

SULIT

	SIRIM QAS INTERNATIONAL SDN. BHD. JABATAN PENSIJILAN SISTEM PENGURUSAN Blok 4, Kompleks SIRIM, No. 1, Persiaran Dato' Menteri Seksyen 2, 40700 Shah Alam, Selangor Darul Ehsan SISTEM PENGURUSAN KESELAMATAN MAKLUMAT LAPORAN AUDIT PEMANTAUAN	No. Fail : 20190602821																
ORGANISASI : UNIVERSITI PUTRA MALAYSIA																		
ALAMAT LOKASI UTAMA YANG DIAUDIT (Untuk pensijilan berkelompok, senarai lokasi tambahan adalah seperti dilampiran - Lampiran 2 dan Lampiran 3): 43400 SERDANG SELANGOR DARUL EHSAN MALAYSIA																		
NOMBOR PENSIJILAN : ISMS 00150		STANDARD : ISO/IEC 27001:2013																
TARIKH AUDIT : 1 Sept., 7 - 9 Okt. 2019 /_6_hari auditor		TARIKH AUDIT YANG LEPAS : 1 – 10 Okt. 2018																
SKOP PENSIJILAN : 1) SISTEM PENGURUSAN KESELAMATAN MAKLUMAT BAGI PROSES PENDAFTARAN PELAJAR BAHARU PRASISWAZAH MERANGKUMI AKTIVITI SEMAKAN TAWARAN HINGGA PENDAFTARAN KOLEJ KEDIAMAN. 2) SISTEM PENGURUSAN KESELAMATAN MAKLUMAT BAGI PROSES PENILAIAN PENGAJARAN PRASISWAZAH DI FAKULTI.																		
<table style="width: 100%; border: none;"> <tr> <td style="width: 15%;">PASUKAN AUDIT :</td> <td style="width: 45%;">1) Nur Aisya Mohd Zamri</td> <td style="width: 20%;">Ketua Juruaudit</td> <td style="width: 20%;">3 hari audit</td> </tr> <tr> <td></td> <td>2) Noridah Yahya</td> <td>Juruaudit</td> <td>2 hari audit</td> </tr> <tr> <td></td> <td>3) Azran Mohammad Ridzuan</td> <td>Juruaudit</td> <td>1 hari audit</td> </tr> <tr> <td></td> <td>4)</td> <td></td> <td></td> </tr> </table>			PASUKAN AUDIT :	1) Nur Aisya Mohd Zamri	Ketua Juruaudit	3 hari audit		2) Noridah Yahya	Juruaudit	2 hari audit		3) Azran Mohammad Ridzuan	Juruaudit	1 hari audit		4)		
PASUKAN AUDIT :	1) Nur Aisya Mohd Zamri	Ketua Juruaudit	3 hari audit															
	2) Noridah Yahya	Juruaudit	2 hari audit															
	3) Azran Mohammad Ridzuan	Juruaudit	1 hari audit															
	4)																	
BILANGAN KAKITANGAN (yang berkaitan dengan skop pensijilan): 3,745 kakitangan (Nota: Kakitangan tetap dan sementara tidak termasuk bilangan kakitangan di Lampiran 2 dan Lampiran 3)																		
<u>Laporan oleh Ketua Pasukan Audit</u> Nama : NUR AISYA MOHD ZAMRI Tandatangan : Tarikh : 9 OKTOBER 2019 		<u>Pengesahan daripada Wakil Organisasi</u> Nama : Tandatangan : Tarikh : 9 OKTOBER 2019 																
Rancangan Audit dan lampiran berikut adalah sebahagian daripada laporan ini : <table style="width: 100%; border: none;"> <tr> <td style="width: 70%;">Laporan Ketakakuran (NCR)</td> <td style="width: 30%; text-align: center;">☒</td> </tr> <tr> <td>Peluang Penambahbaikan (OFI)</td> <td style="text-align: center;">☒</td> </tr> <tr> <td>Senarai Lokasi Tambahan</td> <td style="text-align: center;">☒</td> </tr> <tr> <td>Senarai Lokasi Fungsi Sokongan</td> <td style="text-align: center;">☒</td> </tr> <tr> <td colspan="2">Tandakan (✓) yang berkenaan</td> </tr> </table>		Laporan Ketakakuran (NCR)	☒	Peluang Penambahbaikan (OFI)	☒	Senarai Lokasi Tambahan	☒	Senarai Lokasi Fungsi Sokongan	☒	Tandakan (✓) yang berkenaan		Laporan disemak oleh : (Juruaudit Kanan/ Ketua Seksyen) Tarikh						
Laporan Ketakakuran (NCR)	☒																	
Peluang Penambahbaikan (OFI)	☒																	
Senarai Lokasi Tambahan	☒																	
Senarai Lokasi Fungsi Sokongan	☒																	
Tandakan (✓) yang berkenaan																		

