PENEMUAN AUDIT BADAN PENSIJILAN OLEH SIRIM
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)

HASIL LAPORAN AUDIT PENSIJILAN SEMULA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
MS ISO/IEC 27001:2013 TAHUN 2015

1.0 TUJUAN

Kertas ini adalah bertujuan untuk memaklum kepada Ahli Mesyuarat Kajian Semula Pengurusan (MKSP) Universiti Putra Malaysia (UPM) berkaitan penemuan Audit Pensijilan Semula, Sistem Pengurusan Keselamatan Maklumat oleh SIRIM.

2.0 PENGENALAN

Audit Pensijilan Semula Sistem Pengurusan Keselamatan Maklumat oleh SIRIM telah dilaksana pada 8 hingga 10 Disember 2015. Sepanjang audit, seramai tiga (3) orang Juruaudit telah terlibat bagi mengaudit skop seperti berikut:

a. Sistem Pengurusan Keselamatan Maklumat bagi proses pendaftaran pelajar baharu prasiswazah semasa Minggu Perkasa Putra;
b. Sistem Pengurusan Keselamatan Maklumat untuk 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.

3.0 LOKASI AUDIT

Lokasi audit adalah melibatkan Pusat Jaminan Kualiti, Bahagian Kemasukan dan Tadbir Urus Akademik, Bahagian Hal Ehwal Pelajar, Pusat Pembangunan Maklumat dan Komunikasi (Pusat Data dan Pusat Pemulihan Bencana), Kolej Kediaman (Kolej Kedua, Kolej Tun Dr Ismail, Kolej Kelima, Kolej Keenam dan Kolej Kesepuluh), Pejabat Penasihat Undang-undang, Perpustakaan Sultan Abdul Samad, Pejabat Strategik Korporat dan Komunikasi, Bahagian Keselamatan Universiti dan Pusat Kesihatan Universiti.

4.0 PENEMUAN AUDIT

Hasil Audit Pensijilan Semula, terdapat satu (1) laporan ketakakuran (NCR) dan 10 peluang penambahbaikan (OFI). Ringkasan hasil laporan audit pensijilan semula boleh dirujuk seperti **Jadual 1** bagi Laporan Ketakakuran dan **Jadual 2** bagi Peluang Penambahbaikan.

Jadual 1: Ringkasan Laporan Ketakakuran

BIL.	**KETAKAKURAN**	**KLAUSA**	**BUKTI PENEMUAN** *Hendaklah dibaca bersama Laporan SIRIM yang boleh dirujuk pada e-ISO*
1.	NR-1	10.1	Tindakan pembetulan yang diambil untuk ketakakuran yang dilaporkan semasa audit pemantauan yang lepas tidak dijalankan secara menyeluruh. Keberkesanan tindakan yang diambil tidak dapat dilihat memandangkan masih terdapat ruang di mana ketakakuran itu telah dan mungkin berulang.

Jadual 2: Ringkasan Laporan Peluang Penambahbaikan

BIL	**KLAUSA**	**RINGKASAN PELUANG PENAMBAHBAIKAN** *Hendaklah dibaca bersama Laporan SIRIM yang boleh dirujuk pada e-ISO*
1.	A.7.1.1	***Screening*** 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.
2.	A.8.2.1	***Classification of information*** 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)

BIL	KLAUSA	**RINGKASAN PELUANG PENAMBAHBAIKAN** *Hendaklah dibaca bersama Laporan SIRIM yang boleh dirujuk pada e-ISO*
3.	A.8.2.3	***Handling of assets*** 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.
4.	A.11.2.1	***Equipment siting and protection*** 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.
5.	A.12.1.3	***Capacity management*** 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.
6.	A.13.2.4	***Confidentiality or non disclosure agreements*** Bahagian Penasihat Undang-Undang boleh menambahbaik dari segi meneliti akan perjanjian ke atas kontrak- kontrak yang melibatkan penerimaan dan pertukaran maklumat.
7.	A.16.1.2	***Reporting information security events*** 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.

BIL	**KLAUSA**	**RINGKASAN PELUANG PENAMBAHBAIKAN** *Hendaklah dibaca bersama Laporan SIRIM yang boleh dirujuk pada e-ISO*
8.	6.1.2	***Information security risk assessment*** 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.
9.	6.1.3	***Information security risk treatment*** 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.
10.	8.1	***Operational planning and control*** 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.