5.1.2 (b): AUDIT DALAMAN SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)

LAPORAN KETUA JURUAUDIT AUDIT DALAMAN SISTEM PENGURUSAN KESELAMATAN MAKLUMAT ISO/IEC 27001:2013 TAHUN 2017

1. TARIKH AUDIT

Audit Dalaman Sistem Pengurusan Keselamatan Maklumat (ISMS) Universiti Putra Malaysia tahun 2017 telah dijalankan pada 5 hingga 8 Jun 2017.

2. OBJEKTIF AUDIT

Untuk menentukan sama ada Universiti Putra Malaysia:

(a) 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;
(b) melihat penambahbaikan yang bersesuaian bagi peningkatan berterusan; dan
(c) bersedia untuk menghadapi Audit Pemantauan Semakan Kedua, oleh badan pensijilan (SIRIM).

3. KRITERIA AUDIT

Audit Dalaman dijalankan berdasarkan dokumen dan rujukan berikut:

(a) Standard MS ISO/IEC 27001:2013;
(b) Dokumentasi Sistem Pengurusan Keselamatan Maklumat (ISMS) dan Sistem Pengurusan Kualiti (QMS) UPM yang berkaitan;
(c) Akta dan Peraturan berkaitan; dan
(d) Rujukan lain yang dinyatakan dalam Manual/Prosedur.

4. KAEDAH AUDIT

Kaedah audit yang digunakan oleh Juruaudit adalah:

(a) Semakan maklumat iaitu rekod dan dokumen. Semakan dibuat bermula dari 3 Oktober 2016 (Selepas audit badan pensijilan lepas) hingga bermula audit *(Review);*
(b) Pemerhatian pelaksanaan aktiviti *(Observe);*
(c) Pengujian fungsi peralatan *(Test);* dan
(d) Temubual auditi *(Interview).*

5. SKOP AUDIT

Skop audit adalah seperti berikut:

(a) Sistem Pengurusan Keselamatan Maklumat hanya melibatkan proses Pendaftaran pelajar baharu Prasiswazah UPM Kampus Serdang dan Kampus Bintulu;

(b) Sistem Pengurusan Keselamatan Maklumat untuk Pengoperasian Pusat Data bagi proses pendaftaran pelajar baharu prasiswazah;

(c) Sistem Pengurusan Keselamatan Maklumat untuk pengoperasian pusat pemulihan bencana bagi proses pendaftaran pelajar baharu prasiswazah.

6. LOKASI AUDIT

Lokasi audit adalah seperti berikut:

(a) Semua Kolej Kediaman di Kampus Serdang dan Kampus Bintulu;
(b) Pusat Data Utama (DC) (iDEC -BETA);
(c) Pusat Pemulihan Bencana (DRC) (iDEC -EPSILON);
(d) Peneraju dan entiti/PTJ di bawah skop ISMS iaitu
    i. Pusat Jaminan Kualiti, Bahagian Kemasukan dan Bahagian Urus Tadbir Akademik,
    ii. Pejabat Pembangunan Maklumat dan Komunikasi,
    iii. Pejabat Penasihat Undang-Undang,
    iv. Pejabat Strategi Korporat dan Komunikasi,
    v. Pejabat Pendaftar,
    vi. Pejabat Bursar,
    vii. Pusat Kesihatan Universiti,
    viii. Bahagian Hal Ehwal Pelajar,
    ix. Bahagian Keselamatan dan
    x. Perpustakaan Sultan Abdul Samad.

7. PASUKAN JURUAUDIT

Seramai 41 orang Juruaudit yang mempunyai kelayakan untuk mengaudit Sistem Pengurusan Keselamatan Maklumat telah melaksanakan audit pada tarikh yang ditetapkan. Pasukan audit telah dibahagikan kepada tiga kumpulan iaitu A, B dan C dan sebanyak 7 sub-kumpulan. Pelaksanaan audit dalaman ini diketuai oleh :

a. Encik Krishnan Mariappan dari Pusat Pembangunan Maklumat dan Komunikasi sebagai Ketua Juruaudit Dalaman (KJAD) ISMS dan ;

b. Tuan Sayid Mohamad Nazari Sayid Ismail dari Pusat Pembangunan Maklumat dan Komunikasi sebagai Timbalan KJAD ISMS

8. PROGRAM AUDIT DALAMAN

Program Audit Dalaman telah disediakan oleh Penyelaras Audit (PAD), Pusat Jaminan Kualiti dan disahkan oleh Wakil Pengurusan Universiti Putra Malaysia.

9. PENEMUAN AUDIT

Kekuatan

(a) Tindakan Pengurusan Universiti Putra Malaysia (UPM) untuk meluaskan skop ISMS ke UPM Kampus Bintulu menunjukkan komitmen UPM, Pusat Jaminan Kualiti (CQA) dan Pusat Pembangunan Maklumat dan Komunikasi (iDEC) serta semua Peneraju Proses adalah tinggi dalam pelaksanaan Sistem Pengurusan Keselamatan Maklumat;

(b) Ketersediaan dan kebolehcapaian maklumat terdokumen adalah baik serta memenuhi keperluan Standard MS ISO/IEC 27001:2013;

(c) Penilaian risiko dan rawatan terhadap risiko yang dikenalpasti telah dilaksanakan dengan baik dan memenuhi keperluan Standard MS ISO/IEC 27001:2013;

(d) Pengoperasian Pusat Data Utama dan Pusat Pemulihan Bencana adalah pada tahap terkawal, selamat dan memenuhi keperluan Standard MS ISO/IEC 27001:2013;

(e) Kefahaman dan pembudayaan terhadap keselamatan maklumat telah meningkat dalam kalangan staf di Kampus Serdang terutamanya staf Kolej dan staf Pusat Pembangunan Maklumat dan Komunikasi;

(f) Tindakan terhadap ketakakuran dan cadangan penambahbaikan telah dilaksanakan oleh Peneraju Proses dan dipantau oleh Pusat Jaminan Kualiti (CQA);

(g) Pelaksanaan proses kerja yang baik dan teratur mengikut carta alir yang telah diwujudkan untuk proses pendaftaran pelajar baharu di UPM Kampus Bintulu.

