CONFIDENTIAL

SIRIM QAS INTERNATIONAL	**SIRIM QAS INTERNATIONAL SDN. BHD.** **MANAGEMENT SYSTEM CERTIFICATION DEPARTMENT** **Block 4, SIRIM Complex, No.1, Persiaran Dato' Menteri,** **Section 2, 40700 Shah Alam, Selangor Darul Ehsan**	**File No : QU00510035** **(IS/6-80)**
	INFORMATION SECURITY MANAGEMENT SYSTEM **SURVEILLANCE AUDIT REPORT**	

CLIENT : UNIVERSITI PUTRA MALAYSIA

ADDRESS OF MAIN SITE AUDITED :
(In the case of multisite certification, list additional sites audited in attachments) :

43400 SERDANG,
SELANGOR DARUL EHSAN,
MALAYSIA.

CERTIFICATION NO :	**AR 5761**	**STANDARD :**	**MS ISO/IEC 27001:2013**
AUDIT DATE :	**31/8, 29-30/9/2016 /_6_auditor day(s)**	**LAST AUDIT DATE :**	**8-10/12/2015**

SCOPE OF CERTIFICATION :

SISTEM PENGURUSAN KESELAMATAN MAKLUMAT BAGI PROSES PENDAFTARAN BAHARU PRASISWAZAH SEMASA MINGGU PERKASA PUTRA.

AUDIT TEAM :	1)	NUR AISYA MOHD. ZAMRI	KETUAN PASUKAN AUDIT
	2)	EFIZAN ZAMRI	AHLI PASUKAN AUDIT
	3)	SAZLIN ALIAS	AHLI PASUKAN AUDIT
	4)	NORIDAH YAHYA	AHLI PASUKAN AUDIT

NO OF EMPLOYEES (Applicable to the scope of certification) : 1208

Report by Audit Team Leader

Name : Nur Aisya Mohd. Zamri

Signature :

Date : 30/9/2016

SIRIM QAS INTERNATIONAL SDN BHD NUR AISYA BINTI MOHD ZAMRI

Acknowledgement by Client's Management Representative

Name :

Signature :

Date : 30/9/2016

PROF. DR. M. IQBAL SARIPAN
Wakil Pengurusan
Universiti Putra Malaysia

The Audit Plan and following attachments form part of this report :

Nonconformity Report(s)	–
Opportunities for Improvement	√
List of additional site(s)	√
List of remote supporting functions	–

Tick (√) where applicable

Report reviewed by :

(Senior Auditor/ Section Head)

Date

SURVEILLANCE AUDIT REPORT

1. SIGNIFICANT CHANGES TO ORGANIZATION INFORMATION SECURITY MANAGEMENT SYSTEM

ANTARA PERUBAHAN YANG DIBUAT OLEH ORGANISASI:

1. PERLANTIKAN BAHARU NAIB CANSELOR, IAITU PROFESOR DATIN PADUKA DR. AINI IDERIS BERKUATKUASA 1 JANUARI 2016.
2. PERUBAHAN PEMAKAIAN KAWALAN A.6.2.2 TELEWORKING DARIPADA "NO" KEPADA "YES"
3. PERUBAHAN TERHADAP BEBERAPA PROSES PENDAFTARAN BAHARU PRASISWAZAH SEPERTI PEMERIKSAAN KESIHATAN.
4. PERUBAHAN TERHADAP PROSEDUR, GARIS PANDUAN DAN DOKUMEN-DOKUMEN LAIN MENGIKUT KESESUAIAN DAN PELAKSANAAN SEMASA.

2. MANUAL REFERENCE (including revision number) : STATEMENT OF APPLICABILITY (SOA) NO SEMAKAN 09, NO ISU 01, TARIKH 1 JULAI 2016.

