	SIRIM QAS INTERNATIONAL SDN. BHD. **JABATAN PENSIJILAN SISTEM PENGURUSAN** **Blok 4, SIRIM Complex, No. 1, Persiaran Dato' Menteri Section 2, 40700 Shah Alam, Selangor Darul Ehsan**	**No. Fail : 20190602821**
	ISMS (ISO/IEC 27001:2022) **LAPORAN AUDIT PEMANTAUAN**	

ORGANISASI:
UNIVERSITI PUTRA MALAYSIA

ALAMAT LOKASI UTAMA YANG DIAUDIT :
(Untuk pensijilan berkelompok, senarai lokasi tambahan adalah seperti di lampiran - Lampiran 3 dan Lampiran 4):

43400 SERDANG
SELANGOR DARUL EHSAN
MALAYSIA

TARIKH AUDIT :22/09/2025 - 26/09/2025 / 7.0 hari auditor	**STANDARD : ISO/IEC 27001:2022 (Including AMD 1:2024)**

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.
3. SISTEM PENGURUSAN KESELAMATAN MAKLUMAT BAGI PROSES PENDAFTARAN PELAJAR BAHARU SEPENUH MASA SISWAZAH MERANGKUMI AKTIVITI PENERIMAAN TAWARAN SEHINGGA PENGESAHAN PENDAFTARAN.

INI ADALAH MENEPATI PENYATAAN PEMAKAIAN: TARIKH KEMASKINI 22/09/2025

PASUKAN AUDIT :

1) NUR FATIN E'ZZATI BINTI MASRUHAIZAN	KETUA JURUAUDIT	5 HARI AUDITOR
2) SAZLIN BINTI ALIAS	JURUAUDIT	2 HARI AUDITOR

BILANGAN KAKITANGAN (yang berkaitan dengan skop pensijilan): 5501 anggota kerja
(Nota: Kakitangan tetap dan sementara tidak termasuk bilangan kakitangan di Lampiran 3 dan Lampiran 4

