Health Informatics Centre
University of Dundee

IS 802159 IS 802159

Information Security Management System (ISMS) Audit

PURPOSE

The HIC Services External Audit is commissioned by the HIC Governance Committee and is carried out annually by an external auditing company. The audit includes a review of operating standards, documentation, Standard Operating Procedures, systems, facilities, and projects for compliance with conditions of approval (by Caldicott Guardian, Ethics Committee and other authorities) and requirements of UK data protection legislation. The audit is carried out at the Health Informatics Centre located in Ninewells Hospital.

HIC also receives a second annual external audit involving an external penetration test of HIC's Safe Haven environment and IT systems, to check for system security vulnerabilities.

This SOP describes procedures to follow-up and resolve actions raised in the audit reports and the routine internal audits carried out more widely across HIC processes to provide information on whether HIC Services' Information Security Management System (ISMS) is being effectively implemented, maintained, and followed.

SCOPE

This SOP covers the HIC's response to external HIC audits and wider routine internal audits. It is applicable to all HIC staff. This SOP is made available to all users and potential users of the HIC Service and will be externally visible on the public HIC website.

PROCEDURE

Policy

For overall Policy see Legal and Governance Policy.

External Audit Steps

1. HIC Services will receive 2 external audits annually, one an IT System Penetration test and the other a wider audit of HIC Processes and Procedures.
2. Once the external audits have taken place and the Auditor reports are received by HIC Services, they will be circulated to the Chair of the HIC Information Governance Committee and the HIC Services Executive Committee. They are subsequently discussed, along with HIC's response, at the HIC Information Governance Committee meeting.
3. All action points raised will then be taken from the audit reports and inputted to the HIC Services PM system which allows the progress of each point to be monitored until complete, with space for additional comments and updates. Each action will be assigned to the appropriate member of staff, with a completion deadline, who will then carry out the remedial work needed.

Internal Audit Steps

1. A quarterly internal audit plan of HIC's Information Security Management System (ISMS) will be prepared in advance, covering a 12-month period, to ensure that HIC's ISMS is conforming to the International Standard requirements and is being effectively implemented and maintained.

2. Individual audits are planned, including methods, responsibilities, and reporting; and a scope of audit agreed with the Team Leader as appropriate.
3. Audits are carried out throughout the year, following the audit plan, by staff independent of the work being audited, or by external auditors employed for the purpose.
4. Previously issued corrective/preventative action requests are reviewed at audits and entered, where appropriate, onto the audit plan.
5. The internal audit results, including target implementation dates for completion of corrective/preventative action, will be recorded centrally, and reported to the HIC Governance Manager who is then responsible for assigning responsibility and ensuring remedial action is taken. The results of audits are presented for discussion at the HIC Executive Committee meeting.

APPLICABLE REFERENCES

- Security Policy
- Standard Operating Procedures
- For Definitions see ISMS Glossary

DOCUMENT CONTROLS

Process Manager	**Point of Contact**		
Jenny Johnston	hicbusiness-support@dundee.ac.uk		
Version Number Major is defined by if it is a revision of content/procedure and approval is required. It's represented as: **3**.0, **4**.0, **5**.0. Minor is defined as not requiring approval and includes small changes to spelling, grammar and formatting. It's represented by 3.**1**,3.**2**, 3.**3**.	**Effective Date**	**Edited By**	**Edition Details**
1.0	01/09/13	Duncan Heather	This is a new SOP which expands on a subset of policies and supersedes Version 6 of the HIC Standard Operating Procedure, Management of HIC Datasets. Effective from 1st August 2011.
1.1	01/04/14	Duncan Heather	Add details about more rigorous checking of archive record in section 4 Internal Audit a. vii
2.0	01/01/15	Duncan Heather	General review and update

3.0	01/01/16	Duncan Heather	Change title from “Responding to HIC annual audit” to “Audit of HIC’s Information Security Management System (ISMS)”, broaden content to encompass ISO requirements and move minor detail to separate Work Instructions.
4.0	08/11/18	Duncan Heather	Update to reflect new GDPR
4.0	24/02/20	Tracey Stewart	Updated cover sheet with new approval process information
4.0	15/05/2020	Rachael Torano	Updated with new and approved Header Changes made to cover page to include Op’s review date as agreed at the HIC Information Governance Meeting Document Review and Revision History table header updated. As agreed by the HIC Governance Committee signatures have been removed from cover page and Document Review and Revision History table has been updated to include review dates and notes
4.0	30/06/20	Duncan Heather	Reviewed, no changes made
4.0	18/01/22	Duncan Heather	Reviewed, no changes made
4.1	23/11/23	Symone Sheane	Updated SOP to new template
4.2	19/02/23	Bruce Miller	Moved SOP from SharePoint to Confluence
Last Review Date	**Triggers** • Annual Review • Internal Audit (conducted by TASC annually) has identified opportunities for improvement (OFI) or nonconformities (NC) • External Audit has identified OFI or NC • Significant Event has highlighted OFI • Client Complaint has highlighted OFI • HIC All Staff (individuals of) have identified OFI		
23/11/2023	HIC All Staff (individuals of) have identified OFI		

Next Review Date	BST-1195: SOP Review- ISMS Audit - Test DONE

Approved by the HIC Ops Group Date	**Approved by the HIC Exec Date**
n/a	n/a