



**KERTAS UNTUK MAKLUMAN
MESYUARAT JAWATANKUASA KUALITI UPM KALI KE-38**

**LAPORAN PENILAIAN RISIKO DAN PELAN PEMULIHAN RISIKO
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS) MS ISO/IEC
27001:2013 TAHUN 2017 (SEMAKAN SEPTEMBER 2017)**

1. TUJUAN

Kertas ini adalah bertujuan untuk mendapat pertimbangan dan kelulusan ahli Mesyuarat Jawatankuasa Kualiti Universiti Putra Malaysia Kali Ke-38 berkaitan Laporan Hasil Penilaian Risiko dan Pelan Pemulihan Risiko Sistem Pengurusan Keselamatan Maklumat (ISMS) UPM bagi semakan September 2017.

2. LATARBELAKANG

Penilaian risiko dilaksanakan dengan tujuan untuk menilai tahap risiko aset yang terlibat dalam proses melibatkan skop ISMS supaya pendekatan dan keputusan yang paling berkesan dikenalpasti bagi menyediakan perlindungan dan kawalan ke atas risiko aset berkenaan, berasaskan metodologi Penilaian Risiko Terperinci MyRAM (*Malaysian Public Sector ICT Risk Assessment Methodology*). Pengemaskinian MyRAM dilaksanakan apabila berlaku perubahan atau penambahan aset di dalam skop ISMS yang terlibat. Aset dinilai samada rendah (low), sederhana (medium) atau tinggi (high) berdasarkan ciri utama keselamatan iaitu kerahsiaan (confidentiality), integriti (integrity) dan ketersediaan (availability). Risiko yang telah dikenalpasti akan dilaksanakan tindakan kawalan dan pemulihan risiko sepertimana berikut:

Cadangan	Keterangan
MENGURANGKAN	Keputusan ini ditentukan sekiranya implikasi terhadap risiko adalah kritikal samada HIGH atau MEDIUM. Pengurangan risiko dapat dilaksanakan melalui penambahbaikan dari segi operasi, prosedur, fizikal, individu atau teknikal.
MEMINDAHKAN	Keputusan ini ditentukan sekiranya implikasi terhadap

	risiko tersebut boleh dipindahkan dengan mewujudkan perjanjian (SLA) antara kedua pihak.
MENERIMA	Keputusan ini ditentukan jika implikasi terhadap risiko adalah LOW.
MENGELAKKAN	Keputusan ini ditentukan kerana tiada kawalan yang dapat ditentukan samada untuk mengurangkan atau memindahkan risiko kepada pihak ketiga.

3. LAPORAN

Perincian Laporan Hasil Penilaian Risiko dan Plan Pemulihan Risiko Sistem Pengurusan Keselamatan Maklumat yang dijalankan pada September 2017 adalah seperti pada **Lampiran 1**.

4. SYOR

Ahli mesyuarat diminta mengambil tindakan sepertimana berikut:

- i) mengambil maklum hasil penilaian risiko dan plan pemulihan risiko Sistem Pengurusan Keselamatan Maklumat (ISMS) semakan September 2017;
- ii) mengambil perhatian berhubung bilangan tahap risiko dan punca dominan yang dikenalpasti serta tindakan kawalan dan plan pemulihan risiko yang digunakan oleh peneraju dalam menyediakan perlindungan ke atas risiko berkenaan.

LAPORAN PENILAIAN RISIKO DAN PELAN PEMULIHAN RISIKO SEMAKAN SEPTEMBER 2017

Bil	Nama Proses	Bil Aset	Bil Ancaman	Bil. Tahap Risiko			Punca Dominan	Kawalan Sediaada	Pelan Pemulihan Risiko
				L	M	H			
1.	Kad Pelajar Baharu Siswazah	12	21	21	0	0	Bilik kad pintar tiada penyelenggaraan kebakaran	Penyelenggaraan berkala Alat Pemadam Api	Penyelenggaraan berkala Alat Pemadam Api dan latihan kebakaran.
2.	Pengesahan Laporan Pemeriksaan Kesihatan Pelajar Baharu Prasiswazah	91	139	139	0	0	Pengendalian Borang Akuan Kesihatan dan Borang Akuan Bebas Dadah	Meletakkan Borang tersebut didalam kotak	-
3.	Pembayaran Yuran Pelajar Baharu Prasiswazah	17	24	7	17	0	Power Failure	Penggunaan <i>notebook</i> diutamakan kerana terdapat <i>power supply</i> dari bateri	Penggunaan UPS
4.	Pengesahan Pendaftaran Pelajar Baharu Prasiswazah di Kolej Kediaman	394	428	428	0	0	Kecuaian didalam pengendalian maklumat	Membuat latihan dan program kesedaran ISMS	-
5.	Proses Muatnaik data tawaran pelajar UPU	4	4	1	3	0	Kebarangkalian data digodam dan data dimanipulasi	Panduan <i>Layout Data</i> UPU.	1. Mewujudkan satu folder yang mengandungi kata laluan bagi menyimpan dan menyerahkan data Jaya UPU kepada pihak iDEC untuk proses muat naik ke dalam Sistem Maklumat Pelajar. 2. Menggunakan kaedah <i>Virtual Private Network</i> (VPN) atau menggunakan bilik <i>console</i> untuk proses muatnaik data tawaran UPU.

Bil	Nama Proses	Bil Aset	Bil Ancaman	Bil. Tahap Risiko			Punca Dominan	Kawalan Sediaada	Pelan Pemulihan Risiko
				L	M	H			
6.	Proses Pendaftaran Pelajar Baharu Prasiswazah UPMKB	52	118	87	31	0	Petugas tidak mencukupi, tidak mahir, kecuaiian.	Lantikan petugas baharu, latihan dan pemantauan	-
7.	Sistem sokongan (keselamatan)	13	13	10	3	0	Penentu operasi keselamatan rangkaian	Prosedur Penyelenggaraan ICT	Meningkatkan penyelenggaraan dan pemantauan berkala
8.	Sistem sokongan (rangkaiian)	17	17	11	6	0	1. Tulang belakang operasi rangkaian UPM 2. Rekabentuk yang tidak redundant sepenuhnya	Prosedur Penyelenggaraan ICT	Meningkatkan penyelenggaraan dan pemantauan berkala
9.	Sistem sokongan (Pusat Data)	165	237	84	153	0	1. Aset merupakan penentu operasi DC 2. Aset telah digunakan lebih 5 tahun 3. Penyimpan data utama	1. Prosedur Penyelenggaraan ICT 2. Penggunaan peralatan sokongan (UPS, Genset)	1. Meningkatkan penyelenggaraan dan pemantauan berkala 2. Latihan dan kursus berkaitan
10.	Sistem sokongan (Pangkalan Data)	21	56	7	49	0	penggunaan versi DB yang terkebelakang 4 versi (End of Support)	Prosedur Penyelenggaraan ICT	Laksanakan simulasi DRP ICT
11.	Sistem Aplikasi Maklumat Pelajar Prasiswazah	48	168	84	84	0	Aset telah digunakan lebih 5 tahun	Prosedur Penyelenggaraan ICT	1. Meningkatkan penyelenggaraan dan pemantauan berkala 2. Laksanakan simulasi DRP ICT
12.	Sistem Aplikasi Kewangan	19	57	25	32	0	Aset utama kewangan	Prosedur Penyelenggaraan ICT	1. Meningkatkan penyelenggaraan dan pemantauan berkala 2. Laksanakan simulasi DRP ICT
		853	1282	904	378	0			