Laporan oleh Ketua Pasukan Audit

Nama : NUR FATIN E'ZZATI BINTI MASRUHAIZAN

Tarikh : 03/10/2025

	LAPORAN AUDIT PEMANTAUAN
1	**PERUBAHAN KETARA YANG DIBUAT KEPADA RANCANGAN AUDIT (JIKA BERKENAAN)** Tiada perubahan ketara. Audit dijalankan seperti yang dirancang.
2	**PINDAAN KETARA KEPADA SISTEM PENGURUSAN KESELAMATAN MAKLUMAT ORGANISASI SEJAKAUDIT SEBELUMNYA (JIKA BERKAITAN)** Peralihan kepada Sistem Pengurusan Keselamatan Maklumat (ISMS) versi baharu, ISO/IEC 27001:2022, telah bermula pada awal tahun 2025. Dokumentasi ISMS, termasuk Dokumen Rujukan Pelaksanaan ISMS UPM dan Statement of Applicability (SOA), telah dikemas kini selaras dengan pelarasan standard ISO/IEC 27001:2022. Selain itu, perubahan Wakil Pengurusan (ISO) UPM telah dibuat susulan pelantikan baharu Pengarah Pusat Jaminan Kualiti (CQA), UPM yang berkuat kuasa pada 11 Ogos 2025. Universiti Putra Malaysia Kampus Bintulu (UPMKB) juga telah melalui proses penjenamaan semula pada 30 Jun 2025 dan kini dikenali sebagai Universiti Putra Malaysia Sarawak (UPMS).
3	**NO. SEMAKAN PENYATAAN PEMAKAIAN (SOA):** Semakan terkini Statement of Applicability (SOA) telah dilaksanakan pada 22 September 2025. SOA telah dikemaskini selaras dengan pelarasan standard ISO/IEC 27001:2022. Sebanyak 93 kawalan dikenal pasti sebagai terpakai, sama ada pada tahap ‘optimized’ atau ‘initial’, dengan justifikasi yang jelas. Kawalan sedia ada turut dinyatakan dengan merujuk kepada dokumen yang relevan seperti garis panduan, prosedur, dan arahan kerja.
4	**RINGKASAN KEBERKESANAN TINDAKAN YANG TELAH DIAMBIL KE ATAS KETAKAKURAN YANG DIKERLUARKAN PADA AUDIT TERDAHULU (Senaraikan perincian laporan ketakakuran dan status di lampiran 1)** Dalam audit terdahulu, tiada Laporan Ketakakuran (NCR) telah dilaporkan. Sebanyak enam (6) Peluang Penambahbaikan (OFI) telah dikenalpasti, dan kesemuanya telah diambil tindakan oleh pihak UPM serta disahkan ditutup.
5	**PENGGUNAAN LOGO PENSIJILAN / AKREDITASI & DOKUMEN PENSIJILAN (SIJIL)** Teguran berhubung penggunaan logo telah diberikan semasa audit tahun lepas, dan tindakan pembetulan telah diambil di beberapa tempat seperti portal e-ISO. Namun begitu, didapati logo yang digunakan pada business card masih menggunakan logo UKAS yang lama.
6	**RINGKASAN PENEMUAN AUDIT** **6.1 Keberkesanan audit dalaman** Audit dalaman telah dirancang untuk dilaksanakan sekali setahun, dan bagi tahun 2025 ia dijalankan dari 7 April hingga 6 Jun 2025 oleh kumpulan juruaudit dalaman yang dilantik berdasarkan senarai juruaudit dalaman ISO UPM yang dikemaskini pada 7 Mac 2025. Berdasarkan rekod, juruaudit dalaman adalah terlatih serta berkelayakan. Kaedah pengauditan dilaksanakan secara decentralized audit, di mana penjadualan audit dalaman ditentukan dan diuruskan oleh setiap PTJ. Prinsip kesaksamaan (impartiality) dalam proses audit dapat dibuktikan, manakala liputan audit didapati menyeluruh berdasarkan jadual pelaksanaan dan laporan audit yang direkodkan. Hasil penemuan audit dalaman ISMS merekodkan dua (2) Laporan Ketakakuran (NCR) dan dua puluh empat (24) Peluang Penambahbaikan (OFI). Difahamkan bahawa laporan penemuan ini telah dibentangkan oleh Ketua Juruaudit Dalaman ISMS PTJ (KJAD PTJ) semasa Mesyuarat Penutupan Audit Dalaman di PTJ masing-masing. Setakat ini, tindakan pembetulan bagi NCR telah diambil dan sedang dalam proses verifikasi. Manakala bagi OFI, tindakan pembetulan masih dijalankan dan dipantau melalui Portal Jaminan Kualiti (Portal CQA). Secara keseluruhannya, pelaksanaan audit dalaman adalah selaras dengan keperluan standard terkini ISO/IEC 27001:2022. **6.2 Kajian semula pengurusan** Kajian Semula Pengurusan (KSP) dirancang untuk dilaksanakan sekali setahun melalui Mesyuarat Kajian Semula Pengurusan (MKSP) bagi QMS dan ISMS. MKSP terkini telah diadakan pada 19 Ogos 2025, dipengerusikan oleh

Naib Canselor, YBhg. Dato' Prof. Ir. Dr. Ahmad Farhan Mohd. Sadullah, serta dihadiri oleh barisan Pengurusan Universiti, Dekan, Pengarah, Timbalan Wakil Pengurusan, Pegawai CQA dan Timbalan Wakil ISMS. Mesyuarat tersebut telah dijalankan secara hibrid, iaitu melalui aplikasi Google Meet dan bersemuka di Dewan Senat, UPM. Selain itu, Mesyuarat Jawatankuasa Kerja ISMS turut berfungsi sebagai platform tambahan untuk membincangkan pelaporan prestasi pelaksanaan ISMS dan keselamatan maklumat di UPM. Berdasarkan rujukan minit mesyuarat, agenda yang dibentangkan dalam MKSP adalah selaras dengan keperluan standard.