3. SUMMARY OF REVIEW OF ACTIONS TAKEN ON NONCONFORMITIES IDENTIFIED DURING THE PREVIOUS AUDIT (detail of NCR's and the status are to be listed in the Appendix 1):

Rujuk Appendix 1.

4. USE OF CERTIFICATION / ACCREDITATION MARKS

☐	Not in use	☐	Used; unacceptable
√	Used; acceptable		

5. COMMENTS ON FINDINGS :

5.1 Effectiveness of Internal Audit

Organisasi telah menjalankan audit dalaman ISMS pada 2 – 5 Mei 2016 oleh 14 juruaudit dalam yang terlatih dan bebas daripada aktiviti yang diaudit. Hasil daripada audit tersebut, terdapat 14 penemuan yang dilaporkan di bawah kategori Ketidakpatuhan *(NCR)* dan 18 penemuan adalah di bawah kategori Peluang Penambahbaikan *(OFI)*. Berdasarkan Jadual Audit ISMS 2016 dan Borang Nota Audit Dalam, audit mendapati bahawa liputan audit adalah menyeluruh. Pengendalian penemuan audit juga adalah baik.

5.2 Management Review

Prestasi keseluruhan mesyuarat kajian semula pengurusan yang dijalankan adalah mematuhi kehendak klausa 9.3 berdasarkan pemerhatian berikut:

- Mesyuarat kajian semula pengurusan melalui MKSP yang terkini telah dijalankan pada 30 Jun 2016 yang dipengerusikan oleh Naib Canselor, Profesor Datin Paduka Dr. Aini Ideris. Mesyuarat tersebut telah dihadiri oleh semua kakitangan utama yang berkaitan dengan skop persijilan.
- Diperhatikan bahawa agenda yang dibincangkan sepanjang mesyuarat ini adalah menepati keperluan klausa 9.3 standard ISO/IEC 27001:2013.
- Platform lain dalam membincangkan perjalanan pelaksanaan ISMS ialah Mesyuarat Jawatankuasa Kerja ISMS.

5.3 Information Security Risks Assessment:

Kaedah pelaksanaan pengurusan risiko telah dinyatakan di dalam Garis Panduan Penilaian Risiko Aset yang bertarikh 1/7/2016. Penilaian risiko dibuat melalui aplikasi MyRAM dengan mengenalpasti kesemua aset-aset di bawah skop pensijilan. Hasil daripada penilaian tersebut, didapati tiga (3) daripada empat (4) pelan penguraian risiko(RTP) yang dibuat pada tahun 2015 masih belum ditutup. Ketiga-tiga pelan tersebut telah disemak dikemas kini status terkini semasa perbentangan di dalam mesyuarat kajian semula pengurusan pada 30 Jun 2016 dan mesyuarat Jawatankuasa Kerja ISMS pada 26 Ogos 2016. Antara ancaman-ancaman yang dikenal pasti ialah bencana alam seperti banjir, kegagalan perkakasan, dan juga risiko terhadap *Cash Box* yang menyimpan wang pembayaran yuran oleh prasiswazah semasa hari pendaftaran.

Merujuk kepada laporan yang terkini, status pelaksanaan RTP masih berjalan dan dipantau dari semasa ke semasa. Walau bagaimanapun, penilaian risiko yang dibuat perlulah lebih komprehensif dan pelaporan terhadap tahap risiko yang dikenal pasti melalui MyRAM dan laporan yang dikemukakan semasa mesyuarat kajian semula pengurusan perlulah selaras. – Rujuk Laporan Peluang Penambahbaikan.

5.4 Overall Implementation of Security Controls:

Merujuk kepada SOA yang terkini, sebanyak 113 kawalan yang digunapakai oleh pihak organisasi.

Terdapat lima (5) objektif keselamatan yang dibangunkan. Pengukuran terhadap kelima-lima objektif tersebut telah buat dan dibentangkan di dalam MKSP. Pengendalian ke atas insiden-insiden yang dilaporkan juga baik. Pengujuian Simulasi DRP ICT UPM telah buat pada 24/6/2016.

