POLICY AND GUIDANCE
Do not Photocopy

Document Information Classification: Unrestricted

Title:	**ISMS Manual**
Effective Date:	**07 Oct 2019**
Reference Number:	**ISMS-02-10**
Version Number:	**2.8**
Owner:	**ISMS Management Process Owner,**
Review Date:	**06 Jun 2020**

Table of Contents

1. Purpose

To implement an information security policy it is necessary to set out the organisation's approach to managing its information security objectives. In particular this approach should address the requirements created by the business strategy, regulations and legislation and the information security threat environment.

This document summarises the critical factors that influence this organisation's approach to information security and defines the objectives and principles that will guide all activities relating to information security.

2. Scope

The Information Management Security System that covers the development and operation of a Trusted Research Environment (TRE) and associated services from within the Centre of Health Informatics (CHI), The University of Manchester.

3. Background

3.1. Organisation

The Health eResearch Centre (HeRC) is a regional partnership between four universities, the NHS and a network of industry partners and is funded by grants from research councils, government departments and charities. Working together we form a powerhouse of health data science operating across the North of England and we are a founding member of the UK-wide Farr Institute for Health Informatics.

As part of HeRC, the Centre for Health Informatics (CHI) at the University of Manchester brings together a multi-disciplinary team of researchers, developers and clinicians to understand more about how under-used health data can be re-purposed to improve health.

3.2. Business Strategy

At CHI we routinely collect data to understand more about diseases; what causes them and how they develop. We are also looking at ways that patients can help to generate data that will help them and their health professionals understand more about how their symptoms affect them on a day-today basis.

Data is our business and all data collected, analysed and handled by our researchers must be done in accordance with all legal standards.

In order to remain amongst the leaders in the field of health data science and to support new and existing research projects CHI must provide a secure data hosting and management service. Using a combination of public health information and the technology this can support the delivery of multidisciplinary research projects that are at the forefront of the science of Health Informatics.

3.3. Data Hosting and Management Service

The Trustworthy Research Environment (TRE) is a facility hosted at the University of Manchester, managed and operated by staff at the Centre for Health Informatics. The facility is funded by grants from the Medical Research Council (MRC) and will be used by approved researchers to enable new science and accelerate existing science.

The TRE infrastructure is delivered to users through a range of services as follows:

- Data management service for personal confidential data (e.g. ONS)
- On-site secure data office
- Data management service for de-identified data (e.g. NHS Digital)
- "Walled-garden" with remote access
- Hosting for applications on HSCN (NHS) and University networks
- On demand virtual machines for data analysis
- 2-factor authentication (RSA) available for remote access
- Virtual private network (VPN)
- Configurable project groups and permissions for storage and virtual machines
- eLab data management platform

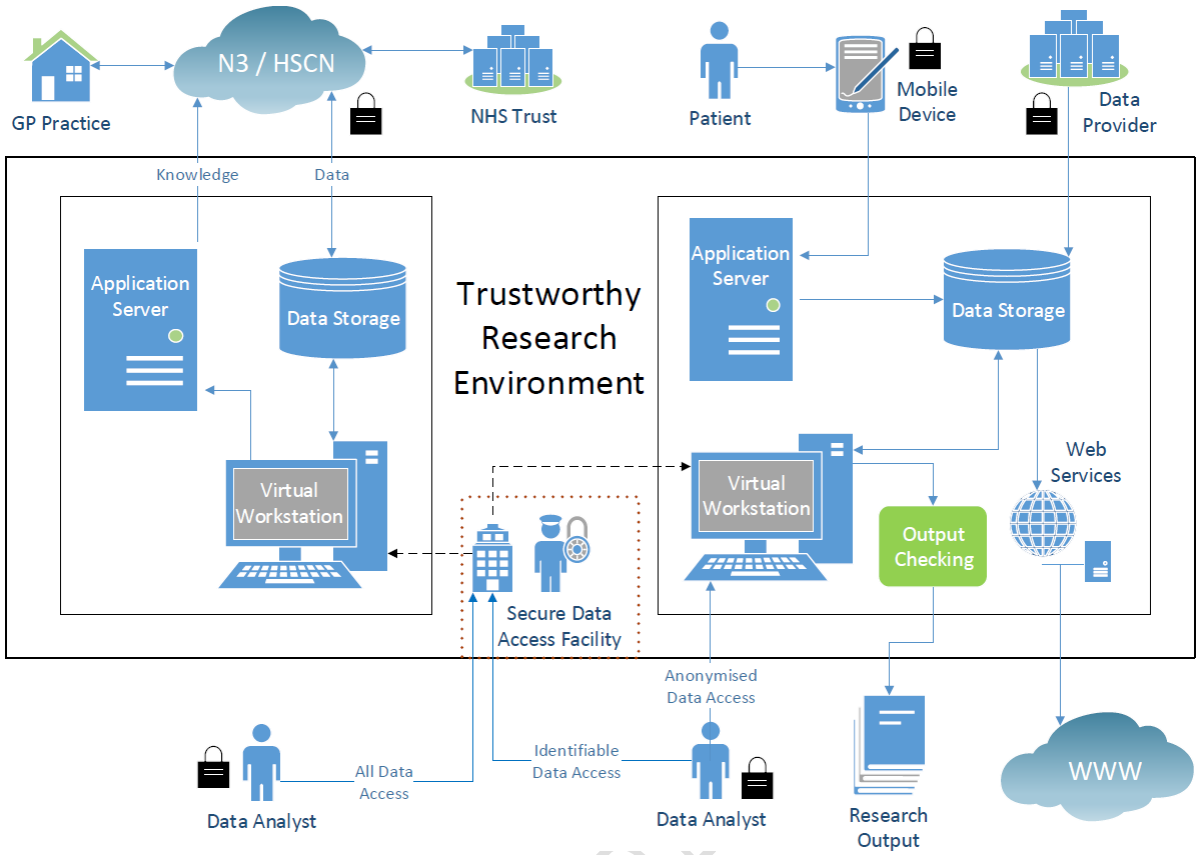
The TRE is comprised of a series of assets that can be classified into the following categories:

