18/PENGENDALIAN INSIDEN</td><td>Garis Panduan Pengendalian Insiden</td></tr>
</table>
</td>
<td>P</td>
</tr>
<tr>
<td></td><td></td>
<td>4.0 PASUKAN PELAKSANA
<s>Pasukan Risk Assessment ISMS UPM dan turut dibantu oleh Pasukan UPMCert.</s></td>
<td>4.0 PASUKAN PELAKSANA
<u>Pasukan Seksyen Keselamatan ICT Pusat Pembangunan Maklumat dan Komunikasi</u></td>
<td>P</td>
</tr>
<tr>
<td></td><td></td>
<td>5.0 PROSES KERJA IMBASAN
<table>
<tr><th>BIL</th><th>PROSES</th><th>RUJUKAN</th><th>TANGGUNG JAWAB</th></tr>
<tr><td>1</td><td>Pemohon melengkapkan Borang</td><td>OPR/iDEC/BR03/Borang</td><td>Semua staf</td></tr>
</table>
</td>
<td>5.0 PROSES KERJA IMBASAN
<table>
<tr><th>BIL</th><th>PROSES</th><th>RUJUKAN</th><th>TANGGUNG JAWAB</th></tr>
<tr><td>1</td><td>Pemohon melengkapkan Borang</td><td>OPR/iDEC/BR03/Borang</td><td>Semua staf</td></tr>
</table>
</td>
<td>P</td>
</tr>
</table>

				Permohonan Perkhidmatan Sokongan ICT	Perkhidmatan Sokongan ICT				Permohonan Perkhidmatan Sokongan ICT	Perkhidmatan Sokongan ICT			
			2	Permohonan diterima dan agihan kerja ditentukan oleh Unit Keselamatan ICT Proses Imbasan akan dilaksanakan sebanyak 2 kali setahun	Mengisi log Imbasan tahap keselamatan server / sistem berkala tahunan UPM/ISMS/ OPR/KES/IR H2.3	Staf ~~UKICT~~			2	Permohonan diterima dan agihan kerja ditentukan oleh Unit Keselamatan ICT Proses Imbasan akan dilaksanakan sebanyak 2 kali setahun	Mengisi log Imbasan tahap keselamatan server / sistem berkala tahunan UPM/ISMS/ OPR/KES/IR H2.3	Staf SKI		
			3	Dapatkan maklumat Server dan Sistem Aplikasi dari staf Unit Pusat Data		Staf ~~UKICT~~			3	Dapatkan maklumat Server dan Sistem Aplikasi dari staf Unit Pusat Data		Staf SKI		
			4	Pelaksanaan Penilaian Tahap Keselamatan Server dan Sistem Aplikasi dilaksanakan bermula dari tarikh arahan (**5-7 hari bekerja diperuntukkan**) Proses dilaksanakan pasukan pelaksana adalah seperti berikut : a) PProses imbasan dilakukan pada peringkat *Operating System* bagi menilai tahap		Staf ~~UKICT~~ Staf ~~UKICT~~			4	Pelaksanaan Penilaian Tahap Keselamatan Server dan Sistem Aplikasi dilaksanakan bermula dari tarikh arahan (**5-7 hari bekerja diperuntukkan**) Proses dilaksanakan pasukan pelaksana adalah seperti berikut : a) PProses imbasan dilakukan pada peringkat *Operating System* bagi menilai tahap		Staf SKI Staf SKI		

				keselamatan ICT Server dan Sistem Aplikasi;					keselamatan ICT Server dan Sistem Aplikasi;				
				b) GGunakan perisian sokongan bagi menilai tahap keselamatan Server dan Sistem Aplikasi;	Borang IRH 2.0 – Maklumat Imbasan Server/Host	Pentadbir Sistem			b) GGunakan perisian sokongan bagi menilai tahap keselamatan Server dan Sistem Aplikasi;	Borang IRH 2.0 – Maklumat Imbasan Server/Host	Pentadbir Sistem	
				c) GGunakan perisian sokongan bagi menjana Laporan imbasan *port* yang berstatus *open*.					c) GGunakan perisian sokongan bagi menjana Laporan imbasan *port* yang berstatus *open*.				
				d) SSetelah proses imbasan selesai, laporan imbasan *port* akan dihantar ke pentadbir sistem.	Borang IRH 2.1 – Maklumbalas Tindakan Susulan Dari Imbasan Host/Server	Pentadbir Sistem			d) SSetelah proses imbasan selesai, laporan imbasan *port* akan dihantar ke pentadbir sistem.	Borang IRH 2.1 – Maklumbalas Tindakan Susulan Dari Imbasan Host/Server	Pentadbir Sistem		
				e) NNyatakan syor /cadangan pengukuhan hasil imbasan *Port* yang berstatus *open* hendaklah ditutup sekiranya tidak digunakan sebagai langkah keselamatan.					e) NNyatakan syor /cadangan pengukuhan hasil imbasan *Port* yang berstatus *open* hendaklah ditutup sekiranya tidak digunakan sebagai langkah keselamatan.				
				f) LLaporan yang dihantar perlulah ada maklumbalas dari pentadbir sistem sama ada tindakan pengukuhan sudah dibuat atau belum					f) LLaporan yang dihantar perlulah ada maklumbalas dari pentadbir sistem sama ada tindakan pengukuhan sudah dibuat atau belum				

				berdasarkan laporan yang diberi oleh staf UKICT g) TTandatangan Borang IRH 2.0 ,Borang IRH 2.1 dan Borang IRH2.2, Borang IRH 2.3						
				berdasarkan laporan yang diberi oleh staf UKICT g) TTandatangan Borang IRH 2.0 ,Borang IRH 2.1 dan Borang IRH2.2, Borang IRH 2.3 h) PProses imbasan kedua dilakukan setelah pentadbir sistem melaksanakan tindakan pengukuhan seperti yang dicadangkan.		STAF SKI		
ISMS (IDEC): 24/2016	**iDEC**	Nama Dokumen: GARIS PANDUAN PENGURUSAN SISTEM PENGKABELAN Kod Dokumen:UPM/ISMS/OPR/~~NET/~~GP12/PEMASANGAN KABEL No. Isu:_01_, No. Semakan:_00_, Tarikh Kuatkuasa: 09/11/2012			Nama Dokumen: GARIS PANDUAN PENGURUSAN SISTEM PENGKABELAN Kod Dokumen:UPM/ISMS/OPR/GP12/PEMASANGAN KABEL No. Isu:_01_, No. Semakan: 01_, Tarikh Kuatkuasa: 01/07/2016				**P**
		5.0 PROSES PERLAKSANAAN a. Sebarang perolehan sistem pengkabelan telekomunikasi perlu mendapat dan melalui proses kelulusan Jawatankuasa Kerja ICT (JKICT). b. Rekabentuk dan cadangan perkakasan sistem pengkabelan telekomunikasi perlu mendapat pengesahan oleh ~~Unit Rangkaian~~ IDEC melalui perkhidmatan sokongan yang diberikan (rujuk Prosedur Perkhidmatan Sokongan ICT (UPM/OPR/iDEC/P002)). **c.** Instalasi pengkabelan telekomunikasi tidak boleh dilaksanakan oleh mana-mana pihak tanpa kebenaran, kelulusan dan pengesahan ~~Unit~~			**5.0 PROSES PERLAKSANAAN** a. Sebarang perolehan sistem pengkabelan telekomunikasi perlu mendapat dan melalui proses kelulusan Jawatankuasa Kerja ICT (JKICT). b. Rekabentuk dan cadangan perkakasan sistem pengkabelan telekomunikasi perlu mendapat pengesahan oleh Seskyen Rangkaian dan Telekomunikasi IDEC melalui perkhidmatan sokongan yang diberikan (rujuk Prosedur Perkhidmatan Sokongan ICT (UPM/OPR/iDEC/P002)). **c.** Instalasi pengkabelan telekomunikasi tidak boleh dilaksanakan oleh mana-mana pihak tanpa kebenaran, kelulusan dan pengesahan Seskyen Rangkaian dan Telekomunikasi, IDEC.				**P**

