File no. : IS/6-189

Date : 30 September 2016

Universiti Malaysia Sabah,
Jabatan Teknologi Maklumat dan Komunikasi,
Jalan UMS,
88400 Kota Kinabalu,
Sabah,
Malaysia.

Tel: 088-320000 Fax: 088-320235

(Attn: Puan Noor Hapipah Samat)

Dear Sir/ Madam

ISO/IEC 27001:2013– SURVEILLANCE AUDIT PLAN

Please be informed that a Surveillance Audit of your organization's Information Security Management systems has been scheduled on _____13-14 October 2016___.

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: 012-2718471
Tel No: 03-55446485
Fax: 03-55446414
www.sirim-qas.com.my

SURVEILLANCE AUDIT PLAN

1. **Audit Objectives**

   a) To determine the continued compliance of the client's information security management system to the ISO/IEC 27001:2013 standard;

   b) To evaluate the ability of the management system to ensure client meets applicable statutory, regulatory and contractual requirements, where applicable;

   c) To evaluate the effectiveness of the management system to ensure the client is continually meet its specified objectives;

   d) To identify areas of improvement of the management system, as applicable;

   e) To assess changes that has been made to the client's information security management system;

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

2. **Date of audit** : 13-14 October 2016

3. **Site of audit** :

   Universiti Malaysia Sabah,
   Jabatan Teknologi Maklumat dan Komunikasi,
   Jalan UMS,
   88400 Kota Kinabalu,
   Sabah,
   Malaysia.
   .

4. **Scope of certification** :

   Sistem Pengurusan Keselamatan Maklumat (ISMS) Bagi Penyediaan Pekhidmatan Pendidikan Meliputi :
   1.) Pengurusan dan Pengoperasian Pusat Data Kampus Induk.
   2.) Pengurusan dan Pembangunan Aplikasi.
   3.) Pengurusan dan Pembangunan Laman Sesawang.

5. **Audit Criteria** :

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

6. **Audit team & Role**

a)	Audit Team Leader	:	Efizan Bt Zamri
b)	Auditor	:	NA
c)	Trainee auditor	:	NA
d)	Technical Expert/ Observer/ Translator/ etc	:	NA

(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.

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
0945 - 1000	Briefing on the Information Security Management System by organization's representative on any changes to the system since last audit	Client's representative
1000 - 1300	Review of actions taken on nonconformities identified during the previous audit	
1000 - 1300	Review of documentation against requirements of ISO/IEC 27001:2013 & Verification of corrective action for previous audit findings. 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. **Support** inclusive of resources, competence, awareness and communication. **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.	Efizan & Client's Representative
1300 - 1400	Lunch Break	

1400 - 1700	Verification on the effectiveness of control as per Statement of Applicability in relation for **Data Center Operation** • 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)	
1700	Review of Day 1 Findings	SIRIM's auditors and client's representatives

Day 2		
Time	**Agenda**	**Responsibility**
0830 - 1530	ISMS Monitoring and Review covering overall regular review of effectiveness, measurement of control effectiveness. Verification on the effectiveness of control as per Statement of Applicability in relation for **Pembangunan Aplikasi/ Pembangunan Laman Sesawang.** • 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 to **Information Security Incident Management (A.16)**	Efizan & Client's Representative

	Audit on requirements related to: **Information Security Aspect of Business Continuity Management (A.17)** **Audit on requirements related to :** **Compliance (A.18)**	
1530 - 1630	Preparation of Report	SIRIM's auditor
1630	Closing Meeting : Presentation of Findings and Recommendation	SIRIM's auditor & client's management