6.3 Penaksiran risiko keselamatan maklumat

Penilaian risiko dilaksanakan oleh organisasi dengan tujuan menilai tahap risiko aset yang terlibat dalam proses di bawah skop ISMS, bagi memastikan pendekatan dan keputusan yang paling berkesan dapat dikenal pasti untuk menyediakan perlindungan serta kawalan terhadap aset tersebut. Penilaian ini adalah berasaskan metodologi MyRAM (Malaysian Public Sector ICT Risk Assessment Methodology) UPM.
Pengemaskinian MyRAM dilaksanakan sekiranya berlaku perubahan atau penambahan aset dalam skop ISMS. Aset dinilai pada tahap Rendah (Low), Sederhana (Medium) atau Tinggi (High) berdasarkan tiga ciri utama keselamatan iaitu Kerahsiaan (Confidentiality), Integriti (Integrity) dan Ketersediaan (Availability). Semakan penilaian risiko telah dilaksanakan pada Mac dan Julai 2025, dan laporan RA telah disediakan bagi enam proses /pasukan berikut:

1. Proses Pendaftaran Pelajar Baharu Siswazah
2. Proses Pendaftaran Pelajar Baharu Prasiswazah Kampus Serdang
3. Proses Pendaftaran Pelajar Baharu Prasiswazah UPMS
4. Sistem Sokongan (Pusat Data)
5. Proses Penilaian Pengajaran Prasiswazah di Fakulti
6. Pusat Jaminan Kualiti

Penilaian risiko dijalankan berdasarkan kategori aset iaitu Hardware, Software, People, Data & Information, Services-Supporting, dan Service-Accessibility. Semakan pada Julai 2025 mendapati sebanyak 802 aset telah dinilai, melibatkan 1,345 ancaman/risiko. Hasil penilaian menunjukkan terdapat 40 risiko pada tahap Sederhana dan 1,345 risiko pada tahap Rendah, manakala tiada risiko pada tahap Tinggi direkodkan. Secara keseluruhannya, pelaksanaan proses penilaian risiko serta pemantauan terhadap pelan rawatan risiko adalah selaras dengan keperluan standard.

6.4 Kawalan keselamatan maklumat secara keseluruhan

Pelaksanaan keseluruhan kawalan keselamatan adalah teratur dan dapat dirumuskan seperti berikut:
- Kawalan Keselamatan: Sebanyak 93 kawalan keselamatan yang dinyatakan dalam Statement of Applicability (SOA) didapati telah dilaksanakan dengan baik.
- Pengurusan Insiden Keselamatan Maklumat: Sejak audit terdahulu, terdapat satu (1) insiden yang dilaporkan dan organisasi telah mengambil tindakan pengurusan insiden melalui mekanisme yang telah ditetapkan.
- Penilaian Risiko: Penilaian risiko dijalankan dua kali setahun dan turut dilaporkan semasa Mesyuarat Kajian Semula Pengurusan. Semua risiko yang dikenal pasti dipantau secara berterusan dengan tindakan sewajarnya diambil apabila diperlukan.
- Pengukuran Keberkesanan (Objektif Keselamatan Maklumat): Sebanyak enam (6) objektif ISMS telah dilaksanakan dan dipantau. Prestasi telah disemak berdasarkan pengukuran keberkesanan yang ditetapkan dan dibentangkan kepada pihak pengurusan.
Secara keseluruhannya, berdasarkan sampel yang disemak semasa audit, kawalan keselamatan didapati telah dilaksanakan selaras dengan keperluan standard. Walau bagaimanapun, pelaksanaan kawalan keselamatan boleh terus dipertingkatkan sebagaimana yang dinyatakan dalam Laporan Ketakakuran (NCR) dan Peluang Penambahbaikan (OFI) yang direkodkan.

