**PELAKSANAAN TINDAKAN PELUANG PENAMBAHBAIKAN (OFI)**

**PENEMUAN AUDIT PENSIJILAN SEMAKAN 1,**

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

**(7 – 9 OKTOBER 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) | **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 firewall, perubahan IP dan pengemaskinian security patch. | iDEC | 1. Pusat Jaminan Kualiti (CQA) 2. Pusat Pembangunan Maklumat dan Komunikasi (iDEC) | **Maklum balas CQA**  Mengemaskini dokumen Penyata Pemakaian (Statement of Applicability (SoA)) mengambilkira penambahbaikan yang dicadangkan.  **Maklum balas iDEC**  Kemaskini SOA dengan menambah kawalan :   1. Prosedur Perkhidmatan ICT 2. Prosedur Pembangunan ICT   Menyediakan dokumen rasmi pengesahan kelulusan dari Ketua Bahagian sekiranya ingin melaksanakan sebarang permohonan perubahan terhadap perkhidmatan. | 29 Julai 2020 | SOA versi terkini |
| OFI-2 | 8.1 | **Perancangan dan kawalan operasi**  A.9.2.6 Penyingkiran atau pelarasan hak akses  Senarai hak akses pengguna terhadap VPN yang dikawal di firewall perlu dilihat semula organisasi agar risiko terhadap akses yang tidak sah dapat dikurangkan.  **Contoh:**  guest, ruzi\_ab. | 1. iDEC | 1. iDEC | **Maklum balas iDEC**  Kertas Cadangan pelan tindakan perlu diserahkan kepada pengurusan iDEC untuk kelulusan. | 30 Oktober 2019 | Rujuk Lampiran V : Pelan Tindakan Penambahbaikan (OFI) terhadap Penemuan Audit Semakan 1 ISMS ISO/IEC 27001:2013 |
| OFI-3 | 8.1 | **Perancangan dan kawalan operasi**  A.12.4.4 Penyegerakan jam  Waktu pada sistem door access 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 | iDEC | iDEC | **Maklum balas iDEC**  Kertas Cadangan pelan tindakan perlu diserahkan kepada pengurusan iDEC untuk kelulusan. |  | Rujuk Lampiran V : Pelan Tindakan Penambahbaikan (OFI) terhadap Penemuan Audit Semakan 1 ISMS ISO/IEC 27001:2013 |
| OFI-4 | **8.3** | **Penguraian risiko keselamatan maklumat**  Proses pentaksiran risiko telah dilaksanakan oleh organisasi dan terdapat beberapa risiko yang berada pada tahap Sederhana (Medium). Maka pihak yang bertanggungjawab mengambil keputusan untuk melaksanakan pelan penguraian risiko. Namun demikian, pelan penguraian risiko tersebut perlu ditambahbaik. lni kerana Pelan Penguraian Risiko yang dibangunkan adalah sama dengan tindakan sedia ada (Existing Safeguard).  **Contoh:** Penyelenggaraan berkala untuk UPS, genset dan precission cooling unit. | iDEC | iDEC | **Maklum balas iDEC**  Kertas Cadangan pelan tindakan perlu diserahkan kepada pengurusan iDEC untuk kelulusan. |  | Rujuk Lampiran V : Pelan Tindakan Penambahbaikan (OFI) terhadap Penemuan Audit Semakan 1 ISMS ISO/IEC 27001:2013 |