LAPORAN AUDIT PEMANTAUAN

1. PERUBAHAN KETARA YANG DIBUAT KEPADA RANCANGAN AUDIT (JIKA BERKENAAN)

Tiada perubahan ketara yang dibuat terhadap rancangan audit.

2. PINDAAN KETARA KEPADA SISTEM PENGURUSAN KESELAMATAN MAKLUMAT ORGANISASI SEJAK AUDIT SEBELUMNYA (JIKA BERKAITAN)

Antara pindaan yang telah dilaksanakan kepada sistem pengurusan keselamatan maklumat organisasi adalah:

- I) Pelaksanaan semakan kajian semula pengurusan digabungkan bersama-sama Sistem Pengurusan Alam Sekitar (EMS),
- II) Kawalan keselamatan bagi A.6.1.5 di dalam *Statement of Applicability* (SOA) telah disemak dan dipinda pemakaiannya kepada "YA", dan
- III) Semakan dan pindaan ke atas beberapa ISMS Objektif.

3. NO. SEMAKAN PENYATAAN PEMAKAIAN (SOA) : BERTARIKH 3 OKTOBER 2019.

4. RINGKASAN KEBERKESANAN TINDAKAN YANG TELAH DIAMBIL KE ATAS KETAKAKURAN YANG DIKELUARKAN PADA AUDIT TERDAHULU (Senaraikan perincian laporan ketakakuran dan status di Lampiran 1)

Tiada ketakakuran yang dikeluarkan pada audit terdahulu. Namun semua peluang penambahbaikan telah disemak dan ditutup.

5. PENGGUNAAN LOGO PENSIJILAN / AKREDITASI & DOKUMEN PENSIJILAN (SIJIL)

☐

Tidak digunakan

☐

Digunakan; tidak diterima

☐

/

Digunakan; diterima

Tindakan yang diperlukan:

6. RINGKASAN PENEMUAN AUDIT

6.1 Keberkesanan audit dalaman

Pelaksanaan audit dalaman ISMS dapat dirumuskan seperti berikut:

- Audit dalaman ISMS telah dilaksanakan pada 13 – 16 Mei 2019 oleh 35 juruaudit dan 38 penolong juruaudit
- Liputan audit adalah menyeluruh
- Sebanyak 11 laporan ketidakpatuhan (NCR) dan 38 Laporan penambahbaikan (OFI) direkodkan bagi sesi pengauditan kali ini
- Pengendalian penemuan-penemuan audit dalaman ini adalah baik.

Secara keseluruhannya, pelaksanaan audit dalaman dan penyelenggaraan rekod-rekod audit dalam adalah amat memuaskan.

6.2 Kajian semula pengurusan

Pelaksanaan kajian semula pengurusan dan dirumuskan seperti berikut:

- Mesyuarat Kajian Semula Pengurusan (MKSP) adalah platform bagi menyemak tahap pelaksanaan dan pencapaian sistem pengurusan. Yang terkini dilaksanakan pada 11 September 2019 yang dipengerusikan oleh Naib Canselor UPM dan dihadiri oleh wakil-wakil yang terlibat.
- Disamping itu, terdapat juga mesyuarat-mesyuarat lain yang dijalankan bagi membincangkan pengurusan dan pengoperasian yang berkaitan pelaksanaan ISMS di setiap pusat dan bahagian.
- Hasil perbincangan direkodkan di dalam minit mesyuarat yang berkaitan.