6.5 Penambahbaikan berterusan

Inisiatif bagi memastikan penambahbaikan berterusan telah didemonstrasikan melalui:
- Pengemaskinian dokumentasi ISMS agar selaras dengan pelaksanaan semasa.
- Tindakan susulan terhadap penemuan daripada audit dalaman.
- Pembentangan status pelaksanaan ISMS melalui slaid dan minit Mesyuarat Kajian Semula Pengurusan (MKSP).
- Pemantauan berterusan terhadap pencapaian objektif keselamatan maklumat (Objektif ISMS).
- Pelaksanaan aktiviti kesedaran berkaitan ISMS.
Selain itu, organisasi turut merancang untuk memperluaskan skop ISMS iaitu skop Pra Universiti, Sumber Manusia, Kewangan dan Penyelidikan bersama peneraju proses berkaitan serta meneliti ketersediaan sistem sokongan yang digunapakai oleh pihak berkepentingan di UPM.

6.6 Perbandingan berguna dengan keputusan audit yang lepas

Audit terdahulu telah diselesaikan tanpa sebarang Laporan Ketakakuran (NCR) dan dengan enam (6) Peluang Penambahbaikan (OFI), yang kesemuanya telah disahkan dan ditutup. Bagi audit penaiktarafan semasa kali ini, sebanyak satu (1) NCR dan enam (6) OFI telah dikenal pasti dan direkodkan. Peningkatan dalam penemuan ini menunjukkan masih terdapat ruang untuk penambahbaikan bagi memperkukuh lagi keberkesanan pelaksanaan ISMS versi baharu ini.

7 **LAPORAN KETAKAKURAN (NCR)**

Jumlah Ketakakuran Kecil (minor NCR) : 1	Senarai : 2501
Jumlah Ketakakuran Besar (major NCR) : 0	Senarai : -

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

Tiada isu yang tidak dapat diselesaikan.

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

Tiada isu penting yang memberi kesan kepada program audit.

10 **KESIMPULAN KEPADA KEPATUHAN DAN KEBERKESANAN SISTEM**

Audit pada tahun ini dijalankan sebagai audit penaiktarafan, dengan tumpuan kepada pelaksanaan keperluan baharu di bawah ISO/IEC 27001:2022. Hasil audit mengesahkan bahawa ISMS organisasi mematuhi keperluan standard, dan kawalan baharu telah dilaksanakan dengan baik.

Dokumentasi ISMS telah dikemas kini selaras dengan pindaan standard. Aktiviti pengurusan risiko turut disemak dan didapati mempunyai mekanisme pemantauan yang mencukupi untuk mengawal tahap risiko. Semakan sampel terhadap beberapa kawalan menunjukkan ia sesuai dan berkesan. Bagi pengurusan insiden, terdapat satu (1) insiden yang dilaporkan, dan organisasi didapati telah menguruskan insiden tersebut dengan menggunakan mekanisme serta prosedur pengendalian insiden yang telah ditetapkan.

Dari aspek pematuhan, ISMS menunjukkan kepatuhan berterusan terhadap ISO/IEC 27001:2022. Dari aspek keberkesanan pula, sistem berfungsi dan mampu mencapai tujuan yang ditetapkan. Walau bagaimanapun, audit turut mengenal pasti satu (1) Laporan Ketakakuran dan enam (6) Peluang Penambahbaikan (OFI) yang memerlukan perhatian serta tindakan bagi meningkatkan lagi tahap kematangan dan keupayaan ISMS.

Selain itu, komitmen dan penglibatan kakitangan dilihat sebagai faktor penting dalam kejayaan pelaksanaan ISMS. Usaha ini wajar diteruskan bagi memastikan penambahbaikan berterusan serta kelestarian sistem dalam jangka panjang.

