**PELAKSANAAN TINDAKAN PELUANG PENAMBAHBAIKAN (OFI)**

**PENEMUAN AUDIT PENSIJILAN SEMULA,**

**SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS) ISO/IEC 27001:2013**

**(1 – 3 OKTOBER 2018)**

**Dikemaskini 26 September 2019**

| **No. OFI** | **Klausa / Annex** | **Pernyataan OFI** | **PTJ diaudit** | **Peneraju Proses yang Terlibat** | **Maklum balas Tindakan** | **Tarikh tindakan** | **Bukti Sokongan** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OFI-1 | 6.1.3 d) | **Mengemukakan penyata pemakaian**  Didapati, Kawalan ~~A.6.5.1~~ (A.6.1.5) Keselamatan Maklumat Dalam Pengurusan Projek tidak terpakai dalam pelaksaan ISMS. Pengecualian kawalan ini sewajarnya disemak semula memandangkan UPM ada melaksanakan beberapa projek seperti UPM ID dan PutraCloud | Pusat Jaminan Kualiti | 1. Pusat Jaminan Kualiti | **Maklum balas CQA**  Membuat pengemaskinian pada Dokumen Penyata Pemakaian (SoA) mengambilkira keperluan kawalan bagi perkara A.6.1.5 (Keselamatan maklumat dalam pengurusan projek) selaras dengan pelaksanaan projek pembangunan ICT yang terlibat dengan skop pensijilan | 22 Februari 2019 | SoA yang telah berkuatkuasa |
| OFI-2 | 7.3  A.9.3.1 | **Kesedaran**  **Penggunaan maklumat pengesahan rahsia**  Kesedaran terhadap pematuhan pengurusan kata laluan yang interaktif dan berkualiti bagi memenuhi keperluan Garis Panduan Keselamatan Teknologi Maklumat dan Komunikasi (GPKTMK) perlu ditambah baik bagi:   1. Pengguna eSMP di kolej Kediaman 2. Pengguna SPICT, di IDEC 3. Pengguna SAS di Pejabat Bursar | 1. Kolej Kediaman 2. iDEC 3. Pejabat Bursar | 1. Pejabat Pendaftar 2. iDEC | **Maklum balas iDEC**  Untuk sistem yang berasaskan UPMiD telah melaksanakan *enforcement strong password* kepada pengguna. | 3 oktober 2018 | BOA perlu buat proses perolehan semula kerana:   1. tiada peruntukan kewangan 2. tawaran harga pembekal melebihi bajet 3. telah maklumkan kepada Bahagian Akademik untuk tindakan peruntukan semula   SSG telah papar infografik GPKTMK di laman web iDEC  SJK telah hebah GPKTM pada warga UPM melalui email INFO\_ICT pada 3 Dis 2018  KB BIT telah hebah kesedaran ancaman kecurian identiti melalui email INFO\_ICT pada 21 Dis 2018. |
| Untuk sistem yang tidak berasaskan UPMiD kawalan UPMiD akan dilaksanakan.  Daftar baru Sebutharga perolehan naiktaraf sistem ESMP. | 20 November 2018 |
| Kesedaran keselamatan pengurusan kata laluan kepada pengguna akan diberi hebahan melalui email INFO ICT atau Buletin UPM.  Taklimat GPKTMK kepada pengguna | 20 November 2018 |
| OFI-3 | 10.1 | **Ketakakuran dan tindakan pembetulan**  Hasil semakan dan tindakan susulan bagi menutup Laporan Penambahbaikkan yang dikeluarkan oleh pasukan audit dalam perlulah sentiasa direkodkan di dalam Portal Jaminan Kualiti. | Pusat Jaminan Kualiti | Pusat Jaminan Kualiti | **Maklum balas CQA**   1. Memberi kesedaran / kefahaman kepada TWP dan TPAD berkaitan dengan penggunaan sistem audit (Portal CQA). 2. Laporan Analisis Penutupan penemuan audit dalaman tahun semasa dan tahun dilaporkan dalam mesyuarat JK Kualiti | 22 Februari 2019 | 1. Bukti kesedaran/ kefahaman berkaitan penggunaan sistem audit (PortalCQA) 2. Petikan minit Mesyuarat JK Kualiti |