		~~Rangkaian~~, IDEC.		
ISMS (IDEC): 25/2016	**iDEC**	Nama Dokumen: GARIS PANDUAN PENGURUSAN PENGAGIHAN RANGKAIAN Kod Dokumen:UPM/ISMS/OPR/~~NET/~~GP13/AGIHAN RANGKAIAN No. Isu:_01_, No. Semakan:_01_, Tarikh Kuatkuasa: 24/10/2014	Nama Dokumen: GARIS PANDUAN PENGURUSAN PENGAGIHAN RANGKAIAN Kod Dokumen:UPM/ISMS/OPR/~~NET/~~GP13/AGIHAN RANGKAIAN No. Isu:_01_, No. Semakan: 02_, Tarikh Kuatkuasa: 01/07/2016	**P**
ISMS (IDEC): 26/2016	**iDEC**	Nama Dokumen: GARIS PANDUAN PENYEDIAAN SWITCH RANGKAIAN Kod Dokumen:UPM/ISMS/OPR/~~NET/~~GP17/AGIHAN RANGKAIAN No. Isu:_01_, No. Semakan:_00_, Tarikh Kuatkuasa: 05/06/2016	Nama Dokumen: GARIS PANDUAN PENYEDIAAN SWITCH RANGKAIAN Kod Dokumen:UPM/ISMS/OPR/~~NET/~~GP17/AGIHAN RANGKAIAN No. Isu:_01_, No. Semakan: 02_, Tarikh Kuatkuasa: 01/07/2016	**P**
		1.0 TUJUAN Garis panduan ini disediakan untuk rujukan staf Seksyen Rangkaian yang terlibat dalam melaksanakan penyediaan switch rangkaian di Universiti Putra Malaysia.	**1.0 TUJUAN** Garis panduan ini disediakan untuk rujukan staf Seksyen Rangkaian dan Telekomunikasi yang terlibat dalam melaksanakan penyediaan switch rangkaian di Universiti Putra Malaysia.	**T**
		6.0 PERUBAHAN TERHADAP KONFIGURASI SWITCH RANGKAIAN Sebarang perubahan kepada konfigurasi switch rangkaian hanya akan dilaksanakan berdasarkan permohonan yang telah diluluskan daripada pegawai Seksyen Rangkaian dan perlu menggunapakai Prosedur Perkhidmatan Sokongan ICT (UPM/OPR/iDEC/P002).	**6.0 PERUBAHAN TERHADAP KONFIGURASI SWITCH RANGKAIAN** Sebarang perubahan kepada konfigurasi switch rangkaian hanya akan dilaksanakan berdasarkan permohonan yang telah diluluskan daripada pegawai Seksyen Rangkaian dan Telekomunikasi dan perlu menggunapakai Prosedur Perkhidmatan Sokongan ICT (UPM/OPR/iDEC/P002).	**T**
ISMS (IDEC): 27/2016	**iDEC**	Nama Dokumen: GARIS PANDUAN PENGURUSAN BACKUP PANGKALAN DATA Kod Dokumen:UPM/ISMS/OPR/~~PD/~~GP14/BACKUP No. Isu:_01_, No. Semakan:_03_, Tarikh Kuatkuasa: 23/01/2015	Nama Dokumen: GARIS PANDUAN PENGURUSAN BACKUP PANGKALAN DATA Kod Dokumen:UPM/ISMS/OPR/~~PD/~~GP14/BACKUP No. Isu:_01_, No. Semakan: 04_, Tarikh Kuatkuasa: 01/07/2016	**P**
		2.0 DOKUMEN RUJUKAN **Kod Dokumen** | **Tajuk Dokumen**	**2.0 DOKUMEN RUJUKAN** **Kod Dokumen** | **Tajuk Dokumen**	**P**

			-	***Garis Panduan Keselamatan Teknologi Maklumat & Komunikasi (GPKTMK)***			-	***Garis Panduan Keselamatan Teknologi Maklumat & Komunikasi (GPKTMK)***	
			~~UPM/SOK/ICT /P001~~	***Prosedur Penyelenggaraan ICT***			UPM/OPR/ IDEC/P003	***Prosedur Penyelenggaraan ICT***	
			UPM/ISMS/OPR/~~PD~~/AK02	***Arahan Kerja Pengurusan Backup***			UPM/ISMS/OPR/AK02	***Arahan Kerja Pengurusan Backup***	
			UPM/ISMS/OPR/~~PD~~/AK07	***Arahan Kerja Pelupusan Pita Backup***			UPM/ISMS/OPR/AK07	***Arahan Kerja Pelupusan Pita Backup***	
		3.0 PANDUAN Perlaksanaan Backup Data adalah diurus melalui proses dalam Prosedur Penyelenggaraan ICT (~~UPM/SOK/ICT/P001).~~					**3.0 PANDUAN** Perlaksanaan Backup Data adalah diurus melalui proses dalam Prosedur Penyelenggaraan ICT (UPM/OPR/IDEC/P003).		**P**
		3.4 Media Storan Media storan adalah terdiri daripada pita berjenis Digital Data Storage(DDS), Virtual Tape Library (VTL) atau lain-lain media yang sesuai. Rujuk Arahan Kerja Pengurusan Backup (UPM/ISMS/OPR/~~PD~~/AK02).					**3.4 Media Storan** Media storan adalah terdiri daripada pita berjenis Digital Data Storage(DDS), Virtual Tape Library (VTL) atau lain-lain media yang sesuai. Rujuk Arahan Kerja Pengurusan Backup (UPM/ISMS/OPR/AK02).		**P**
		4.0 PELAKSANAAN BACKUP DATA i. Pentadbir sistem aplikasi utama universiti perlu memohon perkhidmatan backup ii. melalui Borang Permohonan Perkhidmatan Sokongan ICT (OPR/iDEC/BR03/Sokongan ICT). **iii.** ii. Perlaksanaan backup data mestilah menggunakan semua proses dalam Prosedur Penyelenggaraan ICT (~~UPM/SOK/ICT/P001).~~					**4.0 PELAKSANAAN BACKUP DATA** iv. Pentadbir sistem aplikasi utama universiti perlu memohon perkhidmatan backup v. melalui Borang Permohonan Perkhidmatan Sokongan ICT (OPR/iDEC/BR03/Sokongan ICT). **vi.** ii. Perlaksanaan backup data mestilah menggunakan semua proses dalam Prosedur Penyelenggaraan ICT (UPM/OPR/IDEC/P003).		**P**
		7.0 PELUPUSAN MEDIA PITA BACKUP i. Perlaksanaan proses pelupusan adalah berdasarkan Garis Panduan Pelupusan Aset (SOK/KEW/GP020/AST) dan Arahan Kerja Pelupusan					**7.0 PELUPUSAN MEDIA PITA BACKUP** Perlaksanaan proses pelupusan adalah berdasarkan Garis Panduan Pelupusan Aset (SOK/KEW/GP020/AST) dan Arahan Kerja Pelupusan Pita Backup (UPM/ISMS/OPR /AK07).		**P**

<table>
<tr><td></td><td></td><td>Pita Backup (UPM/ISMS/OPR/~~PD~~/AK07).</td><td></td><td></td></tr>
<tr><td>ISMS (IDEC): 28/2016</td><td>iDEC</td><td>Nama Dokumen: GARIS PANDUAN PENGGUNAAN DATA PENGUJIAN
Kod Dokumen:UPM/ISMS/OPR/~~PD/~~GP15/DATA PENGUJIAN
No. Isu:_01_, No. Semakan:_00_, Tarikh Kuatkuasa: 09/11/2012</td><td>Nama Dokumen: GARIS PANDUAN PENGGUNAAN DATA PENGUJIAN
Kod Dokumen:UPM/ISMS/OPR/GP15/DATA PENGUJIAN
No. Isu:_01_, No. Semakan: 01_, Tarikh Kuatkuasa: 01/07/2016</td><td>P</td></tr>
<tr><td>ISMS (IDEC): 29/2016</td><td>iDEC</td><td>Nama Dokumen: GARIS PANDUAN PENGURUSAN UPM-ID
Kod Dokumen:UPM/ISMS/OPR/~~PD/~~GP16/UPM-ID
No. Isu:_01_, No. Semakan:_00_, Tarikh Kuatkuasa: 24/10/2014</td><td>Nama Dokumen: GARIS PANDUAN PENGURUSAN UPM-ID
Kod Dokumen:UPM/ISMS/OPR/~~PD/~~GP16/UPM-ID
No. Isu:_01_, No. Semakan: 01_, Tarikh Kuatkuasa: 01/07/2016</td><td>P</td></tr>
<tr><td></td><td></td><td>2.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Garis Panduan Keselamatan Teknologi Maklumat & Komunikasi (GPKTMK)</td></tr><tr><td>~~UPM/SOK/ICT /P001~~</td><td>Prosedur Penyelenggaraan ICT</td></tr></table></td><td>2.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Garis Panduan Keselamatan Teknologi Maklumat & Komunikasi (GPKTMK)</td></tr><tr><td>UPM/OPR/ IDEC/P003</td><td>Prosedur Penyelenggaraan ICT</td></tr></table></td><td></td></tr>
<tr><td></td><td></td><td>3.0 PANDUAN