Secara keseluruhannya, audit mendapati, pelaksanaan kawalan keselamatan bagi proses pendaftaran baharu prasiswazah semasa Minggu Perkasa Putra, pengurusan pusat data serta pusat pemulihan data adalah baik. Walau bagaimanapun, terdapat beberapa pelaksanaan bagi kawalan-kawalan keselamatan yang perlu diperkemaskan lagi. Rujuk Laporan Peluang Penambahbaikan.

5.4 Continual Improvement :

Penambahbaikan berterusan dapat dilihat daripada tindakan yang diambil hasil daripada penemuan audit dalam ISMS, perbincangan MKSP dan mesyuarat jawatankuasa kerja ISMS, penambahbaikan proses-proses kerja dan bengkel-bengkel berkaitan ISMS.

5.5 Useful comparisons with previous audit results :

Tiada laporan ketakakuran dikeluarkan.

6. NONCONFORMITY REPORT

Total no. of minor NCR(s) : - List : -

7. ANY UNRESOLVED ISSUES, IF IDENTIFIED

No unresolved issue identified.

SURVEILLANCE AUDIT REPORT

8. SUMMARY OF FINDINGS – Maturity of system and effectiveness of system in meeting set objectives including agreed requirements and other positive and negative observations

Organisasi telah memastikan bahawa kaedah penilaian risiko dapat menangani semua keperluan yang berkaitan. Terdapat juga bukti-bukti yang menunjukkan pelaksanaan kawalan untuk mengurangkan risiko yang dikenal pasti.

Secara keseluruhan, organisasi telah melaksanakan Sistem Pengurusan Keselamatan Maklumat (ISMS) dengan baik. Komitmen daripada pihak pengurusan dan kesedaran daripada pegawai juga jelas. Audit mendapati bahawa pengurusan dan pelaksanaan ISMS di UPM bertambah baik berbanding dengan tahun-tahun yang lepas.

Walau bagaimanapun, isu yang diketengahkan dalam Laporan Peluang Penambahbaikan boleh diambil kira bagi mengukuhkan lagi pelaksanaan keseluruhan ISMS di Universiti Putra Malaysia.

9. RECOMMENDATION :

[√] No NCR recorded. Recommended to continue certification *with/ ~~without~~ change.

[ ] NCR(s) recorded. Recommended to continue certification *with/ without change conditional upon satisfactory verification of corrective actions taken. Recommendation to continue certification *with/ without change will be made after :

- [ ] On-site audit of the following area(s) including verification of corrective action : _____
- [ ] Off-site verification of corrective action(s). Records of implementation of proposed corrective action to be submitted for verification.

* Nature of change (if applicable) : Perubahan ke atas pemakaian kawalan di dalam Statement of Applicability (SOA).

- [ ] Suspension of certification, a re-audit of the system shall be carried out before a recommendation is made to lift the suspension.
- [ ] Withdrawal

Note :

a) *Corrective Action Plans for all nonconformities (minor/ major) raised shall be submitted to the Audit Team Leader within one month and evidence of implementation within 3 months of the date of this report. Failure to comply shall result in either suspension or withdrawal of the certification.*

b) *If there is any unresolved issue at the end of the audit, it shall be brought to the attention of the management of SIRIM QAS Intl for resolution. The client will be notified in writing of the decision within two weeks of the date of this report.*

FOLLOW UP ON NCR(s)

~~It is confirmed that all corrective actions taken have been satisfactorily verified.~~ Recommended to continue certification.

