PENEMUAN AUDIT DALAMAN SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)

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

1.0 PENDAHULUAN

Audit Dalaman Sistem Pengurusan Keselamatan Maklumat (ISMS) Universiti Putra Malaysia kali keempat telah dijalankan pada 3 hingga 5 Mei 2016. Audit Dalaman ini merupakan audit dalaman pertama setelah UPM memperolehi pensijilan Sistem Pengurusan Keselamatan Maklumat MS ISO/IEC 27001:2013 melibatkan lokasi audit yang lebih meluas iaitu:

1. Bahagian Hal Ehwal Pelajar
2. Bahagian Kemasukan Akademik
3. Bahagian Keselamatan
4. Pejabat Bursar
5. Pejabat Penasihat Undang-undang
6. Pejabat Pendaftar
7. Pejabat Strategi Korporat dan Komunikasi (CoSComm)
8. Perpustakaan Sultan Abdul Samad
9. Pusat Kesihatan Universiti
10. Pusat Jaminan Kualiti (CQA)
11. Pusat Pembangunan Maklumat dan Komunikasi (iDEC)
12. Semua Kolej Kediaman

Skop Audit Dalaman dijalankan mengikut skop Sistem Pengurusan Keselamatan Maklumat, Universiti Putra Malaysia iaitu:

1. Pendaftaran Pelajar Baharu Prasiswazah semasa Minggu Perkasa Putra;
2. Pengoperasian Pusat Data bagi proses Pendaftaran Pelajar Baharu Prasiswazah; dan
3. Pengoperasian Pusat Pemulihan Bencana bagi proses Pendaftaran Pelajar Baharu Prasiswazah

Audit Dalaman ini adalah berdasarkan kepada bukti objektif yang ditemui melalui semakan ke atas maklumat terdokumen (*documented information*), temubual dengan staf yang menjalankan aktiviti dan pemerhatian pelaksanaan aktiviti tersebut. Sampel pengauditan telah dilakukan secara rawak.

2.0 TUJUAN

Tujuan audit dalaman adalah untuk:

(a) memantau sama ada ISMS di Universiti Putra Malaysia telah dilaksana dan diselenggara secara efektif mengikut dokumen ISMS Universiti Putra Malaysia dan keperluan piawaian ISO/IEC 27001:2013;

(b) memberi maklum balas tentang peluang bagi penambahbaikan berterusan *(continuous improvement)* ISMS yang telah diamalkan;

(b) memenuhi keperluan Klausa 9.2 Sistem Pengurusan Keselamatan Maklumat ISO/IEC 27001:2013.

3.0 KUMPULAN AUDIT

Seramai 14 orang Juruaudit Dalaman ISMS Universiti Putra Malaysia telah dilantik untuk mengaudit proses dalam skop pensijilan ISMS MS ISO/IEC 27001:2013. Proses audit dalaman ini diketuai oleh seorang Ketua Juruaudit Dalaman (KJAD) dan semua Juruaudit Dalaman telah dibahagikan kepada tiga (3) kumpulan audit di mana setiap kumpulan terdiri daripada seorang Ketua Kumpulan dan beberapa orang ahli.

4.0 JADUAL DAN AKTIVITI AUDIT

Jadual program audit dalaman telah disediakan oleh Penyelaras Audit Dalaman ISMS dengan persetujuan dari pihak pengurusan Universiti Putra Malaysia.

Tarikh akhir untuk melaksanakan tindakan pembetulan telah ditetapkan dalam tempoh 21 hari bekerja atau tarikh yang telah dipersetujui oleh Juruaudit UPM. Pihak Juruaudit Dalaman akan menyemak serta menilai keberkesanan tindakan pembetulan tersebut pada 6 Jun 2016 atau tarikh lain yang dipersetujui oleh auditi.

5.0 PENEMUAN AUDIT

Hasil daripada audit dalaman yang telah dijalankan, didapati komitmen Pengurusan UPM, Pusat Jaminan Kualiti dan Peneraju Proses adalah tinggi dalam menyelaras dan melaksana Sistem Pengurusan Keselamatan Maklumat. 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. Penilaian risiko (*risk assessment)* dan rawatan risiko (*risk treatment*) telah dilaksanakan dengan baik dan memenuhi keperluan Standard MS ISO/IEC 27001:2013. Pengoperasian Pusat Data Utama dan Pusat Pemulihan Bencana adalah pada tahap selamat dan memenuhi keperluan Standard MS ISO/IEC 27001:2013. Amalan keselamatan maklumat adalah baik walaupun kefahaman dan pembudayaan terhadap

ISMS dalam kalangan staf pelaksana masih boleh dipertingkatkan. Pemantauan dan tindakan terhadap ketakakuran dan cadangan penambahbaikan telah dilaksanakan oleh Pusat Jaminan Kualiti (CQA) dan Peneraju Proses dengan baik.