Secara keseluruhannya, pelaksanaan kajian semula pengurusan adalah baik. Semua agenda telah dibincangkan dan dirumuskan di dalam mesyuarat bersama pihak atasan adalah memenuhi keperluan standard ISMS.

LAPORAN AUDIT PEMANTAUAN

6.3 Penaksiran risiko keselamatan maklumat

Penaksiran risiko keselamatan maklumat dapat dirumuskan seperti di bawah:

- Metodologi Pengurusan Risiko telah disediakan melalui dokumen *Risk Assessment and Risk Treatment Plan Guideline* bagi memastikan pentaksiran risiko keselamatan maklumat menghasilkan keputusan yang konsisten, sah dan dapat dibandingkan.
- Laporan pentaksiran risiko terkini telah dikeluarkan dan diluluskan oleh pihak pengurusan pada Ogos 2019 bagi proses-proses Pendaftaran Pelajar Baharu Prasiswazah (UPM Serdang), Pendaftaran Pelajar Baharu Prasiswazah (UPM Kampus Bintulu), Penilaian Pengajaran Prasiswazah di Fakulti, dan Pusat Data (IDEC).
- Hasil daripada pentaksiran risiko terkini, terdapat tiga (3) pelan penguraian risiko yang telah dibangunkan berkaitan sistem perparitan bagi pusat data di IDEC, pembangunan pusat data baru, dan pembelian server aplikasi BLASTTA untuk dijadikan server DR kekal.

Secara keseluruhannya, pelaksanaan proses penaksiran risiko serta pemantauan terhadap pelan penguraian adalah memenuhi keperluan standard.

6.4 Kawalan keselamatan maklumat secara keseluruhan

Pelaksanaan kawalan keselamatan maklumat di UPM dapat dirangkumkan seperti di bawah:

- Merujuk kepada Penyataan Pemakaian (SOA) yang bertarikh 3 Oktober 2019, didapati tiada pengecualian terhadap 114 kawalan keselamatan sepertimana yang dinyatakan di dalam keperluan standard Annex A.
- Tujuh (7) ISMS objektif telah dibuat pengukuran dan dibentangkan semasa kajian semula pengurusan. Namun, semakan dan pindaan terhadap objektif-objektif ini juga telah dibuat selaras mengikut kesesuaian pada masa kini. Ini menjadikan empat (4) ISMS objektif yang terkini berkuatkuasa Julai 2019.
- Pengendalian insiden keselamatan dan pelaksanaan pengujian pemulihan bencana juga baik.

Secara keseluruhannya, kawalan keselamatan yang dilaksanakan dapat mengurangkan risiko keselamatan bagi bagi proses pendaftaran baharu prasiswazah merangkumi aktiviti semakan tawaran hingga pendaftaran kolej kediaman, proses penilaian pengajaran serta pengoperasian pusat data.

6.5 Penambahbaikan berterusan

Inisiatif-inisiatif yang dibuat bagi memastikan penambahbaikan berterusan dapat dilihat berdasarkan hasil penilaian risiko yang dibuat, maklum balas daripada pihak-pihak berkepentingan, tindakan yang dilaksanakan terhadap penemuan audit dalam serta hasil perbincangan semasa mesyuarat yang berkaitan.

6.6 Perbandingan berguna dengan keputusan audit yang lepas

Satu (1) laporan ketakakuran kecil dikeluarkan rentetan daripada laporan peluang penambahbaikan semasa audit yang lepas dan empat (4) peluang penambahbaikan dilaporkan pada audit semasa.

7. LAPORAN KETAKAKURAN (NCR)

Jumlah Ketakakuran Kecil (minor NCR) : 1 Senarai : NCR03902821-1

Jumlah Ketakakuran Besar (major NCR) : - Senarai : -

Kumpulan ketakakuran kecil yang membawa kepada ketakakuran besar : -

8. ISU-ISU YANG TIDAK DAPAT DISELESAIKAN, JIKA BERKENAAN

Tiada isu – isu yang tidak dapat diselesaikan.