11 **KESESUAIAN SKOP PENSIJILAN YANG DICADANGKAN**

Ya

12 **ADAKAH KESEMUA OBJEKTIF AUDIT TELAH DIPENUHI?**

Ya

13 **PENGESYORAN**

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

Jenis pindaan (sekiranya berkaitan)

Naiktaraf ke ISO/IEC 27001:2022 dan perubahan versi SOA.

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.

d) Pengauditan adalah berdasarkan proses pensampelan maklumat yang sedia ada

SUSULAN TERHADAP KETAKAKURAN YANG DIKELUARKAN

Tidak berkenaan

Ketua Pasukan Audit : NUR FATIN E'ZZATI BINTI MASRUHAIZAN

LAPORAN AUDIT PEMANTAUAN

No. Fail: 20190602821

ISO/IEC 27001:2022 (Including AMD 1:2024)		**KEPERLUAN YANG DIAUDIT**	**FUNGSI/ PROSES/ LOKASI PROJEK**								**NCR**	
Nyatakan proses yang diaudit			**P1**	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**Besar**	**Kecil**
4 Context of the organization												
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	/	/	/	/	/	/	/	/	/		
6.1.1	General	/	/	/	/	/	/	/	/	/		
6.1.2	Information security risk assessment	/	/	/	/	/	/	/	/	/		
6.1.3	Information security risk treatment	/	/	/	/	/	/	/	/	/		
6.2	Information security objectives and planning to achieve them	/	/	/	/	/	/	/	/	/		
6.3	Planning of changes	/	/	/	/	/	/	/	/	/		
7 Support												
7.1	Resources	/	/	/	/	/	/	/	/	/		
7.2	Competence	/	/	/	/	/	/	/	/	/		
7.3	Awareness	/	/	/	/	/	/	/	/	/		
7.4	Communication	/	/	/	/	/	/	/	/	/		
7.5	Documented information	/	/	/	/	/	/	/	/	/		

7.5.1	General	/	/	/	/	/	/	/	/	/		
7.5.2	Creating and updating	/	/	/	/	/	/	/	/	/		
7.5.3	Control of documented information	/	/	/	/	/	/	/	/	/		
8 Operation												
8.1	Operational planning and control	/	/	/	/	/	/	/	/	1		1
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	/	/	/	/	/	/	/	/	/		
9.2.1	General	/	/	/	/	/	/	/	/	/		
9.2.2	Internal audit programme	/	/	/	/	/	/	/	/	/		
9.3	Management review	/	/	/	/	/	/	/	/	/		
9.3.1	General	/	/	/	/	/	/	/	/	/		
9.3.2	Management review inputs	/	/	/	/	/	/	/	/	/		
9.3.3	Management review results	/	/	/	/	/	/	/	/	/		
10 Improvement												
10.1	Continual improvement	/	/	/	/	/	/	/	/	/		
10.2	Nonconformity and corrective action	/	/	/	/	/	/	/	/	/		
11 Other Certification Requirements												
11.1	Use of marks/ certificate	/	/	/	/	/	/	/	/	/		
	Jumlah NCR		-	-	-	-	-	-	-	1		1

Nota:

1) Tandakan (/) di kotak yang berkenaan untuk keperluan standard yang telah diaudit dan (-) untuk keperluan standard yang tidak diaudit.
2) Sekiranya keperluan standard telah diaudit dan ada ketakakuran terlibat, gantikankan tanda (/) dengan jumlah ketakakuran.
3) Sekiranya keperluan standard tidak berkenaan, tandakan "TB" di kotak yang berkenaan.

