POLICY AND GUIDANCE
Do not Photocopy

Document Information Classification: Unrestricted

Title:	**ISMS Roles and Responsibilities**
Effective Date:	**01 Aug 2019**
Reference Number:	**ISMS-02-07**
Version Number:	**2.7**
Owner:	**ISMS Management Process Owner,**
Review Date:	**01 Aug 2021**

Table of Contents

1. Purpose

It is necessary to ensure that the responsibilities and authorities for roles relevant to information security are defined, allocated and communicated. The purpose of this document is to define the required roles for the Information Security Management System (ISMS) and the responsibilities of each role to information security.

2. Scope

This document defines the high level required roles for the ISMS and their responsibilities.

3. Responsibilities

Within the Information Security Management System there are a number of roles, each with their own responsibilities, which need to be allocated to specific individuals or groups within the organisation.

The list below details the specific information security responsibilities of each role within the ISMS structure. It does not include any other types of responsibility e.g. managerial, technical and should not be taken as a full job description:

I. Management Sponsor (incorporates SIRO)
- Provide leadership and commitment to the ISMS
- Ensure a successful ISMS implementation

II. Information Security Steering Group (ISSG)
- Establish the ISMS policy, objectives and plans
- Communicate the importance of meeting ISMS objectives and the need for continual improvement
- Maintain an awareness of business needs and major changes
- Ensure that Stakeholder requirements are determined and are met with the aim of improving customer satisfaction
- Ensuring that sufficient resources are provided to support the effective implementation of information governance (IG) and security in order to ensure compliance with the law, professional codes of conduct and the NHS information governance assurance framework.

III. Information Security Manager (ISM)
- Developing and implementing IG procedures and processes;
- Operation of the ISMS
- Maintenance and improvement of the ISMS
- Raising awareness and providing advice and guidelines about IG to all staff;
- Ensuring that any training that is made available is taken up;
- Coordinating the activities of any other staff given data protection, confidentiality, information quality, records management and Freedom of Information responsibilities;
- Ensuring that personal data is kept secure and that all data flows, internal and external are periodically checked against the Caldicott Principles;
    - Monitoring information handling in the organization to ensure compliance with law, guidance and internal procedures;

    - Where necessary, ensuring citizens are appropriately informed about the organisation's information handling activities.
- Escalation of security incidents to IG-SIRI (see SOP-07-05 for more details)

IV. Information Asset Owner (IAO)
- Responsible for the security, maintenance and availability of an asset.
- Understanding the type of information held on/in their asset, what is added and what is removed, how information is moved, and who has access and why.
- Address risks to information, and ensure that information is fully used within the law for the public good.
- Provide a written judgement of the security and use of their asset annually to support the audit process.
-

V. CHI Operational Lead (COL)
- Oversees Recruitment of Staff and Students within the Centre for Health Informatics (CHI)
- Oversees finance, personnel/HR, training, strategic planning, marketing and communications
- Approves building and alarm code access

VI. Head of Operations ISMS (HOI)
- Compliance of staff and users to the ISMS
- Managing resources within the ISMS
- Planning activities to meet ISO27001 certification objectives
- Provides a link between the day-to-day running of the ISMS by the ISM and the more strategic activities of the ISSG.

VII. Process Owner (PO)
- Compliance of staff with their process policies and procedures
- To coordinate the creation, dissemination, revising and reviewing of ISMS Documentation related to that process
- To keep the relevant items in the ISMS Risk Register up to date and to add new risk items as appropriate (ISMS-02-06)
- To act as 'Monitoring and Measurement Owner (see SOP-04-04 ISMS Measurement and Monitoring)

VIII. TRE Staff (TS)
- All staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they are aware of and comply with the requirements of the ISMS.
- Reporting information security incidents

In addition to the above, all ISMS documents define specific procedural responsibilities for the staff and/or teams that interact with the different ISMS processes.

4. Cross-referenced ISMS Documents

Number	Type	Title
ISMS-02-06	ISMS\Policy & Guidance\ISMS Management - policy & guidance	Information Security Risk Register
SOP-04-04	ISMS\SOP\ISMS Improvement - SOP	ISMS Measurement and Monitoring
ISMS-02-04	ISMS\Policy & Guidance\ISMS Management - policy & guidance	ISMS Role Assignments
SOP-02-01	ISMS\SOP\ISMS Management - SOP	ISMS Document Control

5. Appendices

None