9. ISU-ISU PENTING YANG MUNGKIN MEMBERI KESAN KEPADA PROGRAM AUDIT

Tiada isu yang mungkin memberi kesan kepada program audit.

LAPORAN AUDIT PEMANTAUAN

10. KESIMPULAN KEPADA KEPATUHAN DAN KEBERKESANAN SISTEM

Secara keseluruhannya, komitmen terhadap pelaksanaan ISMS pada amnya adalah baik dan berterusan. Kefahaman dan pelaksanaan dapat dilihat melalui rekod-rekod yang disemak serta kesungguhan anggota kerja di semua peringkat. Koordinasi dan amalan bekerja secara berkumpulan dilihat berjaya memantapkan lagi pelaksanaan ISMS. Penglibatan daripada fungsi sokongan juga dilihat sangat memuaskan.

Bagi mengukuhkan lagi ISMS yang sedia ada, penambahbaikan yang direkodkan didalam Laporan Ketakakuran dan Peluang Penambahbaikan perlulah disemak dan mengambil tindakan yang sesuai agar dapat memperkemaskan lagi pelaksanaan ISMS di Universiti Putra Malaysia.

11. KESESUAIAN SKOP PENSIJILAN

☒

Ya

☐

Tidak (sila komen) :

12. ADAKAH KESEMUA OBJEKTIF AUDIT TELAH DIPENUHI?

☒

Ya

☐

Tidak (sila komen) :

13. PENGESYORAN :

☐

Tiada Laporan Ketakakuran. Disyorkan untuk diteruskan pensijilan *dengan/ tanpa pindaan.

☒

Laporan Ketakakuran Kecil direkodkan. Disyorkan untuk diteruskan pensijilan ***dengan/ tanpa** pindaan setelah Laporan Ketakakuran ditutup dengan memuaskan.

☐

Laporan Ketakakuran Besar direkodkan. Pengesyoran untuk diteruskan pensijilan *dengan/ tanpa pindaan hanya akan dibuat setelah :

☐

Audit di lokasi terhadap keperluan berikut termasuk verifikasi terhadap tindakan pembetulan :

☐

Verifikasi terhadap tindakan pembetulan di luar lokasi audit. Bukti pelaksanaan tindakan pembetulan hendaklah dikemukakan untuk verifikasi.

* Jenis pindaan :
(sekiranya berkaitan)

Pindaan terhadap pemakaian kawalan di dalam *Statement of Applicability (SOA)*.

☐

Penggantungan pensijilan. Audit semula perlu dijalankan sebelum pengesyoran untuk menarik penggantungan yang telah dibuat.

☐

Penarikan balik pensijilan.

- Nota :**
- a) *Pelan tindakan pembetulan untuk kesemua ketakakuran yang dikeluarkan hendaklah dihantar kepada Ketua Pasukan Audit dalam tempoh 1 bulan dan bukti pelaksanaan dalam tempoh 3 bulan dari tarikh laporan ini. Kegagalan mematuhi kehendak ini boleh menyebabkan pensijilan digantung atau ditarik balik.*
 - b) *Jika terdapat sebarang isu yang tidak dapat diselesaikan pada akhir audit, ia akan dibawa kepada perhatian pengurusan SIRIM QAS Intl untuk diputuskan. Pelanggan akan diberitahu secara bertulis keputusan itu dalam tempoh dua minggu dari tarikh laporan ini.*
 - c) *Jika bukti tindakan pembetulan yang dikemukakan tidak mencukupi, SIRIM QAS Intl berhak untuk menjalankan semula audit bagi mengesahkan keberkesanan tindakan pembetulan yang telah diambil.*

LAPORAN AUDIT PEMANTAUAN

SUSULAN TERHADAP KETAKAKURAN YANG DIKELUARKAN

Adalah disahkan kesemua tindakan pembetulan yang diambil adalah memuaskan. Disyorkan untuk diteruskan pensijilan.