- **Information Assets – TRE Data**: Structured (databases), Semi-structured (image, audio, video files, machine/disk images, software code, bit streams) Unstructured (text, csv).
- **Information Assets - System information**: User accounts, Audit trails, System configuration.
- **Software Assets**: Operating systems, Software applications, Testing tools, Development tools and utilities.
- **TRE Infrastructure**: Servers, Storage devices, Network devices, Backup power.
- **Physical assets**: Building infrastructure, Security controls.
- **Services**: IT and Communications services, University Estates (e.g. mains electrical, cooling), University Security (door access control).

The TRE Service comprises three core activities:

- TRE Development (managing changes to the TRE infrastructure)
- TRE Operations (customer support, data management, TRE project and user management)
- TRE Systems Administration (software patching, maintenance, service provisioning)

The scope of the TRE is shown diagrammatically in the diagram below.



3.4. Security Threat Environment

When it comes to information security and overall threats to the TRE, the landscape is always changing. There are many types of security threat that can be considered with some of the key threats shown in the table below:

Threats	Motives/Goals	Methods	Security Policies
• Employees • Malicious • Ignorant • Non-employees • Outside attackers • Natural disasters • Floods • Earthquakes • Hurricanes • Riots and wars	• Deny services • Steal information • Alter information • Damage information • Delete information • Make a joke • Show off	• Social engineering • Viruses, Trojan horses, worms • Packet replay • Packet modification • IP spoofing • Mail bombing • Various hacking tools • Password cracking	• Vulnerabilities • Assets • Information and data • Productivity • Hardware • Personnel

It is expected that the greatest threat to the TRE will come from humans, through actions that are either malicious or ignorant, looking to access or steal the information. Whilst it is important to keep up to date with all potential security threats this will be done in parallel with applying protective measures which can be classified as follows:

- **Prevention** -Establish controls that prevent information from being damaged, altered, or stolen.
- **Detection** - Establish measures that can detect when information has been damaged, altered, or stolen, how it has been damaged, altered, or stolen, and who has caused the damage.
- **Reaction** –Establish processes that allow recovery of information, even if information is lost or damaged.

3.5. Regulations and Legislation

The applicable laws, regulations and contractual requirements that will be applied to the operation of the TRE are listed and maintained in ISMS-02-03 Index of Relevant Policy.

4. Principles and Key Objectives

4.1. ISMS Principles

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management. It is therefore of paramount importance that information is efficiently managed, and that appropriate policies, procedures, management accountability and structures provide a robust framework for information security management.

CHI management are committed to the implementation, monitoring, review and continual improvement of the systems managing quality and information security and will ensure the following principles are observed:

- The preservation of confidentiality, integrity and availability of information, as well as ensuring the authenticity and reliability of information that is of value to the organisation and its users.
- Meet our objectives and those of our funders, e.g. MRC
- Deliver services that meet the needs of our users, e.g. Approved Researchers
- Comply with applicable laws, regulations and contractual requirements
- Information will be protected against unauthorised access;
- Information will be supported by the highest quality data;
- Continual improvement of the system
- All services are managed through documented processes delivered through an Information Management Security System (ISMS)

All breaches of confidentiality and information security, actual or suspected, will be reported and investigated.

4.2. Key Objectives

Key objectives will be established for the ISMS to guide all activities relating to information security.

The ISMS shall meet the following key objectives:

1. Ensure staff are trained to comply with applicable laws and regulations
2. Take reasonable measures to prevent unauthorised access to the TRE
3. Maintain confidentiality of information

4. Integrity of imported information will be maintained
5. Deliver services that meet the needs of our users
6. Manage all security events to minimise impact on the TRE

5. Approach

Specific procedures and policies will be defined as part of the ISMS separate from this document. These will address key aspects including:

- the assignment of general and specific responsibilities for information security management to defined roles;
- processes for handling deviations and exceptions

At a lower level, the information security policy will be supported by topic-specific policies, which will further mandate the implementation of information security controls and will be structured to address the needs of certain target groups within the organization or to cover specific topics.