FUNGSI/ PROSES/ LOKASI PROJEK

- P1 - Pengurusan - Pusat Jaminan Kualiti (CQA)
- P2 - Pusat Pembangunan Maklumat dan Komunikasi (iDEC)
- P3 - Pendaftaran Pelajar Baharu Prasiswazah
- P4 - Penilaian Pengajaran di Fakulti
- P5 - Pendaftaran Pelajar Baharu Siswazah
- P6 - Pejabat Pengurusan Keselamatan dan Kesihatan Pekerja
- P7 - Pejabat Pendaftar
- P8 - UPM Sarawak

LAMPIRAN 1 : VERIFIKASI KEATAS LAPORAN KETAKAKURAN YANG DIKELUARKAN PADA AUDIT TERDAHULU:

No. Fail: 20190602821

No.	No. Rujukan Laporan Ketakakuran	Bukti yang dilihat bagi perlaksanaan tindakan pembetulan	Keberkesanan tindakan pembetulan	Komen
Tiada Laporan Ketakakuran yang dibangkitkan sebelum ini				

LAMPIRAN 2

SENARAI LOKASI TAMBAHAN				
No. Fail: 20190602821				
No.	**Nama & alamat lokasi**	**Skop Sijil (sekiranya berbeza daripada lokasi utama)**	**Bilangan kakitangan yang efektif**	**Diaudit**
1	**UNIVERSITI PUTRA MALAYSIA UNIVERSITI PUTRA MALAYSIA SARAWAK, JALAN NYABAU, 97008 BINTULU, SARAWAK, MALAYSIA**	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. 3. SISTEM PENGURUSAN KESELAMATAN MAKLUMAT BAGI PROSES PENDAFTARAN PELAJAR BAHARU SEPENUH MASA SISWAZAH MERANGKUMI AKTIVITI PENERIMAAN TAWARAN SEHINGGA PENGESAHAN PENDAFTARAN. INI ADALAH MENEPATI PENYATAAN PEMAKAIAN: TARIKH KEMASKINI 22/09/2025	15	/

Nota :

Senaraikan semua lokasi mengikut semakan kontrak.

LAMPIRAN 3

SENARAI LOKASI FUNGSI SOKONGAN					
No. Fail. : **20190602821**					
No.	**Alamat Lokasi**	**Tarikh Audit**	**Aktiviti**	**Bilangan Kakitangan**	**Diaudit/ Tidak Diaudit**
1	UNIVERSITI PUTRA MALAYSIA, BETA DATA CENTRE, 43400 SERDANG, SELANGOR.	24 September 2025	PUSAT DATA	-	Diaudit
2	UNIVERSITI PUTRA MALAYSIA, EPSILON DATA RECOVERY CENTRE, 43400 SERDANG, SELANGOR	24 September 2025	PUSAT PEMULIHAN BENCANA (DRC)	-	Diaudit
3	UNIVERSITI PUTRA MALAYSIA, PERPUSTAKAAN SULTAN ABDUL SAMAD, 43400 SERDANG, SELANGOR	-	PUSAT SIMPANAN SALINAN MEDIA	-	Tidak diaudit

SIRIM QAS INTERNATIONAL SDN. BHD.

NONCONFORMITY REPORT (NCR)

Client:

UNIVERSITI PUTRA MALAYSIA (UPM)

Status: Open

File No. : 20190602821	Audit Type: Surveillance Audit 1	NCR No: 2501

Standard Name: ISO/IEC 27001:2022
Last audit date:
Classification: Minor

Section 1 - Details of nonconformity
Requirement:

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by:
- establishing criteria for the processes;
- implementing control of the processes in accordance with the criteria.
Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned. The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. The organization shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.

A.8.24 Use of Cryptography
Rules of the effective use of cryptography, including cryptographic key management, shall be defined and implemented.

Finding
Semasa audit, diperhatikan bahawa Laporan Penilaian Pengajaran (DOKUMEN SULIT) yang dihantar kepada pensyarah yang terlibat melalui email tidak dilindungi dengan kaedah 'encryption'.

