File no. : IS/6-80

Date : 3 December 2015

Universiti Putra Malaysia,
Infocomm Development Centre (IDEC)
43400 Serdang,
Selangor Darul Ehsan,
Malaysia.

Tel: 03-89471568 Fax: 03-89472098

(Attn: Puan Noraihan Binti Noordin)

Dear Sir/ Madam

ISO/IEC 27001:2013– RECERTIFICATION AUDIT PLAN

Please be informed that a Recertification Audit of your organization's Information Security Management systems has been scheduled on 8-10 December 2015.

Enclosed please find the audit plan. Please note that the audit plan serves as a guide and may change as the audit progresses.

Thank you

Yours sincerely

Efizan Binti Zamri

……..

Lead Auditor
Services Section
Management System Certification Department
SIRIM QAS International Sdn Bhd
Hp No: 019-2444833
Tel No: 03-55446485
Fax: 03-55446414
www.sirim-qas.com.my

RECERTIFICATION AUDIT PLAN

1) Audit Objectives

a) To determine the continued conformity and effectiveness of the Information Security Management systems in its entirety in the light of internal and external changes and its continued relevance and applicability for the scope of certification.

b) To determine commitment of the organization to maintain the effectiveness and improvement of the management system in order to enhance overall performance.

c) To determine effective interaction between all elements of the system and whether the operation of the certified management system contributes to the achievement of the organization's policy and objectives

d) To verify the effective implementation of corrective actions arising from the findings of the previous audit.

2) Date of audit : 8-10 December 2015.

3) Site of audit :

Main Site :
Universiti Putra Malaysia,
Infocomm Development Centre (IDEC)
43400 Serdang,
Selangor Darul Ehsan,
Malaysia.

Site 2:
Universiti Putra Malaysia,
Infocomm Development Centre (IDEC),
Beta Data Centre
43400 Serdang,
Selangor Darul Ehsan,
Malaysia.

Site 3:
Universiti Putra Malaysia,
Infocomm Development Centre (IDEC),
Epsilon Data Recovery Centre,
UPM/Server Farm,
43400 Serdang,
Selangor Darul Ehsan,
Malaysia.

Scope of certification :
Main Site:
Sistem Pengurusan Keselamatan Maklumat Bagi Sistem- Sistem Kritikal Merangkumi Sistem Aplikasi Pelajar, Sistem Pengurusan Sumber Manusia, Sistem Pengurusan Kewangan dan Laman Web Utama Universiti Putra Malaysia.

Site 2:
Sistem Pengurusan Keselamatan Maklumat Untuk Pengoperasian Pusat Data.

Site 3:
Sistem Pengurusan Keselamatan Maklumat Untuk Pengoperasian Pusat Pemulihan Bencana.

5) Audit criteria :

a) ISO/IEC 27001:2013
b) Organization's ISMS Documentation

6) Audit team

a) Audit Team Leader : Efizan Bt Zamri

b) Auditor/ Evaluator : Sazlin Bt Alias
c) Auditor : Nor Aza Bt Ramli (day 1 & 2 only)

d) ~~Technical Expert/Observer/etc~~

(If there is any objection on the proposed audit team, the client is required to inform in writing to the Audit Team Leader or the Head of Section)

7) Methodology of audit

a) Review of documentation and records,
b) Observation of processes and activities,
c) Interview with client's personnel responsible for the audited area including top management.

8) Confidentiality requirements

The members of the audit team from SIRIM QAS International Sdn. Bhd. undertake not to disclose any confidential information obtained during the audit including information contained in the final report to any third party, without the express approval of the client unless required by law.

9) Working Language : English and Bahasa Melayu

10) Reporting

i) Language : English/Bahasa Melayu
ii) Format : Verbal and written
iii) Expected date of issue : After closing meeting
iv) Distribution List : Original copy issued to the client and copy maintained in the client file

11) Facilities and assistance required :

i) Meeting room
ii) Facilities for photocopying
iii) Personal protective equipment (where necessary)
iv) A representative appointed by the client, acting as a guide to assist the audit team.