5.1. Management of Objectives

Detailed information security measures based on the key objectives will be produced (ISMS-02-12) as part of the ISMS Improvement process and confirmed and reported by the ISMS Management Team.

5.2. Controls Statement of Applicability

The ISO27001 controls will be applied to support the delivery of the key objectives and to minimise the impact of the risk threats. Risk assessment will be performed periodically to address any changes in the information security requirements and in the risk situation. The output of these assessments will be used to determine whether the implemented controls still provide the necessary level of protection and relevant controls will be implemented to manage unacceptable risk. Where there are changes in risks or the organisation's objectives it may also be appropriate for controls to be removed.

5.3. ISMS Processes

The ISMS will be managed using a set of process groups with supporting documentation to enable delivery and management of the objectives. These shall be further divided into the key ISMS processes to support the management and delivery of the ISMS.

ISMS No	Process Group	ISMS Process	Process Description
01	Personnel and Training	Staff Induction, Update and Exit	Management of the full lifecycle of personnel that are in scope of the ISMS. Is additional to the University's own HR processes and ensures that each person joining or leaving the Centre for Health Informatics has all relevant details recorded.
		Staff Training and Competency	Ensuring the person assigned to each role is suitably qualified and knowledgeable. Includes definition of competencies for core ISMS roles and management of training courses within the ISMS.
02	ISMS Management	ISMS Event and Incident Management	For the reporting and management of any security event or opportunity for ISMS improvement. Also includes for management of security incidents.
		ISMS Document Management	Lifecycle management of all ISMS documents including creation, review, approval, distribution, acknowledgement of understanding and version control.
		ISMS Management	A risk-based approach to managing the compliance and performance of the ISMS processes to ensure the organisation meets its information security objectives. Includes the core documents that describe the main purpose and scope of the ISMS, and how the implemented security controls map to the requirements of the ISO27001 standard. Reviews the scope of the ISMS and significant risks and security incidents.
		ISMS Risk Management	Understanding the organisation's information assets and how the primary asset (data) is dependent on them. Includes regular review to ensure risk scores are accurate and the necessary treatment is taking place.
03	TRE Operations	TRE Operations	The running of the Trustworthy Research Environment service, and its team of staff
		TRE Project and User Account Management	Keeping a thorough and highly accurate record of the research projects that are hosted in the TRE, and the members of those projects who are allocated TRE user accounts. This process closely aligns with TRE Access Control operations.

		TRE User Competency and End-Point Security	Making sure a TRE user meets the required levels of competence and training, and that their workstation has been correctly setup to connect to the TRE.
04	ISMS Improvement	ISMS Improvement	Managing all activities that contribute towards improvement of each ISMS Process including audit (internal and external) and management review (ISMS Board and Management Review meetings).
05	Asset and Supplier Management	TRE Asset and Supplier Management	Maintaining accurate asset registers for all the information assets within scope of the ISMS, including IT infrastructure, people, documentation, buildings, suppliers and services and data. Managing the regular review and audit of supplier service delivery.
		TRE Data Management	Liaising with the data controller and project lead in operational planning and coordination of data import and export. Data curation and maintaining the TRE Data asset register.
06	Information and Physical Security	TRE Physical Security	Ensuring the building that houses the TRE server room is adequately secure. In addition to maintaining door and safe locks, it requires collaboration with University Estates Security and enforcing the procedural controls that affect individual who enters the building.
07	ISMS Governance	TRE Information Governance	Providing support during the completion of data sharing agreements, contracts, privacy impact assessments and data flow definitions. Ensuring the data coming into the TRE, and the people who are granted access to that data correspond with the requirements set by the data controller.
08	Communications	ISMS Communication	Overseeing the communication with ISMS stakeholders, making sure all in-scope people and suppliers are kept up to date and notified of any required actions.
09	TRE System Admin	TRE Infrastructure and Security Management	Ensuring the core TRE infrastructure meets the ISMS requirements to maintain the confidentiality, integrity and availability of the TRE data. Closely aligned with TRE Operations in conducting Change Management and Access Control.

5.4. Use of Q-Pulse

The ISMS will be managed in Q-Pulse a software application focused on quality, compliance and improvement that is used to manage the ISMS in line with regulatory and stakeholder requirements.

Q-Pulse consists of a number of modules. The most commonly used modules are:

- Documents: Used for reading, approving, reviewing and securely storing all documentation.
- Actions: Used for raising and managing all non-conformances and improvement ideas.
- Audit: Used to manage all stages of any audit occurring in the organisation.

Other modules include Assets, Suppliers, TRE Projects, People and TRE User Accounts, Training and Qualifications and Analysis.

Q-Pulse will be used to document all actions, audits, documents, assets and people under the scope of the ISMS.

6. Cross-references

Number	Type	Title
ISMS-02-12	ISMS\Policy & Guidance\ISMS Management - policy & guidance	Information Security Measures
ISMS-02-03	ISMS\Policy & Guidance\ISMS Management - policy & guidance	Index of relevant policy
ISMS-02-12	ISMS\Policy & Guidance\ISMS Management - policy & guidance	Information Security Measures

7. Appendices

None