Perlaksanaan Backup Data adalah diurus melalui proses dalam Prosedur Penyelenggaraan ICT (~~UPM/SOK/ICT/P001).~~</td><td>4.0 PANDUAN

Perlaksanaan Backup Data adalah diurus melalui proses dalam Prosedur Penyelenggaraan ICT (UPM/OPR/IDEC/P003).</td><td>P</td></tr>
<tr><td>ISMS (IDEC): 30/2016</td><td>iDEC</td><td>Nama Dokumen: GARIS PANDUAN PENGURUSAN UPM-ID
Kod Dokumen:UPM/ISMS/OPR/~~PD/~~GP16/UPM-ID
No. Isu:_01_, No. Semakan:_00_, Tarikh Kuatkuasa: 24/10/2014</td><td>Nama Dokumen: GARIS PANDUAN PENGURUSAN UPM-ID
Kod Dokumen:UPM/ISMS/OPR/~~PD/~~GP16/UPM-ID
No. Isu:_01_, No. Semakan: 01_, Tarikh Kuatkuasa: 01/07/2016</td><td>P</td></tr>
<tr><td></td><td></td><td>Senarai pelawat termasuk pemohon<table><tr><th>Nama</th><th>No.IC/ Passport</th><th>No. Pas ~~Pelawat (Diisi oleh pegawai bertugas)~~</th><th>Sila tanda sekiranya membawa peralatan persendirian?</th></tr><tr><td></td><td></td><td></td><td>☐</td></tr></table></td><td>Senarai pelawat termasuk pemohon<table><tr><th>Nama</th><th>No.IC/ Passport</th><th>No. Pas</th><th>Sila tanda sekiranya membawa peralatan persendirian?</th></tr><tr><td></td><td></td><td></td><td>☐ Nama :
☐ Kuantiti :
☐ Aset ID/No. Siri :</td></tr></table></td><td>P</td></tr>
</table>

		Pengesahan Pegawai Bertugas Dengan ini saya mengesahkan bahawa pemohon tidak membawa sebarang peralatan atau perkakasan yang tidak dibenarkan selain yang telah diisytiharkan ~~dalam Borang Penggunaan Peralatan ICT Persendirian.~~	**Pengesahan Pegawai Bertugas** Dengan ini saya mengesahkan bahawa pemohon tidak membawa sebarang peralatan atau perkakasan yang tidak dibenarkan selain yang telah diisytiharkan seperti diatas.	**P**

LAMPIRAN 7

MESYUARAT JAWATANKUASA KERJA KEDUA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
MS ISO/IEC/27001:2013

LAPORAN PELAKSANAAN ISMS PASUKAN PUSAT DATA

1. TUJUAN

Laporan ini bertujuan untuk memaklumkan pihak Jawatankuasa Kerja Sistem Pengurusan Keselamatan Maklumat (ISMS) ISO/IEC 27001 tentang perkembangan pelaksanaan Sistem Pengurusan Keselamatan Maklumat (ISMS) di Pusat Data Universiti Putra Malaysia.

2. LATARBELAKANG

Pusat Data Universiti Putra Malaysia (UPM) telah menerima pengiktirafan Pensijilan MS ISO/IEC 27001:2007 pada 4 Januari 2013 dan seterusnya menerima pengiktirafan Pensijilan ISO/IEC 27001:2013 pada Mac 2015. Skop pensijilan Pusat Data UPM meliputi sistem dan operasi yang terlibat di dalam skop pensijilan termasuk perkakasan, perisian, sistem utiliti, rangkaian dan keselamatan.

3. LAPORAN

3.1 DOKUMENTASI

Sebanyak 53 dokumen direkodkan melibatkan prosedur, garis panduan, arahan kerja, borang, dan log yang meliputi pengurusan di pusat data (pusat data,rangkaian, pangkalan data dan keselamatan ICT). Rujuk jadual di bawah untuk pembahagian kelas dokumen:

Bil.	Kelas Dokumen	Bilangan
1.	Prosedur	5
2.	Garis Panduan	20
3.	Arahan Kerja	6
4.	Borang	9
5.	Log	13
Jumlah		**53**

3.2 KAWALAN AKSES

Pelaksanaan kawalan akses Pusat Data menggunakan sistem akses e-jari berasaskan biometrik di setiap pintu masuk ke Pusat Data UPM. Setiap pelawat dan pembekal yang berurusan dengan Pusat Data UPM yang datang perlu mengisi borang pendaftaran pelawat atau pembekal.

Penggunaan Sistem Pengurusan Pusat Data (drcim.upm.edu.my) juga telah meningkatkan kecekapan dalam proses kawalan akses di Pusat Data UPM.

Statistik kemasukan pelanggan ke Pusat Data UPM merekodkan sebanyak 364 akses bagi tahun 2016 (sehingga Mei) yang terdiri daripada pelawat rasmi dan pembekal. Sehingga Mei 2016 sebanyak 6 pembekal berdaftar secara rasmi di Pusat Data UPM bagi menjalankan kerja-kerja penyelenggaraan berkala ketika ini.

3.3 ASET

Aset yang direkodkan adalah melibatkan perkakasan dan perisian bagi sistem yang terlibat di dalam skop pensijilan termasuk peralatan rangkaian, keselamatan, sistem kebakaran dan sistem utiliti di Pusat Data UPM.

3.4 INFRASTRUKTUR DAN KAWALAN

Sepanjang pelaksaaan ISMS, beberapa penambahbaikan ke atas infrastruktur dan kawalan ke atas Pusat Data UPM telah dilaksanakan bagi memenuhi keperluan dan tindakan pembetulan hasil dapatan audit yang telah dijalankan. Berikut disenaraikan penambahbaikan dan pelaksanaan tindakan yang telah dijalankan ke atas Pusat Data UPM:

BIL.	PENAMBAHBAIKAN	PELAKSANAAN TINDAKAN
1.	Sistem UPS	Naik taraf sistem bekalan kuasa 180kVA kepada 300kVA
2.	Bekalan kuasa kecemasan (Generator)	Naik taraf sistem bekalan kuasa kecemasan kepada 200kVA

3.	Sistem Kawalan Akses	i. Naik taraf sistem kawalan akses Biometrik ii. Pendaftaran pelawat iii. Pendaftaran pembekal
4.	Bilik Persediaan (*Staging Room)*	Naik taraf kemudahan di bilik persediaan
5.	CCTV	Menambah ruang storan sistem CCTV Pusat Data
6.	Almari bekunci	Penggunaan almari berkunci kepada pelawat Pusat Data UPM
7.	Sistem Prngurusan Pusat Data (drcim.upm.edu.my)	Penggunaan sistem bagi menguruskan operasi Pusat Data (Pengurusan Aset, Pengurusan Rak Server, Temujanji, Rekod Kawalan Akses).

4. SYOR

Ahli Mesyuarat dengan segala hormatnya dimohon untuk mengambil maklum berhubung pelaksanaan Sistem Pengurusan Keselamatan Maklumat (ISMS) di Pusat Data Universiti Putra Malaysia.

LAMPIRAN 8

MESYUARAT JAWATANKUASA KERJA KEDUA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
MS ISO/IEC 27001:2013

KERTAS MAKLUMAN
LAPORAN PENEMUAN AUDIT DALAMAN SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS) TAHUN 2016

1. TARIKH AUDIT

Audit Dalaman Sistem Pengurusan Keselamatan Maklumat (ISMS) Universiti Putra Malaysia (UPM) 2016 telah dijalankan pada 3 hingga 5 Mei 2016.