12) Details of Audit Plan : As follows

DETAILS OF AUDIT PLAN

Day 1		
Time	**Agenda**	**Responsibility**
0930–0945	Opening Meeting	SIRIM's auditors and client's representatives
0930–0945	Briefing on the Information Security Management System by organization's representative on any changes to the system since last audit	Client's representative
0945-1700	Review of documentation against requirements of ISO/IEC 27001:2013	
	Review of actions taken on nonconformities identified during the previous audit	
	Audit on the activities related to following requirements: ***Documented information*** *inclusive of creating and updating and control of documented information.* ***Context of the organization*** *inclusive of understanding the organization and its context, understanding the needs and expectations of interested parties, determining the scope of the ISMS.* ***Leadership*** *inclusive of leadership and commitment, policy and organizational roles, responsibilities and authorities.* ***Planning*** *inclusive of actions to address risks and opportunities, information security risk assessment, information security risk treatment and information security objectives and plans to achieve them.* ***Operation*** *inclusive of operational planning and control, information security risk assessment and information security risk treatment.* ***Performance evaluation*** *inclusive of monitoring, measurement, analysis and evaluation, internal audit and management review.* ***Improvement*** *inclusive of nonconformity and corrective action and continual improvement.* *Samples on the effectiveness of controls implemented from Annex A.* **Internal Audit & Management Review** ISMS Covering the continual Improvement Activities, Corrective Action. Verification on the effectiveness of control implemented related to **A.7 Human Resource Security.**	SIRIM's Auditor (Efizan) & Client's Representative

	Verification on the effectiveness of control as per Statement of Applicability in relation For *Perpustakaan* • Asset management (A.8) • Cryptography (A.10) • Physical and environmental security (A.11) • Access control (A.9) • Operations security (A.12) • Supplier Relationship (A.15) • Communications security (A.13) • System acquisition, development, maintenance (A.14)	
	Verification on the effectiveness of control as per Statement of Applicability in relation For *Bahagian Kemasukan dan Tadbir Urus Akademik. (0.5 x 2 = 1 AD (auditor days)* • Asset management (A.8) • Cryptography (A.10) • Physical and environmental security (A.11) • Access control (A.9) • Operations security (A.12) • Supplier Relationship (A.15) • Communications security (A.13) • System acquisition, development, maintenance (A.14)	SIRIM's Auditor (Sazlin/ Aza) & Client's Representative
	Verification on the effectiveness of control as per Statement of Applicability in relation For *Bahagian Hal Ehwal Pelajar (0.5 x 2 = 1 AD (auditor days)* • Asset management (A.8) • Cryptography (A.10) • Physical and environmental security (A.11) • Access control (A.9) • Operations security (A.12) • Supplier Relationship (A.15) • Communications security (A.13) • System acquisition, development, maintenance (A.14)	SIRIM's Auditor (Sazlin/ Aza) & Client's Representative
1700	Review of Day 1 Findings	SIRIM's auditors and client's representatives

Day 2		
Time	**Agenda**	**Responsibility**
0930–1700	Verification on the effectiveness of control as per Statement of Applicability in relation For *Bahagian Keselamatan* • Asset management (A.8) • Cryptography (A.10) • Physical and environmental security (A.11) • Access control (A.9) • Operations security (A.12) • Supplier Relationship (A.15) • Communications security (A.13) • System acquisition, development, maintenance (A.14)	SIRIM's Auditor (Efizan) & Client's Representative
	Verification on the effectiveness of control as per Statement of Applicability in relation For *Pusat Pembangunan Maklumat dan Komunikasi & Pejabat Pendaftar* • Asset management (A.8) • Cryptography (A.10) • Physical and environmental security (A.11) • Access control (A.9) • Operations security (A.12) • Supplier Relationship (A.15) • Communications security (A.13) • System acquisition, development, maintenance (A.14) Audit on requirements related to: • Verification on the effectiveness of control as per Statement of Applicability in relation to **Information Security Incident Management (A.16) &** • **Compliance (A.18)** Audit on requirements related to: • Information Security Aspect of **Business Continuity Management (A.17)** • ISMS Monitoring and Review covering overall regular review of effectiveness, measurement of control effectiveness.	SIRIM's Auditor (Sazlin /Aza) & Client's Representative
1700	Review of Day 2 Findings	SIRIM's auditors and client's representatives

Day 3		
Time	**Agenda**	**Responsibility**
0930–1300	Interview Session with Top Management Verification on the effectiveness of control as per Statement of Applicability in relation For *Kolej Kediaman* • Asset management (A.8) • Cryptography (A.10) • Physical and environmental security (A.11) • Access control (A.9) • Operations security (A.12) • Supplier Relationship (A.15) • Communications security (A.13) • System acquisition, development, maintenance (A.14)	SIRIM's Auditor (Efizan) & Client's Representative
	Verification on the effectiveness of control as per Statement of Applicability in relation For *Pusat Kesihatan Universiti* • Asset management (A.8) • Cryptography (A.10) • Physical and environmental security (A.11) • Access control (A.9) • Operations security (A.12) • Supplier Relationship (A.15) • Communications security (A.13) • System acquisition, development, maintenance (A.14)	SIRIM's Auditor (Sazlin) & Client's Representative
1300-14:00	Lunch Break – Continue Audit (1400-1500)	
1500–1630	Preparation of Report	SIRIM's auditor
1630	Closing Meeting : Presentation of Findings and Recommendation	SIRIM's auditor