Ketua Pasukan Audit : Nur Aisya Mohd Zamri

(Nama)

(Tandatangan)

(Tarikh)

LAPORAN AUDIT PEMANTAUAN													
(RINGKASAN MENGIKUT FUNGSI/ PROSES/ LOKASI PROJEK)													
ISO/ IEC 27001:2013		KEPERLUAN YANG DIAUDIT	FUNGSI/ PROSES/ LOKASI PROJEK										LAPORAN KETAKAKURAN
			Urusetia / Pusat Jaminan Kualiti	Pusat Pembangunan Maklumat & Komunikasi - IDEC	Bhgn. Kemasukan & Bhgn Urus Tadbir Akademik	Bhgn Hal Ehwal Pelajar	Pej. Strategi Korporat & Komunikasi	Pej. Penasihat Undang-Undang	Kolej Kediaman – Kolej 10 dan KTDI	Fakulti – Kejuruteraan dan Rekabentuk dan Senibina	UPM Kampus Bintulu		
4	Konteks organisasi												
4.1	Memahami organisasi dan konteksnya	/	/										0
4.2	Memahami keperluan dan jangkaan pihak yang berkepentingan	/	/										0
4.3	Menentukan skop sistem pengurusan keselamatan maklumat	/	/										0
4.4	Sistem pengurusan keselamatan maklumat	/	/										0
5	Kepimpinan												
5.1	Kepimpinan dan komitmen	/	/										0
5.2	Dasar keselamatan	/	/										0
5.3	Peranan, tanggungjawab dan bidang kuasa organisasi	/	/										0
6	Perancangan												
6.1	Tindakan menyatakan risiko dan peluang	/	/	/	/	/	/	/	/	/	/		0
6.2	Objektif keselamatan dan perancangan untuk mencapainya	/	/	/	/	/	/	/	/	/	/		0
7	Sokongan												
7.1	Sumber	/	/										0
7.2	Kekompetenan	/	/										0
7.3	Kesedaran	/	/	/	/	/	/	/	/	/	/		0
7.4	Komunikasi	/	/	/	/	/	/	/	/	/	/		0
7.5	Maklumat didokumentasikan	/	/	/	/	/	/	/	/	/	/		0
8	Operasi												
8.1	Perancangan dan kawalan operasi	/	/	/	/	/	/	/	/	/	/		0
8.2	Penilaian risiko	/	/	/	/	/	/	/	/	/	/		0
8.3	Pemulihan risiko	/	/	/	/	/	/	/	/	/	/		0
9	Penilaian prestasi												
9.1	Pemantauan, pengukuran, analisis dan penilaian	/	/										0
9.2	Audit dalaman	/	/										0
9.3	Kajian semula pengurusan	/	/										0
10	Penambahbaikan												
10.1	Ketidakakuran dan tindakan pembetulan	/	1	/	/	/	/	/	/	/	/		1
10.2	Penambahbaikan berterusan	/	/	/	/	/	/	/	/	/	/		0
Lain-lain keperluan pensijilan													
1.	Penggunaan logo pensijilan/ sijil	/	/										0
	Jumlah ketidakakuran	0	1	0	0	0	0	0	0	0	0	0	1

Nota :

- a) Tandakan (√) di kotak yang berkenaan untuk keperluan standard yang telah diaudit dan memuaskan dan tandakan "TB" sekiranya keperluan standard tidak berkaitan.
b) Sekiranya ada ketidakakuran dikeluarkan, gantikan tanda (√) dengan jumlah ketidakakuran (contoh: jika satu ketidakakuran dikeluarkan semasa audit dijalankan, sila tandakan (1)).

[illegible]

Jika tindakan pembetulan tidak dilaksanakan dengan berkesan, Laporan Ketakakuran baru akan dikeluarkan semula dan rekodkan di ruangan “Ulasan”.