2. TUJUAN AUDIT

Audit Dalaman dijalankan untuk menentukan sama ada UPM:

i. melaksanakan pengurusan keselamatan maklumat berdasarkan keperluan Standard MS ISO/IEC 27001:2013 dengan efektif selaras dengan Peraturan Keselamatan ICT UPM serta objektif dan sasaran Sistem Pengurusan Keselamatan Maklumat UPM; dan

ii. bersedia untuk menghadapi Audit Pemantauan Semakan 1 oleh Badan Pensijilan.

3. KRITERIA AUDIT

Audit Dalaman dijalankan berdasarkan dokumen dan rujukan berikut:

i. Standard MS ISO/IEC 27001:2013
ii. Dokumentasi ISMS UPM
iii. Akta dan Peraturan berkaitan
iv. Rujukan lain yang dinyatakan dalam Manual Kualiti/Prosedur

4. KAEDAH AUDIT

Kaedah pelaksananaan Audit Dalaman merangkumi:

i. Lawatan tapak/tempat *(Site visit)*
ii. Pemerhatian

iii. Temubual
iv. Penilaian ke atas prosedur, rekod dan dokumen berkaitan
v. Pelaporan penemuan audit secara lisan dan bertulis.

5. SKOP AUDIT

Audit Dalaman dijalankan mengikut skop Sistem Pengurusan Keselamatan Maklumat UPM yang hanya melibatkan proses :

i. Sistem Pengurusan Keselamatan Maklumat hanya melibatkan proses Pendaftaran Pelajar Baharu Prasiswazah semasa Minggu Perkasa Putra dalam Sistem Maklumat Pelajar;

ii. Sistem Pengurusan Keselamatan Maklumat untuk Pengoperasian Pusat Data bagi proses Pendaftaran Pelajar Baharu Prasiswazah; dan

iii. Sistem Pengurusan Keselamatan Maklumat untuk Pengoperasian Pusat Pemulihan Bencana bagi proses Pendaftaran Pelajar Baharu Prasiswazah.

6. KUMPULAN AUDIT

Seramai 14 orang Juruaudit Dalaman ISMS UPM yang telah dibahagikan kepada tiga (3) kumpulan audit telah mengaudit proses dalam skop Sistem Pengurusan Keselamatan Maklumat UPM.

7. PROGRAM AUDIT DALAMAN

Program Audit Dalaman telah disediakan oleh Ketua Seksyen Audit Kualiti, Pusat Jaminan Kualiti UPM dan disahkan oleh Wakil Pengurusan UPM. Program Audit telah dimaklumkan kepada semua peneraju proses, pusat tanggungjawab dan Juruaudit Dalaman pada 26 April 2016.

8. PENEMUAN AUDIT

<u>Kekuatan</u>

i. Komitmen Pengurusan UPM, Pusat Jaminan Kualiti dan Peneraju Proses adalah tinggi dalam menyelaraskan dan melaksanakan Sistem Pengurusan Keselamatan Maklumat.
ii. Tahap dokumentasi adalah baik, memenuhi keperluan Standard MS ISO/IEC 27001:2013 dan mudah dicapai oleh semua staf menerusi portal e-ISO menggunakan id dan kata laluan (UPMID) masing-masing.

iii. Penilaian risiko (*risk assessment)* dan rawatan risiko (*risk treatment*) telah dilaksanakan dengan baik dan memenuhi keperluan Standard MS ISO/IEC 27001:2013.

iv. Pengoperasian Pusat Data Utama dan Pusat Pemulihan Bencana adalah pada tahap selamat dan memenuhi keperluan Standard MS ISO/IEC 27001:2013.

v. Amalan keselamatan maklumat adalah baik walaupun kefahaman dan pembudayaan terhadap ISMS dalam kalangan staf pelaksana masih boleh dipertingkatkan.

vi. Pemantauan dan tindakan terhadap ketakakuran dan cadangan penambahbaikan telah dilaksanakan oleh Pusat Jaminan Kualiti (CQA) dan Peneraju Proses dengan baik.

Kelemahan

i. Kawalan terhadap pengoperasian proses didapati kurang memuaskan.

ii. Kawalan terhadap maklumat terdokumen yang digunakan adalah kurang memuaskan dari segi kemaskini dan keselamatan.

iii. Komunikasi dari segi hebahan tentang kepentingan keselamatan maklumat masih kurang.

iv. Kefahaman tentang keselamatan maklumat masih bolehdipertingkatkan.

v. Staf yang melaksanakan tugas masih belum membudayakan amalan terbaik dalam keselamatan maklumat.

Cadangan

i. Kaedah kawalan id pengguna yang digunakan semasa Pendaftaran Pelajar Baharu perlu dipertingkatkan.

ii. Perancangan untuk perluasan skop ISMS dibuat secara terperinci dengan sasaran.

iii. Kursus untuk Juruaudit Dalaman diadakan kepada staf PTJ selain dari Pusat Pembangunan Maklumat dan Komunikasi

9. BILANGAN KETAKAKURAN DAN PELUANG PENAMBAHBAIKAN

Sebanyak 16 Laporan Ketakakuran dan 20 Peluang Penambahbaikan dicatatkan semasa Audit Dalaman Sistem Pengurusan Keselamatan Maklumat tahun 2016. Perincian Penemuan adalah seperti di **Lampiran A**.