Kelemahan

(a) Perubahan pada maklumat terdokumen berikutan peluasan skop masih belum dilaksanakan dengan sepenuhnya;

(b) Tahap kefahaman tentang Sistem Pengurusan Keselamatan Maklumat dalam kalangan staf UPM Kampus Bintulu adalah pada tahap yang rendah;

(c) Pembahagian tugas dan tanggungjawab masih perlu diperincikan mengikut portfolio yang betul di UPM Kampus Bintulu.

10. LAPORAN PENEMUAN AUDIT DALAMAN

Hasil daripada audit dalaman yang telah dijalankan beberapa Laporan Ketakakuran (NCR) dan Peluang Penambahbaikan (OFI) telah direkodkan. Laporan penemuan audit telah dibentang semasa Mesyuarat Penutupan Audit Dalaman pada 22 Jun 2017. Bilangan penemuan audit adalah sebagaimana **Jadual 1**, manakala perincian bagi penemuan audit mengikut Pusat Tanggungjawab (PTJ) dan Klausa adalah sebagaimana **Lampiran 1**.

Jadual 1: Bilangan Penemuan Audit Dalaman

Penemuan	Bilangan
NCR	14
OFI	13
Perincian penemuan audit boleh dirujuk dalam portal Jaminan Kualiti (PortalCQA) http://portalcqa.upm.edu.my/	

11. PENUTUPAN PENEMUAN AUDIT

Pemakluman dan edaran secara *online* penemuan audit kepada semua Timbalan Wakil Pengurusan (TWP) dan Timbalan Penyelaras Audit (TPAD) di bawah skop ISMS adalah pada 3 Julai 2017. mengambil kira cuti Hari Raya Aidilfitri.

Sehubungan itu cadangan tarikh bagi penutupan penemuan audit adalah pada 31 Julai 2017. Walau bagaimanapun, penetapan tarikh sebenar tindakan bagi penutupan audit dalaman adalah berdasarkan tarikh yang dinyatakan atau tarikh lain yang dipersetujui oleh Juruaudit mengikut kesesuaian tempoh tindakan.

Maklum balas bagi tindakan ke atas penemuan audit (NCR dan OFI) perlu dilengkapkan oleh TWP atau TPAD melalui Portal Jaminan Kualiti (Portal CQA) secara *online* di bawah pautan Audit Dalaman.

12. KESIMPULAN

Hasil dari proses audit dalaman yang telah dijalankan, ketakakuran yang ditemui adalah menjurus kepada perancangan dan kawalan operasi, kawalan maklumat terdokumen dan tahap kefahaman staf berpunca dari peluasan skop ISMS ke UPM Kampus Bintulu.

Disediakan oleh:

KRISHNAN MARIAPPAN
Ketua Juruaudit Audit Dalaman ISMS
Universiti Putra Malaysia

Lampiran

PERINCIAN PENEMUAN AUDIT MENGIKUT PUSAT TANGGUNGJAWAB DAN KLAUSA

1. Penemuan Audit (NCR dan OFI) mengikut Pusat Tanggungjawab (PTJ)

Bil.	Pusat Tanggungjawab	Kod PTJ	Jumlah NCR	Jumlah OFI
1	Bahagian Kemasukan dan Bahagian Urus Tadbir Akademik	AKAD	0	1
2	Pusat Jaminan Kualiti	CQA	1	2
3	Fakulti Sains Pertanian dan Makanan	FSPM	4	1
4	Pusat Pembangunan Maklumat dan Komunikasi	IDEC	3	4
5	Kolej Canselor	KC	0	1
6	Kolej Mohamad Rashid	KMR	0	1
7	Kolej Sultan Alaeddin Suleiman Shah	KOSSAS	1	0
8	Pejabat Pendaftar	PEND	3	0
9	Perpustakaan Sultan Abdul Samad	PSAS	1	3
10	Pejabat Strategi Korporat dan Komunikasi	PSKK	1	0
JUMLAH KESELURUHAN			**14**	**13**

2. Penemuan Audit Mengikut Klausa

Bil.	Klausa	Jumlah NCR	Jumlah OFI
1.	4.1 *Understanding the organization and its context*	0	1
2.	4.2 *Understanding the needs and expectations of interested parties*	0	1
3.	6.2 *Information security objectives and planning to achieve them*	1	0
4.	6.1.2 *Information security risk assessment (Planning)*	2	2
5.	6.1.3 *Information security risk treatment*	1	1
6.	7.2 *Competence*	0	1
7.	7.3 *Awareness*	1	0
8.	7.5.2 *Creating and updating*	0	2
9.	7.5.3 *Control of documented information*	0	1
10.	8.1 *Operational planning and control*	8	3
11.	8.2 *Information security risk assessment (Operation)*	0	1
12.	10.1 *Nonconformity and corrective action*	1	0
JUMLAH KESELURUHAN		14	13