| OFI-4 | **8.1**  **A.12.1.1** | **Kawalan dan Perancangan Operasi**  **Prosedur operasi yang didokumenkan**  Kawalan perubahan semasa pembangunan sistem/aplikasi dan selepas tamat tempoh ‘warranty’ dilaksanakan mengikut prosedur yang ditetapkan. Namun, kaedah kawalan perubahan bagi sistem/aplikasi yang berada dalam tempoh ‘warranty’ perlu diperjelaskan lagi agar sebarang perubahan yang dibuat dapat dilaksanakan dengan lebih baik. | iDEC | iDEC | **Maklum balas iDEC**  Pindaan Prosedur Pembangunan ICT akan diadakan Bengkel Semakan Dokumen 21 November 2018 | 22 Februari 2019 | Rujuk portal reg.upm.edu.my/eISO  Kod Rujukan Dokumen:  UPM/OPR/iDEC/P001 |
| OFI-5 | **A.17.1.1** | **Perancangan kesinambungan keselamatan maklumat**  Simulasi bagi pelan pemulihan bencana (DRP) ICT versi 4.0 telah berjaya dijalankan pada 27 Julai 2018. Semakan terhadap dokumen DRP ICT yang baharu sedang dibuat berdasarkan laporan keputusan hasil daripada simulasi tersebut. Pasukan DRP ICT perlu mengambil kira aplikasi Penilaian Pengajaran sebagai salah satu komponen di dalam aktiviti ini memandangkan proses penilaian pengajaran ini baru dimasukkan di dalam skop pensijilan.  Walau bagaimanapun, kelemahan yang berkaitan dengan proses kesinambungan perkhidmatan serta ancaman bagi aplikasi ini telah direkodkan di dalam MyRAM. | iDEC | 1. Pejabat Strategi Korporat dan Komunikasi (CoSComm) 2. iDEC | **Maklum balas Idec**  Pelan DRP untuk Penilaian Pengajaran(CADe) telah dirancang dan akan dilaksanakan pada Simulasi DR pada 4 Oktober 2019 dengan menggunakan Infrastruktur sementara DR CADe | 4 oktober 2019 | Email hebahan notifikasi Hebahan Simulasi DRP ICT 2019 |
| OFI-6 | **A.11.2.8** | **Peralatan pengguna tanpa jagaan**  Organisasi boleh menambahbaik kawalan untuk komputer yang ditinggalkan tanpa jagaan supaya sentiasa mematuhi kawalan yang ditetapkan dalam GPKTMK.(contoh: komputer di Pejabat Bursar). | Pejabat Bursar | iDEC | **Maklum balas iDEC**  Kesedaran Kawalan Clear screen/screen saver telah dihebahkan melalui email [info\_ict@upm.edu.my](mailto:info_ict@upm.edu.my) pada 14 Mei 2019 | **14 Mei 2019** | Hebahan Kesedaran kawalan clear screen:  Email [info\_ict@upm.edu.my](mailto:info_ict@upm.edu.my) kesedaran kawalan clear screen |
| OFI-7 | **A.12.2.1** | **Kawalan daripada perisian hasad**  Komputer pengguna telah dipasang dengan antivirus sewajarnya. Namun demikian, pemantauan ke atas pengemaskinian antivirus tersebut perlu dilihat dan boleh ditambahbaik untuk memastikan antivirus terkini. (contoh: komputer di Fakulti Bahasa Moden dan Komunikasi, Fakulti Ekonomi dan Pengurusan, dan Fakulti Perhutanan) | 1. Fakulti Bahasa Moden dan Komunikasi 2. Fakulti Ekonomi dan Pengurusan 3. Fakulti Perhutanan | iDEC | **Maklum balas iDEC**   1. kemaskini antivirus telah tersenarai dalam senarai Semak penyelenggaraan PC. 2. Hebahan kewajipan pemasangan perisian antivirus bagi semua komputer aset upm. | 4 Okt 2019 | Rujuk portal reg.upm.edu.my/eISO.  Kod rujukan: OPR/iDEC/SS01/PENYELENGGARAAN KOMPUTER  Email [info\_ict@upm.edu.my](mailto:info_ict@upm.edu.my) Tindakan segera: kewajipan pemasangan perisian antivirus bagi semua komputer aset upm. |