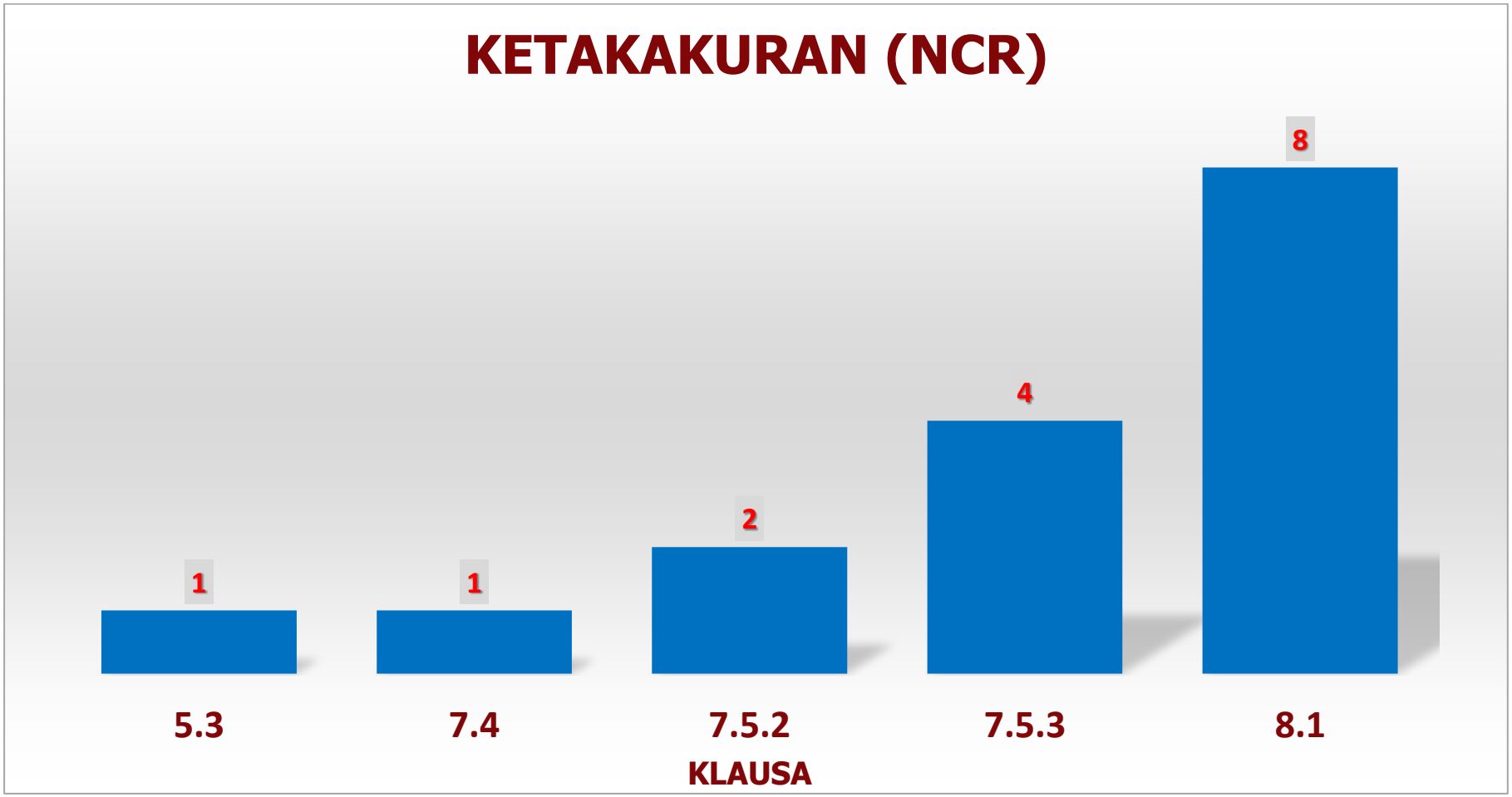
10. TARIKH TUTUP NCR

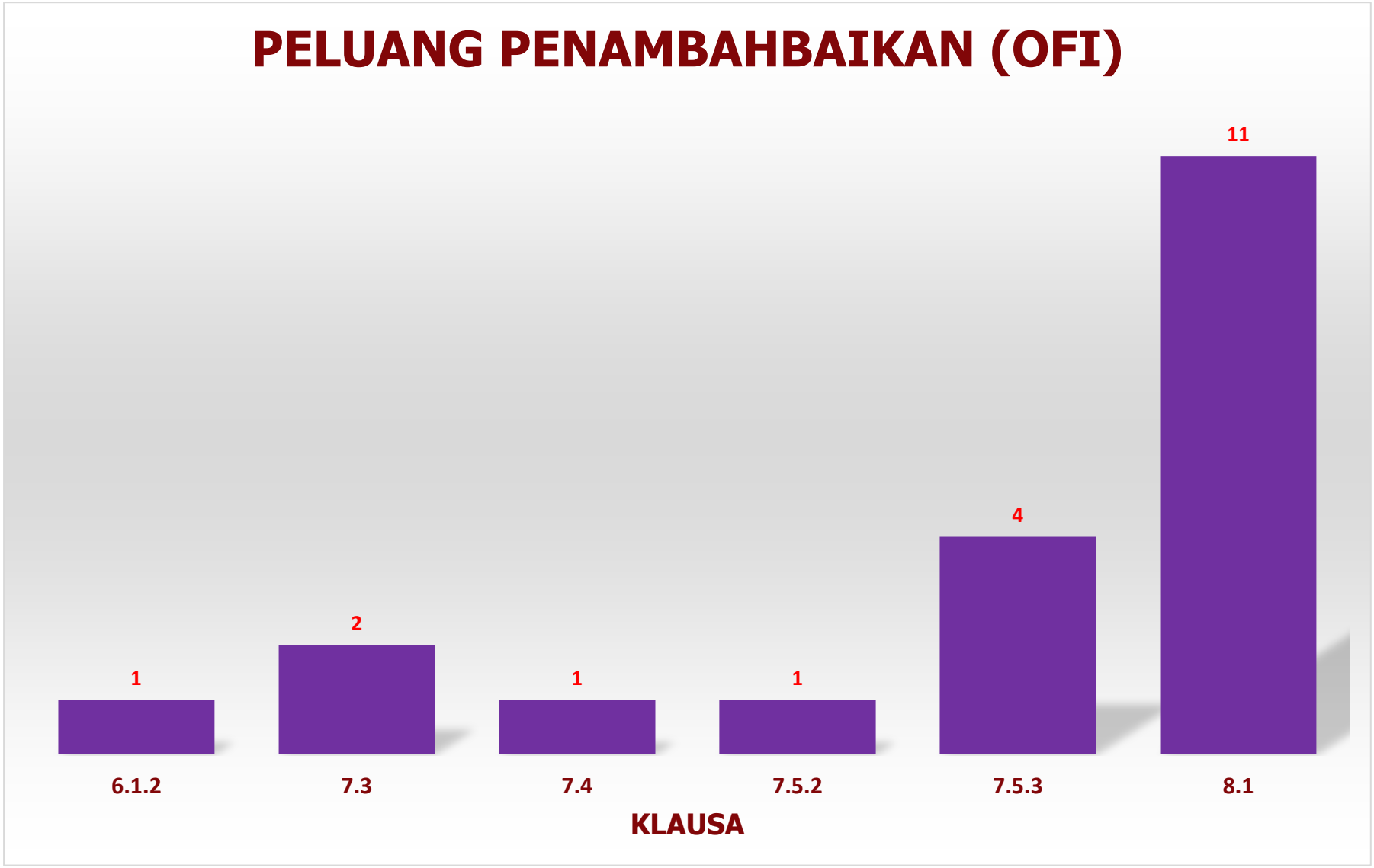
Semua ketakauran (NSR) hendaklah diambil tindakan dan ditutup dalam tempoh 21 hari bekerja atau pada tarikh yang telah dipersetujui oleh Juruaudit Dalaman UPM.

11. KESIMPULAN

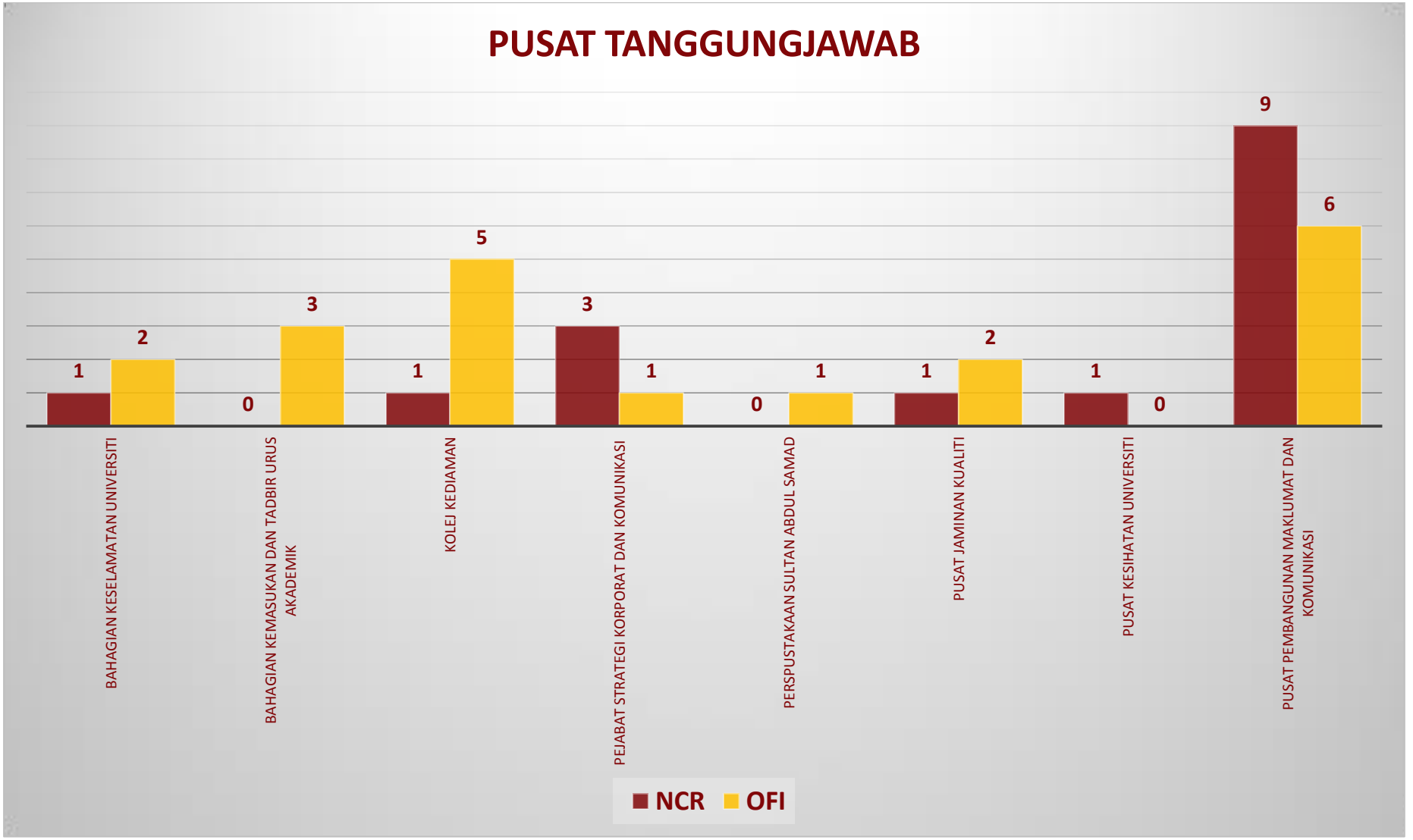
Hasil dari audit dalaman yang telah dijalankan, ketakakuran yang ditemui adalah menjurus kepada kawalan terhadap operasi perkhidmatan dan kawalan terhadap maklumat terdokumen.