Audit Team Leader :	NUR AISYA MOHD. ZAMRI		30 Sept. 2016
	(Name)	(Signature)	(Date)

SURVEILLANCE AUDIT REPORT

SUMMARY BY FUNCTION/ DEPARTMENT/ PROCESS/ PROJECT SITE

ISO/IEC 27001: 2013		Requirement audited	FUNCTION / DEPARTMENT/ PROJECT SITE											NCR
			Pengurusan dan CQA	Bhgn. Kemasukan dan Bhgn. Urus Tadbir Akademik	Pusat Kesihatan Universiti	Pusat Pembangunan dan Komunikasi (iDEC)	Pej. Strategik Korporat dan Komunikasi	Pej. Penasihat Undang-undang	Bhgn. Keselamatan	Pej. Bursar	Kolej (Zone 1 dan Zone 3)			
4	**Context of the organizations.**													
4.1	Understanding the organization and its context.	√	√											
4.2	Understanding the needs and expectations of interested parties	√	√											
4.3	Determining the scope of the information security management system	√	√											
4.4	Information security management system	√	√											
5	**Leadership**													
5.1	Leadership and commitment	√	√											
5.2	Policy	√	√											
5.3	Organizational roles, responsibilities and authorities	√	√											
6	**Planning**													
6.1	Actions to address risks and opportunities	√	√	√	√	√	√	√	√	√	√			
6.2	Information security objectives and plans to achieve them	√	√	√	√	√	√	√	√	√	√			
7	**Support**													
7.1	Resources	√	√											
7.2	Competence	√	√											
7.3	Awareness	√	√											
7.4	Communication	√	√	√	√	√	√	√	√	√	√			
7.5	Documented information.	√	√	√	√	√	√	√	√	√	√			
8	**Operation**													
8.1	Operation planning and control	√	√	√	√	√	√	√	√	√	√			
8.2	Information security risk assessment	√	√	√	√	√	√	√	√	√	√			
8.3	Information security risk treatment	√	√	√	√	√	√	√	√	√	√			
9	**Performance evaluation**													
9.1	Monitoring, measurement, analysis and evaluation.	√	√											
9.2	Internal Audit	√	√											
9.3	Management Review	√	√											
10	**Improvement**													
10.1	Nonconformity and corrective action	√	√	√	√	√	√	√	√	√	√			
10.2	Continual improvement	√	√	√	√	√	√	√	√	√	√			
	Total No. of NCR(s)		0	0	0	0	0	0	0	0	0			0

Note :

a) Indicate in the "Requirement audited" column with a (√) the requirements that were audited and (-) for requirements that were not audited.

b) In the case where requirements were audited and nonconformities detected, replace the (√) with the number of nonconformities (No of major/ no. of minor)

c) Indicate with (NA) if the requirement is not applicable

APPENDIX 1

VERIFICATION OF-PREVIOUSLY RAISED NONCONFORMITY REPORTS

No.	NCR Reference No.	Evidence sighted for the implementation of the corrective action	Effectiveness of corrective action (Y/N)	Remarks
1.	NR-1	Tiada isu yang berulang. Tindakan pembetulan yang dibuat ke atas penemuan audit sebelum ini berkesan.	Y	

Note:
If the corrective action has not been effectively implemented, a new NCR shall be reissued and indicate in the "Remarks" column.

Auditor Name: Nur Aisya Mohd. Zamri

Date: 30/9/2016

APPENDIX 2

LIST OF ADDITIONAL SITE(S)				
No.	**Address of site**	**Scope (if different from the main site)**	**No. of employees**	**Audited / Not Audited**
1.	Universiti Putra Malaysia Beta Data Centre 43400 Serdang, Selangor Darul Ehsan.	Sistem Pengurusan Keselamatan Maklumat Bagi Pengoperasian Pusat Data Bagi Pendaftaran Pelajar Baharu Prasiswazah	6	Diaudit
2.	Universiti Putra Malaysia Epsilon Data Recovery Centre 43400 Serdang, Selangor Darul Ehsan.	Sistem Pengurusan Keselamatan Maklumat Bagi Pengoperasian Pusat Pemulihan Data Bagi Pendaftaran Pelajar Baharu Prasiswazah		Tidak diaudit