Objective evidence
1) email Laporan Penilaian Pengajaran (SULIT) kepada pensyarah
2) Garis Panduan Pengendalian Maklumat (iDEC/ISMS/GP01)
3) GARISPANDUAN KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (GPKTMK) VERSI 6.0

Auditor
NUR FATIN E'ZZATI BINTI MASRUHAIZAN
Client Representative
PUAN ZENAIDA MD ZENON

Section 2 - Result of investigation and determination of root cause

Client Representative
PUAN ZENAIDA MD ZENON

Section 3 - Correction (if applicable) and corrective action plan including completion date

Client Representative
PUAN ZENAIDA MD ZENON
Accepted by

Section 4 - Verification of corrective action(s) (to be filled up by Auditor)

Verify by:
NCR close out:

File No: 20190602821

OPPORTUNITIES FOR IMPROVEMENT			
Clause	**Details**	**Comments on action taken**	**STATUS**
4	**Context of the organization** 4.1 Understanding the organization and its context 4.2 Understanding the needs and expectations of interested parties Organisasi boleh mempertimbangkan untuk menentukan sama ada perubahan iklim merupakan isu yang relevan dalam konteks organisasi serta keperluan pihak berkepentingan yang berkaitan. Sekiranya relevan, aspek perubahan iklim boleh dimasukkan ke dalam proses penilaian risiko.		**Status** Open
Auditor: NUR FATIN E'ZZATI BINTI MASRUHAIZAN			
8.1	**Operational planning and control** A.8.11 Data Masking Kad staf secara fizikal disediakan kepada warga kerja. Walaubagaimanpun, organisasi bolehlah mempertimbangkan penggunaan kaedah data masking bagi nombor kad pengenalan (IC) yang tertera pada kad tersebut untuk meningkatkan perlindungan data peribadi. (Pejabat Pendaftar)		**Status** Open
Auditor: NUR FATIN E'ZZATI BINTI MASRUHAIZAN			
8.1	**Operational planning and control** A.5.20 Addressing information security within supplier agreements Penyelenggaraan firewall dilaksanakan secara berkala oleh vendor dengan kawalan capaian diuruskan oleh pegawai IDEC yang berkaitan. Organisasi boleh mempertimbangkan penambahbaikan dengan memastikan keperluan keselamatan maklumat turut diperjelaskan dan disokong melalui perjanjian (NDA) bersama pembekal. (UPM Sarawak)		**Status** Open
Auditor: NUR FATIN E'ZZATI BINTI MASRUHAIZAN			
8.1	**Operational planning and control** A.8.32 Change Management Organisasi telah melaksanakan kerja naik taraf rangkaian di UPM (Serdang dan Sarawak) seperti pemasangan access point dan switches melalui penglibatan vendor, dengan pemantauannya dijalankan oleh pegawai IDEC di Serdang. Sebagai peluang penambahbaikan, organisasi bolehlah memperkukuhkan pelaksanaan dengan memastikan perubahan yang dibuat di UPM Sarawak turut direkodkan secara konsisten melalui proses kawalan perubahan. (UPM Sarawak)		**Status** Open
Auditor: NUR FATIN E'ZZATI BINTI MASRUHAIZAN			

8.1	**Operational planning and control** A.7.14 Equipment Maintenance Utiliti sokongan seperti UPS dan genset disediakan di Bilik Server. Organisasi boleh mempertimbangkan untuk melaksanakan penyelenggaraan dan pengujian secara berkala bagi membantu memastikan kemudahan ini sentiasa berfungsi dengan baik. (UPM Sarawak)		**Status** Open
Auditor: NUR FATIN E'ZZATI BINTI MASRUHAIZAN			
8.1	**Operational planning and control** A.7.7 Clear Desk Clear Screen Organisasi boleh mempertimbangkan penambahbaikan dalam amalan clear desk dengan memastikan dokumen hardcopy seperti Senarai Semak Pendaftaran Pelajar yang telah disahkan oleh PKU disimpan dengan lebih teratur selepas digunakan, bagi mengurangkan potensi pendedahan maklumat. (Sekolah Pengajian Siswazah)		**Status** Open
Auditor: NUR FATIN E'ZZATI BINTI MASRUHAIZAN			