Dari segi perlaksanaan ISMS, Universiti Putra Malaysia adalah bersedia untuk diaudit oleh badan pensijilan tertakluk kepada tindakan pembetulan yang berkesan diambil terhadap ketakakuran yang ditemui dalam masa yang telah ditetapkan.


KETAKAKURAN (NCR)
1
1
2
4
8
5.3
7.4
7.5.2
7.5.3
8.1
KLAUSA


PELUANG PENAMBAHBAIKAN (OFI)
1
2
1
1
4
11
6.1.2
7.3
7.4
7.5.2
7.5.3
8.1
KLAUSA

Lampiran A


PUSAT TANGGUNGJAWAB
1
2
0
3
1
5
3
1
0
1
1
2
1
0
9
6
BAHAGIAN KESELAMATAN UNIVERSITI
BAHAGIAN KEMASUKAN DAN TADBIR URUS AKADEMIK
KOLEJ KEDIAMAN
PEJABAT STRATEGI KORPORAT DAN KOMUNIKASI
PERSPUSTAKAAN SULTAN ABDUL SAMAD
PUSAT JAMINAN KUALITI
PUSAT KESIHATAN UNIVERSITI
PUSAT PEMBANGUNAN MAKLUMAT DAN KOMUNIKASI
NCR
OFI

LAMPIRAN 9

MESYUARAT JAWATANKUASA KERJA KEDUA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
MS ISO/IEC 27001:2013

KERTAS MAKLUMAN
PERANCANGAN MENGADAKAN SOAL SELIDIK PENDAFTARAN PELAJAR BAHARU PRASISWAZAH SEMASA MINGGU PERKASA PUTRA DI UNIVERSITI PUTRA MALAYSIA

1.0 TUJUAN

Kertas ini ini bertujuan untuk memaklumkan ahli Mesyuarat Jawatankuasa Kerja ISMS berkaitan cadangan mengadakan soal selidik mengenai kerahsiaan, integriti, kebolehsediaan dan kepuasan perkhidmatan pendaftaran dalam kalangan pelajar baharu prasiswazah yang mendaftar semasa Minggu Perkasa Putra di Universiti Putra Malaysia pada Sesi Kemasukan 2016/2017 akan datang.

2.0 LATAR BELAKANG

Pelaksanaan soal selidik ini adalah berdasarkan kepada saranan dalam Mesyuarat Kajian Semula Pengurusan (MKSP) Sistem Pengurusan Keselamatan Maklumat (ISMS) Kali Keempat pada 27 November 2015 yang mencadangkan supaya kajian dibuat bagi proses pendaftaran pelajar baharu dengan mengedarkan borang kajian kepada pihak yang berkepentingan dengan skop baharu seperti pelajar atau ibubapa. Tujuan pelaksanaan soal selidik ini adalah untuk mengetahui tahap penerimaan kerahsiaan, integriti, kebolehsediaan dan kepuasan perkhidmatan pendaftaran dalam kalangan pelajar. Persepsi pelajar baharu yang juga merupakan pemegang taruh ini akan mencerminkan tahap perlaksanaan ISMS di proses pendaftaran pelajar baharu di Universiti Putra Malaysia.

3.0 OBJEKTIF PELAKSANAAN SOAL SELIDIK

Objektif perlaksanaan soal selidik adalah untuk mendapat maklumbalas pemegang taruh (pelajar baharu) mengenai keberkesanan pelaksanan ISMS di UPM seperti berikut:

i. Tahap kepercayaan pelajar kepada kerahsiaan maklumat yang diberikan kepada universiti semasa pendaftaran

ii. Tahap ketepatan maklumat dalam surat tawaran universiti kepada pelajar berkaitan nama, no. kad pengenalan, program pengajian ditawarkan dan penempatan kolej

iii. Tahap kesediaan setiap kaunter yang melayan anda semasa proses pendaftaran

iv. Tahap kepuasan anda semasa berurusan dengan semua kaunter pendaftaran pelajar

4.0 CADANGAN PELAKSANAAN

Kajian soal selidik ini akan dijalankan pada hari pendaftaran pelajar baharu prasiswazah bagi sesi kemasukan 2016/2017 yang dijadualkan akan dilaksanakan pada 31 Ogos 2016 (Sabtu).

Soalan-soalan kajian yang bakal diajukan adalah berdasarkan tahap mengenai kerahsiaan, integriti, kebolehsediaan dan kepuasan perkhidmatan pendaftaran pelajar baharu terhadap jenis perkhidmatan yang diterima daripada setiap peneraju/entiti yang menawarkan perkhidmatan. Respon pemegang taruh adalah berdasarkan tahap kepuasan mereka mengikut skala 1 hingga 5 yang telah ditetapkan.

Kaedah pelaksanaan soal selidik adalah secara atas talian di mana *wokstation* soal selidik akan ditempatkan di setiap kolej kediaman semasa hari pendaftaran pelajar baharu. Pelajar akan menjawab soal selidik berkenaan selepas menyempurnakan semua kaunter pendaftaran.

Pelaksanaan soal selidik ini akan mendapat kerjasama daripada beberapa PTJ Universiti seperti Bahagian Kemasukan dan Tadbir Urus Akademik, Bahagian Hal Ehwal Pelajar, Kolej kediaman dan Pusat Pembangunan dan Teknologi Maklumat (IDEC).

5.0 SYOR

Semua ahli Mesyuarat Jawatankuasa Kerja ISMS adalah diminta mengambil mengambil maklum pelaksanaan Soal Selidik Pendaftaran Pelajar Baharu Prasiswazah Semasa Minggu Perkasa Putra di setiap kolej kediaman.

LAMPIRAN 10

AUDIT PENSIJILAN SEMULA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
MS ISO/IEC 27001:2013
UNIVERSITI PUTRA MALAYSIA
08 – 10 DISEMBER 2015

(Dikemaskini: 14 Jun 2016)

PELAN TINDAKAN PADA PELUANG PENAMBAHBAIKAN	
Pusat Tanggungjawab	**Bahagian Pengurusan Sumber Manusia, Pejabat Pendaftar**
No. OFI	**1**
Klausa	**A.7.1.1 Screening**
Butiran Peluang Penambahbaikan: Saringan keselamatan untuk Pengawal Keselamatan perlu dilihat kembali bagi memastikan mereka di akses bagi mengurangkan sebarang risiko dan ancaman kepada organisasi. Dokumen prosedur atau garis panduan juga perlu dikemaskini bagi memperlihatkan kategori anggota kerja yang perlu menjalani saringan keselamatan.	

PELAKSANAAN TINDAKAN	**DOKUMEN SOKONGAN BERKAITAN SEBAGAI BUKTI PELAKSANAAN**
	Status: ▪ Pelan Tindakan - x ▪ Bukti Tindakan dihantar ke CQA - x

AUDIT PENSIJILAN SEMULA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
MS ISO/IEC 27001:2013
UNIVERSITI PUTRA MALAYSIA
08 – 10 DISEMBER 2015

PELAN TINDAKAN PADA PELUANG PENAMBAHBAIKAN

Pusat Tanggungjawab	**Bahagian Perkhidmatan Sumber Manusia, Pejabat Pendaftar**
No. OFI	**2**
Klausa	**A.8.2.1 Classification of information**

Butiran Peluang Penambahbaikan:

Didapati pemakaian borang-borang tidak mengandungi dokumentasi klasifikasi. Ini boleh dilihat kembali bagi memastikan sebarang borang yang memiliki sentiviti informasi atau peribadi dapat dijaga dan diatur melalui prosedur yang sepatutnya. (Bahagian Keselamatan : Borang Permohonan Kad Pelajar dan Kolej : Borang Maklumat Peribadi Pelajar)