Namun, sebanyak 14 ketakakuran (NCR) telah ditemui dan 20 peluang penambahbaikan (OFI) telah dicadangkan. Taburan ketakakuran serta peluang penambahbaikan mengikut klausa yang telah diaudit adalah seperti **Jadual 1** dan **Jadual 2.**

Jadual 1: Ketakakuran (NCR) Mengikut Klausa

Penemuan	Klausa	Bilangan	Peratus (%)
Ketakakuran (NCR)	8.1	7	50.0
	7.5	5	35.7
	7.4	1	7.1
	5.3	1	7.1
Jumlah		**14**	

Ketakakuran yang paling tinggi (50.0%) adalah pada Perancangan dan Kawalan Operasi (Klausa 8.1) dimana tujuh (7) ketakakuran telah ditemui diikuti dengan Maklumat Terdokumen (35.7%) dimana lima (5) ketakakuran telah ditemui. Satu ketakakuran (7.1%) telah ditemui pada Peranan Organisasi, Tanggungjawab dan Kuasa (Klausa 5.3) dan Komunikasi (Klausa 7.4) masing-masing.

Jadual 2: Peluang Penambahbaikan (OFI) Mengikut Klausa

Cadangan	Klausa	Bilangan	Peratus (%)
Peluang Penambahbaikan	8.1	11	55.0
	7.5	5	25.0
	7.3	2	10.0
	7.4	1	5.0
	6.1.2	1	5.0
Jumlah		**20**	

Peluang penambahbaikan yang telah dicadangkan adalah terdiri dari 55.0% pada Perancangan dan Kawalan Operasi (Klausa 8.1), 25.0% pada Maklumat Terdokumen (Klausa 7.5), 10.0% pada Kesedaran (Klausa 7.3) dan masing-masing 5.0% pada Komunikasi (Klausa 7.4) dan Penilaian Risiko Keselamatan Maklumat (Klausa 6.1.2).

6.0 TINDAKAN PEMBETULAN

Universiti Putra Malaysia sedang mengambil tindakan ke atas semua ketakakuran yang dikeluarkan dan telah bersetuju dengan 19 daripada 20 peluang penambahbaikan yang telah dicadangkan. Tindakan ke atas semua peluang penambahbaikan sedang dilaksanakan namun terdapat cadangan yang memerlukan peruntukan kewangan untuk dilaksanakan.

7.0 RUMUSAN

Hasil dari proses audit dalaman yang telah dijalankan, ketakakuran yang ditemui adalah menjurus kepada perancangan dan kawalan operasi serta kawalan terhadap maklumat terdokumen. Didapati Universiti Putra Malaysia mengambil tindakan yang berkesan dalam meningkatkan prasarana dan kemudahan untuk memenuhi keperluan ISMS ISO/IEC 27001:2013.

Dari segi pelaksanaan ISMS, Universiti Putra Malaysia adalah bersedia untuk diaudit oleh Badan Pensijilan SIRIM tertakluk kepada tindakan pembetulan yang berkesan diambil terhadap ketakakuran yang ditemui dalam masa yang telah ditetapkan.

Pihak pengurusan Universiti Putra Malaysia perlu terus meningkatkan tahap kefahaman ISMS dalam kalangan semua staf UPM melalui latihan, komunikasi dalaman dan penyampaian maklumat mengenai ISMS kepada semua staf, pihak dalaman dan luaran yang ada kepentingan, pemilik risiko serta pembekal yang berkaitan.

7.0 PENUTUP

Adalah diharapkan semua staf Universiti Putra Malaysia dapat mengambil tindakan pembetulan dan pencegahan yang bersesuaian untuk kesemua ketakakuran yang ditemui dalam Audit Dalaman ISMS ini. Staf yang terlibat dalam perancangan dan kawalan operasi dan kawalan maklumat terdokumen perlu meningkatkan tahap kefahaman dan mempraktikan amalan terbaik dalam melaksanakan tugas seiring dengan keperluan keselamatan maklumat

Ketua Juruaudit Dalaman dan semua Juruaudit Dalaman ISMS ingin merakamkan ucapan setinggi-tinggi terima kasih atas kerjasama dan layanan baik yang diberikan oleh setiap peringkat staf Universiti Putra Malaysia sepanjang perlaksanaan audit dalaman ini.

Disediakan oleh:
KRISHNAN A/L MARIAPPAN
Ketua Juruaudit Dalaman ISMS Tahun 2016
15 Jun 2016