Tarikh : 9 Oktober 2019

SENARAI LOKASI KEKAL TERMASUK LOKASI UTAMA					
No. Fail : 20190602821					
No.	Alamat Lokasi	Tarikh Audit	Skop (sekiranya berbeza daripada lokasi utama)	Bilangan kakitangan	Diaudit/ Tidak diaudit
1	Universiti Putra Malaysia 43400 Serdang, Selangor.	7 - 9 Okt. 2019	Sistem Pengurusan Keselamatan Maklumat Bagi Proses Pendaftaran Pelajar Baru Prasiswazah Merangkumi Aktiviti Semakan Tawaran Hingga Pendaftaran Kolej Kediaman.	3,745	Diaudit
2.	Universiti Putra Malaysia Kampus Bintulu Sarawak Jalan Nyabau, 97008 Bintulu, Sarawak.	1 Sept. 2019	Sistem Pengurusan Keselamatan Maklumat Bagi Proses Pendaftaran Pelajar Baru Prasiswazah Merangkumi Aktiviti Semakan Tawaran Hingga Pendaftaran Kolej Kediaman.	289	Diaudit

SENARAI LOKASI FUNGSI SOKONGAN					
No. Fail : 20190602821					
No.	Alamat Lokasi	Tarikh Audit	Aktiviti	Bilangan kakitangan	Diaudit/ Tidak diaudit
1.	Universiti Putra Malaysia Bahagian Media Arkib dan Pemuliharaan Perpustakaan UPM, 43400 Serdang, Selangor	-	Pusat simpanan media backup	0	Tidak diaudit
2.	Universiti Putra Malaysia Beta Data Centre, 43400 Serdang, Selangor.	7 Okt. 2019	Pusat Data	0	Diaudit
3.	Universiti Putra Malaysia Epsilon Data Recovery Centre, 43400 Serdang, Selangor.	-	Pusat Pemulihan Bencana (DRC)	0	Tidak diaudit

SIRIM QAS INTERNATIONAL SDN. BHD.**File No :** 20190602821**NONCONFORMITY REPORT (NCR)****NCR No :** NCR03902821**Audit Type :** Surveillance 1 Audit**Classification :** Minor**Last audit date :** 09-Oct-2019**Standard Name:** ISO/IEC 27001:2013

Page 1 of 3

Client : UNIVERSITI PUTRA MALAYSIA**Section 1 - Details of nonconformity****Requirement:****Standard ISO/IEC 27001:2013****10.1 Ketakakuran dan tindakan pembetulan**

b) menilai keperluan untuk bertindak menghapuskan punca ketakakuran, supaya ia tidak berulang atau berlaku di tempat lain, dengan:

- 1) mengkaji semula ketakakuran;
- 2) menentukan punca ketakakuran; dan
- 3) menentukan jika ketakakuranyang serupa wujud, atau berpotensi berlaku;

Finding:

Terdapat tiga (3) penemuan Laporan Peluang Penambahbaikan audit yang dilaporkan pada audit lepas (1-3 Oktober 2018) berlaku pengulangan.

Objective evidence:

Bukti Penemuan :

Laporan peluang penambahbaikan audit 2018 untuk klausa dan kawalan Keselamatan berikut:

1. Klausa 8.1 (A.11.2.8) - Peralatan pengguna tanpa jagaan

- PC pentadbir sistem Penilaian Pengajaran di Fakulti Kejuruteraan tidak mempunyai kawalan untuk komputer yang ditinggalkan tanpa jagaan.

2. Klausa 8.1 (A.12.2.1) – Kawalan daripada perisian hasad

- PC pentadbir sistem Penilaian Pengajaran di Fakulti Kejuruteraan tidak menegemaskini definisi antivirus yang terkini dan

imbasan tidak dilaksanakan pada sela masa yang sewajarnya.

Tarikh kemaskini yang terakhir adalah pada 31 Julai 2017 dan imbasan yang terakhir pada 23 Februari 2019

3. Klausa 8.1 (A.9.3.1) - Penggunaan maklumat pengesahan rahsia

- Kata laluan yang dimasukkan tidak mematuhi Garis Panduan Pengurusan Identiti.