PELAKSANAAN TINDAKAN	DOKUMEN SOKONGAN BERKAITAN SEBAGAI BUKTI PELAKSANAAN
Pejabat pendaftar telah mengeluarkan hebahan Buletin bertarikh 7 Oktober 2015 daripada Encik Ramli bin Sulong, Ketua, Bahagian Perkhidmatan Sumber Manusia, berkaitan "Klasifikasi Fail Am dan Fungsian Universiti Putra Malaysia". Setelah perbincangan dibuat bersama CQA proses pengemaskinian kod klasifikasi fail perlu dikemaskini oleh semua PTJ diberi keutamaan kepada dokumen yang berkaitan dengan ISO. Melalui Mesyuarat Adhoc Jawatan kuasa Pengurusan Rekod telah bersetuju proses pengemaskinian ini dilakukan melalui kawalan rekod yang diterajui oleh Pusat Jaminan Kualiti (CQA). Pada 5 Februari 2016 Pusat Jaminan Kualiti (CQA) telah mengeluarkan arahan supaya Peneraju yang berkaitan Skop Utama dan SkopSokongan ISO UPM melaksanakan pengumpulan senarai Klasifikasi Fail ISO bagi tujuan mengemaskini kod failing tersebut berpandukan Panduan Pengurusan Fail dan Rekod Universiti sebagai dokumen rujukan. Proses pengemaskinian kod filing sedang dilaksanakan oleh semua PTJ yang terlibat.	1. Emel berkaitan Klasifikasi Fail Sistem Pengurusan ISO PTJ kepada Peneraju Skop Utama dan Sokongan ISO UPM Status: ▪ Pelan Tindakan - √ ▪ Bukti Tindakan dihantar ke CQA - √

AUDIT PENSIJILAN SEMULA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
MS ISO/IEC 27001:2013
UNIVERSITI PUTRA MALAYSIA
08 – 10 DISEMBER 2015

PELAN TINDAKAN PADA PELUANG PENAMBAHBAIKAN

Pusat Tanggungjawab	**Bahagian Keselamatan**
No. OFI	**3**
Klausa	**A.8.2.3 Handling of assets**

Butiran Peluang Penambahbaikan:

Borang untuk permohonan kad pelajar dilihat mengandungi nama penuh dan no kad pengenalan pelajar, difahamlan borang ini menjadi kertas kitar semula (recycle paper). Menerusi prosedur simpanan borang haruslah dalam tempoh 4 tahun. Pemilik proses perlu melihat kembali akan kawalan ini bagi mengelakkan isu pelanggaran sekuriti.

PELAKSANAAN TINDAKAN	DOKUMEN SOKONGAN BERKAITAN SEBAGAI BUKTI PELAKSANAAN
	Status: ▪ Pelan Tindakan - x ▪ Bukti Tindakan dihantar ke CQA - x

AUDIT PENSIJILAN SEMULA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
MS ISO/IEC 27001:2013
UNIVERSITI PUTRA MALAYSIA
08 – 10 DISEMBER 2015

PELAN TINDAKAN PADA PELUANG PENAMBAHBAIKAN

Pusat Tanggungjawab	**Kolej**
No. OFI	**4**
Klausa	**A.11.2.1 Equipment siting and protection**

Butiran Peluang Penambahbaikan:

Didapati untuk Borang Maklumat Peribadi Pelajar yang sudah bergaduan diletakkan di dalam Stor Kolej. Lokasi bagi meletakkan borang tersebut yang mengandungi maklumat peribadi pelajar boleh dilihat kembali bagi menghindarkan dari segi risiko di akses oleh anggota yang tidak berkaitan.

PELAKSANAAN TINDAKAN	DOKUMEN SOKONGAN BERKAITAN SEBAGAI BUKTI PELAKSANAAN
Surat makluman ke semua kolej berkaitan arahan bagi perkara berikut; a) Melupus fail pelajar yang telah bergraduat dengan cara merincih. b) Bagi fail peribadi yang sedang dalam proses untuk dirincih dan disimpan dalam stor, ia perlu disimpan dalam laci berkunci atau menghadkan akses stor kepada pegawai stor terbabit sahaja. Bagi fail pelajar bergraduat yang sedia ada, jangkaan masa pelaksanaan ialah sepanjang Semester 2 Sesi 2015/2016.	Surat edaran oleh Timbalan Wakil Pengurusan (Kolej) ke semua kolej pada 27 April 2016 berkaitan Pengurusan Fail Peribadi Pelajar Bergraduat. Status: ▪ Pelan Tindakan - √ ▪ Bukti Tindakan dihantar ke CQA - √

AUDIT PENSIJILAN SEMULA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
MS ISO/IEC 27001:2013
UNIVERSITI PUTRA MALAYSIA
08 – 10 DISEMBER 2015

PELAN TINDAKAN PADA PELUANG PENAMBAHBAIKAN

Pusat Tanggungjawab	**Bahagian Keselamatan**
No. OFI	**5**
Klausa	**A.12.1.3 Capacity management**

Butiran Peluang Penambahbaikan:

Difahamkan pengeluaran kad pelajar hanya berlaku dalam tempoh 2 bulan selepas pelajar mendaftar di Minggu Perkasa Putra. Organisasi boleh melihat kembali dari segi pengurusan kapasiti bagi memastikan kemampuan anggota kerja untuk proses pengeluaran ke atas kad pelajar. Selain dari itu kad pelajar juga dilihat sebagai lambang identiti pelajar dan merupakan pengenalan diri dan dilihat dari segi sekuriti akan memberikan impak keselamatan kepada organisasi.

PELAKSANAAN TINDAKAN	DOKUMEN SOKONGAN BERKAITAN SEBAGAI BUKTI PELAKSANAAN
	Status: ▪ Pelan Tindakan - x ▪ Bukti Tindakan dihantar ke CQA - x

AUDIT PENSIJILAN SEMULA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
MS ISO/IEC 27001:2013
UNIVERSITI PUTRA MALAYSIA
08 – 10 DISEMBER 2015

PELAN TINDAKAN PADA PELUANG PENAMBAHBAIKAN	
Pusat Tanggungjawab	**Pejabat Penasihat Undang-undang**
No. OFI	**6**
Klausa	**A.13.2.4 Confidentiality or non disclosure agreements**
Butiran Peluang Penambahbaikan: Bahagian Penasihat Undang- Undang boleh menambahbaik dari segi meneliti akan perjanjian ke atas kontrak- kontrak yang melibatkan penerimaan dan pertukaran maklumat.	

PELAKSANAAN TINDAKAN	**DOKUMEN SOKONGAN BERKAITAN SEBAGAI BUKTI PELAKSANAAN**
Pejabat Penasihat Undang-Undang menambahbaik senarai semak sedia ada dan digunapakai bermula pada 1hb Mac 2016.	Senarai Semak Surat Cara Undang-undang (Perjanjian/Persefahaman). Status: ▪ Pelan Tindakan - √ ▪ Bukti Tindakan dihantar ke CQA - √

AUDIT PENSIJILAN SEMULA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
MS ISO/IEC 27001:2013
UNIVERSITI PUTRA MALAYSIA
08 – 10 DISEMBER 2015

PELAN TINDAKAN PADA PELUANG PENAMBAHBAIKAN

Pusat Tanggungjawab	**Pasukan Penilaian Risiko**
No. OFI	**7**
Klausa	**A.16.1.2 Reporting information security events**

Butiran Peluang Penambahbaikan:

Tidak ada laporan insiden yang dilaporkan untuk tempoh Feb 2015 sehingga tarikh audit dijalankan. Garis panduan berkenaan insiden telah dibangunkan dan digunapakai oleh organisasi. Walaubagaimanapun kefahaman mengenai definisi insiden di dalam organisasi dan kesedaran untuk melaporkan insiden yang menepati definisi tersebut oleh semua pihak yang terlibat boleh ditambahbaik.

PELAKSANAAN TINDAKAN	DOKUMEN SOKONGAN BERKAITAN SEBAGAI BUKTI PELAKSANAAN
Definisi insiden keselamatan ICT telah di nyatakan di dalam prosedur tindak balas insiden ICT dan disenaraikan insiden yang mungkin akan/boleh berlaku di dalam organisasi. Sebarang insiden keselamatan ICT akan dilaporkan kepada pemilik proses dan Jawatankuasa Komunikasi Krisis dengan kadar segera menerusi kaedah yang telah ditetapkan untuk tujuna hebahan.	Prosedur tindak balas insiden ICT (UPM/ISMS/SOK/P001) : Perkara 5.0 Mekanisma pelaporan Status: ▪ Pelan Tindakan - √ ▪ Bukti Tindakan dihantar ke CQA - √

AUDIT PENSIJILAN SEMULA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
MS ISO/IEC 27001:2013
UNIVERSITI PUTRA MALAYSIA
08 – 10 DISEMBER 2015

PELAN TINDAKAN PADA PELUANG PENAMBAHBAIKAN

Pusat Tanggungjawab	**Pusat Kesihatan Universiti**
No. OFI	**8**
Klausa	**6.1.2 Information security risk assessment**

Butiran Peluang Penambahbaikan:

Laporan penilaian dan pentaksiran risiko telah dibangunkan (dibawah Pusat Kesihatan Universiti), namun begitu laporan ini perlu ditambahbaik berdasarkan isu masa CCTV yang tidak selaras berikutan berlaku gangguan bekalan tenaga elektrik.