APPENDIX 3

LIST OF REMOTE SUPPORT FUNCTIONS				
No.	**Address**	**Activities**	**No. of employees**	**Audited / Not Audited**
	Tidak berkaitan			

Rujukan fail: IS / 6 – 80

PELUANG PENAMBAHBAIKKAN		
Klausa	**Butiran**	**Komen terhadap tindakan yang telah diambil**
	(Efizan Zamri – 31/8/2016)	
6.1	***Actions to address risks and opportunities*** Semasa pendaftaran pelajar, kaunter semakan dikendalikan oleh fasilitator universiti dan telah disemak dari segi kecukupan dokumen. Organisasi boleh menambahbaik dari segi verifikasi di mana pelajar yang mendaftar adalah pelajar yang berkenaan bagi mengelak risiko bukan pelajar yang sebenar mendaftar.	
8.1 A.8.2.2	***Operational planning and control*** ***Labelling of information*** Didapati pemakaian fail pelajar yang di tempatkan di Kolej boleh dilihat kembali bagi memastikan fail tersebut yang memiliki sensitiviti informasi atau peribadi dapat dijaga dan diatur melalui prosedur yang sepatutnya.	
	(Sazlin Alias – 29/9/2016)	
8.1 A.15.1.2	***Operational planning and control*** ***Addressing security within supplier agreements*** Keperluan kerahsiaan perlu diambil kira didalam penyediaan Perjanjian Perkhidmatan Peyelenggaraan Peralatan. Rujuk CR Classic, Laser Imager and Remote Operation di Unit Radialogi, Pusat Kesihatan Universiti.	
	(Nur Aisya Mohd. Zamri - 29-30/9/2016)	
6.1.3 (a)	***Information security risk treatment*** Audit mendapati salah satu tahap risiko yang dikenal pasti semasa membuat penilaian risiko melalui aplikasi MyRAM adalah tidak selaras seperti mana yang dilaporkan di dalam MKSP.	
	Laporan tamat	

Juruaudit: NUR AISYA MOHD. ZAMRI / SAZLIN ALIAS / EFIZAN ZAMRI Tarikh: 31/8, 29-30/9/2016

Rujukan fail: IS /6-80

PELUANG PENAMBAHBAIKKAN		
Klausa	**Butiran**	**Komen terhadap tindakan yang telah diambil**
6.1.2(c)	***Information security risk assessment*** Penilaian risiko telah dilaksanakan oleh organisasi. Walau bagaimanapun penilaian ini boleh disemak semula bagi memastikan kesemua aset yang terlibat termasuk komputer pengguna dinilai risikonya. Sampel yang dilihat di Pejabat Bursar dan Bahagian Keselamatan.	
8.1 **A.12.2.1**	***Operational planning and control*** ***Control against malware*** Semasa pengauditan di Pejabat Bursar dan Bahagian Keselamatan masih terdapat beberapa computer (pc) anggota kerja yang belum dipasang antivirus.	
A.17.1.1	***Planning information security continuity*** Pelan Komunikasi Krisis Versi 2.0 telah dibangunkan. Namun demikian kandungan terhadap pelan ini boleh ditambah baik dengan memasukkan senarai kakitangan dan nombor telefon yang boleh dihubungi semsas berlakunya krisis.	
A.17.1.3	***Verify, review and evaluate information security continuity*** Pelan Pemulihan Bencana dan Laporan Pengujian Simulasi DRP ICT UPM 2016 Versi 4.0 telah dibangunkan. Walau bagaimanapun apabila pengauditan dijalankan terhadap Borang Laporan Perlaksanaan Pemulihan untuk sistem aplikasi, pangkalan data dan rangkaian tiada dicatatkan masa sebenar yang diambil untuk pemulihan bencana **LAPORAN TAMAT**	

Juruaudit : Noridah Binti Yahya

Tarikh: 30 September 2016