Lokasi : Fakulti Kejuruteraan

Kata laluan untuk kemasukan ke PC: Kombinasi kata laluan hanya mengandungi huruf sahaja

Kata laluan untuk kemasukan Sistem Penilaian Pengajaran (*Putrablast*) : Kombinasi kata laluan hanya mengandungi huruf sahaja

SIRIM QAS INTERNATIONAL SDN. BHD.		
File No : 20190602821	NONCONFORMITY REPORT (NCR)	NCR No : NCR03902821
Audit Type : Surveillance 1 Audit	Classification : Minor Standard Name: ISO/IEC 27001:2013	Last audit date : 09-Oct-2019 Page 2 of 3
Client : UNIVERSITI PUTRA MALAYSIA		
<u>Lokasi : Kolej 10</u> Kata laluan untuk kemasukan Sistem Maklumat Pelajar (SMP) : Kombinasi kata laluan tidak mempunyai symbol <u>Lokasi : Kolej TunDr Ismail (KTDI)</u> Kata laluan untuk kemasukan Sistem Maklumat Pelajar (SMP) : • Admin 1: Kombinasi kata laluan hanya mengandungi nombor sahaja • Admin 2: Kata laluan yang dimasukkan kurang daripada 8 aksara (6 aksara sahaja) serta tidak mengandungi symbol. Justification (for IATF only) : Auditor NORIDAH BINTI YAHYA Client Representative		
Section 2 - Result of investigation and determination of root cause Client Representative:		
Section 3 - Correction (if applicable) and corrective action plan including completion date Client Representative:Accepted by		

SIRIM QAS INTERNATIONAL SDN. BHD.**File No :** 20190602821**NONCONFORMITY REPORT (NCR)****NCR No :** NCR03902821**Audit Type :** Surveillance 1 Audit**Classification :** Minor
Standard Name: ISO/IEC 27001:2013**Last audit date :** 09-Oct-2019

Page 3 of 3

Client : UNIVERSITI PUTRA MALAYSIA**Section 4 - Verification of corrective action(s) (to be filled up by Auditor)**

Verified by: NORIDAH BINTI YAHYA

NCR close out:

Close date:

OPPORTUNITIES FOR IMPROVEMENT		
Clause	Details	Comments on action taken
6.1.3 (d)	Penguraian risiko keselamatan maklumat Rujukan dokumen untuk kawalan A.12.1.2 (Pengurusan perubahan) yang dinyatakan di dalam SOA perlu dilihat semula agar dokumen rujukan yang digunakan merangkumi juga proses perubahan dalaman yang kecil seperti perubahan <i>firewall</i> , perubahan IP dan pengemaskinian <i>security patch</i> .	
8.1	Perancangan dan kawalan operasi <i>A.9.2.6 Penyingkiran atau pelarasan hak akses</i> Senarai hak akses pengguna terhadap VPN yang dikawal di <i>firewall</i> perlu dilihat semula organisasi agar risiko terhadap akses yang tidak sah dapat dikurangkan. Contoh: guest, ruzi_ab.	
8.1	Perancangan dan kawalan operasi <i>A.12.4.4 Penyegerakan jam</i> Waktu pada sistem <i>door access</i> di pusat data dan bilik NOC perlu dilihat semula oleh organisasi supaya disegerakkan mengikut satu sumber rujukan masa yang tepat. (Contoh: Bilik NOC +15 minit awal dan di pusat data -7 minit lewat)	
8.3	Penguraian risiko keselamatan maklumat Proses pentaksiran risiko telah dilaksanakan oleh organisasi dan terdapat beberapa risiko yang berada pada tahap Sederhana (<i>Medium</i>). Maka pihak yang bertanggungjawab mengambil keputusan untuk melaksanakan pelan penguraian risiko. Namun demikian, pelan penguraian risiko tersebut perlu ditambahbaik. Ini kerana Pelan Penguraian Risiko yang dibangunkan adalah sama dengan tindakan sedia ada (<i>Existing Safeguard</i>). Contoh: Penyelenggaraan berkala untuk UPS, genset dan <i>precision cooling unit</i> .	

Auditor : NORIDAH BINTI YAHYA

Date : 08-Oct-2019