PELAKSANAAN TINDAKAN	DOKUMEN SOKONGAN BERKAITAN SEBAGAI BUKTI PELAKSANAAN
Pusat Kesihatan Universiti akan mewujudkan log pemantauan masa CCTV yang akan dilakukan 2 kali seminggu. Penggunaan log ini akan berkuatkuasa pada 1 Januari 2016.	1. Borang Log Pemantauan Masa CCTV Status: ▪ Pelan Tindakan - √ ▪ Bukti Tindakan dihantar ke CQA - √

AUDIT PENSIJILAN SEMULA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
MS ISO/IEC 27001:2013
UNIVERSITI PUTRA MALAYSIA
08 – 10 DISEMBER 2015

PELAN TINDAKAN PADA PELUANG PENAMBAHBAIKAN

Pusat Tanggungjawab	**Pasukan Penilaian Risiko & Pusat Kesihatan Universiti**
No. OFI	**9**
Klausa	**6.1.3 Information security risk treatment**

Butiran Peluang Penambahbaikan:

Penilaian risko untuk aset 'Laporan Pemeriksaan Kesihatan' (dibawah Pusat Kesihatan Universiti) dan untuk aset bagi Pengurusan Kolej telah dilaksanakan, walaubagaimanapun penguraian risiko untuk aset tersebut perlu disemak semula.

PELAKSANAAN TINDAKAN	DOKUMEN SOKONGAN BERKAITAN SEBAGAI BUKTI PELAKSANAAN
Pusat Kesihatan Universiti Memasukkan pernyataan dibawah ke dalam planned saveguards ke dalam sistem Myram 1. Mewujudkan modul medical checkup didalam sistem eklinik2 dan data akan disimpan secara online. 2. Modul dijangkakan dapat digunapakai pada September 2016.	1. Sistem Myram yang telah dikemaskini Status: ▪ Pelan Tindakan - √ ▪ Bukti Tindakan dihantar ke CQA - √
Pasukan Penilaian Risiko	Status: ▪ Pelan Tindakan - x ▪ Bukti Tindakan dihantar ke CQA - x

AUDIT PENSIJILAN SEMULA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
MS ISO/IEC 27001:2013
UNIVERSITI PUTRA MALAYSIA
08 – 10 DISEMBER 2015

PELAN TINDAKAN PADA PELUANG PENAMBAHBAIKAN

Pusat Tanggungjawab	**Bahagian Urus Tadbir Akademik & Pusat Pembangunan Maklumat dan Komunikasi**
No. OFI	**10**
Klausa	**8.1 Operational planning and control**

Butiran Peluang Penambahbaikan:

A.9.4.3 Password management system

Katalaluan untuk capaian Sistem Maklumat Pelajar telah ditetapkan kepada lapan (8) aksara(alphanumeric), walaubagaimanapun pengurusan katalaluan boleh ditambahbaik selaras dengan Garis Panduan Pengurusan Identiti.

PELAKSANAAN TINDAKAN	DOKUMEN SOKONGAN BERKAITAN SEBAGAI BUKTI PELAKSANAAN
Bahagian Urus Tadbir Akademik BAKD telah melaksanakan Bengkel Pengurusan Identiti Pengguna (ID) dan Kata Laluan (PW) Sistem Maklumat Pelajar (SMP) pada 21 April 2016. Keputusan hasil bengkel berkenaan direkodkan ke dalam Catatan Perbincangan seperti disertakan	1. Catatan Perbincangan semasa Bengkel Pengurusan Identiti Pengguna (ID) dan Kata Laluan (PW) pada 21 April 2016. 2. Jadual Pelaksanaan (Timeline) Pembangunan Garis Panduan ID dan PW SMP Status: ▪ Pelan Tindakan - √ ▪ Bukti Tindakan dihantar ke CQA - √
Pusat Pembangunan Maklumat dan Komunikasi Mengemaskini dokumen garis panduan pengurusan identiti (UPM/ISMS/SOK/GP07/IDENTITI) dengan menambah keperluan pengurusan identiti bagi sistem aplikasi secara umum.	Garis panduan pengurusan identiti (UPM/ISMS/SOK/GP07/IDENTITI) Status: ▪ Pelan Tindakan - √ ▪ Bukti Tindakan dihantar ke CQA - √

STATUS TINDAKAN LAPORAN PELUANG PENAMBAHBAIKAN (OFI)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS) ISO/IEC 27001:2013 AUDIT BADAN PENSIJILAN SIRIM
TAHUN 2015

DIKEMASKINI: 14 Jun 2016

Bil.	Pusat Tanggungjawab (PTJ)	BIL. OFI	No. OFI	Keputusan Tindakan (Ya / Tidak)	Pelan Tindakan	Bukti Tindakan	Status Tindakan
1	Bahagian Keselamatan	2	**No. 3**	**Ya**	**X**	**X**	**X**
			No. 5	**Ya**	**X**	**X**	**X**
2	Bahagian Urus Tadbir Akademik	1	**No. 10** (Tindakan bersama IDEC)	**Ya**	**√**	**√**	**√**
3	Pusat Pembangunan Maklumat dan Komunikasi (iDEC)	3	**No. 7 -** Pasukan Penilaian Risiko	**Ya**	**√**	**√**	**√**
			No. 9 (Tindakan bersama PKU & Pasukan Penilaian Risiko)	**Ya**	**X**	**X**	**X**
			No. 10 (Tindakan bersama iDEC & Bah. Urus Tadbir Akad)	**Ya**	**√**	**√**	**√**
4	Kolej Kediaman	1	**No. 4**	**Ya**	**√**	**√**	**√**
5	Pejabat Penasihat Undang-undang	1	**No. 6**	**Ya**	**√**	**√**	**√**
6	Pejabat Pendaftar	2	**No. 1**	**Ya**	**X**	**X**	**X**
			No. 2	**Ya**	**√**	**√**	**√**
7	Pusat Kesihatan Universiti	2	**No. 8**	**Ya**	**√**	**√**	**√**
			No. 9 (Tindakan bersama PKU & IDEC)	**Ya**	**√**	**√**	**√**
JUMLAH OFI		**10**	**JUMLAH OFI DITERIMA**	**10**	**JUMLAH OFI TUTUP**		**6**
					PERATUS PENUTUPAN (%)		**60**

LAMPIRAN 11

CADANGAN KAJIAN SOAL SELIDIK PROSES PENDAFTARAN PELAJAR BAHARU SESI KEMASUKAN 2016/2017

1. Maklumat Demografi

i. Jantina
ii. Kolej kediaman

2. Cadangan Soalan Soal Selidik

Bil	Soalan	Pencapaian Skala				
		1 (Sangat Tidak Memuaskan)	**2 (Tidak memuaskan)**	**3 (Kurang Memuaskan)**	**4 (Memuaskan)**	**5 (Sangat memuaskan)**
1.	Tahap kepercayaan anda kepada kerahsiaan maklumat yang anda serahkan kepada universiti semasa pendaftaran					
2.	Tahap ketepatan maklumat dalam surat tawaran universiti kepada anda berkaitan nama, no. kad pengenalan, program pengajian ditawarkan dan penempatan kolej					
3.	Tahap kesediaan setiap kaunter yang melayan anda semasa proses pendaftaran					
4.	Tahap kepuasan anda semasa berurusan dengan kaunter bendahari ketika menyerah slip/pembayaran yuran					
5.	Tahap kepuasan anda semasa berurusan dengan kaunter Keselamatan ketika penyerahan borang permohonan kad matrik					
6.	Tahap kepuasan anda semasa berurusan dengan kaunter Kolej Kediaman ketika pengambilan kunci bilik penginapan					