POLICY AND GUIDANCE
Do not Photocopy

Document Information Classification: Unrestricted

Title:	**Information Security Measures**
Effective Date:	**09 May 2019**
Reference Number:	**ISMS-02-12**
Version Number:	**2.8**
Owner:	**ISMS Management Process Owner,**
Review Date:	**17 Apr 2021**

Table of Contents

1. Purpose

Information security is achieved by implementing a suitable set of controls that need to be reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met.

This document defines the quality and information security measures, established from the key ISMS objectives, to assess the effectiveness of the existing controls and support the ISMS management review process.

2. Scope

This policy covers the production and communication of S.M.A.R.T Quality and Information Security Measures based upon the ISMS key objectives identified in the ISMS Manual – ISMS-02-10.

3. Responsibilities

The Information Security Steering Group (ISSG) is responsible for:

- Establishing the measures
- Reviewing the suitability of the measures in assessing the effectiveness of existing controls

The Information Security Manager (ISM) is responsible for:

- Distribution and communication of the measures
- Management and collection of data for presentation to the ISSG

4. Policy

4.1. SMART Classification

Each measure, whether for Quality (Q) or Information Security (IS), will follow the S.M.A.R.T classification system:

- S – Specific
- M – Measurable
- A – Assignable
- R – Realistic
- T – Time-Based

4.2. Reporting and Review

Measures will be calculated on a bi-monthly basis and reported to the ISSG at the management review meetings.

To ensure the security and business objectives can continue to be met the management review meetings will determine any necessary updates to the measures.

An annual full review of the measures by the ISSG will also be completed.

No	Key Objective	Measure	Assigned To
1	Ensure staff are adequately trained to comply with applicable laws and regulations	All new staff complete their CHI induction within 1 month of start date.	Staff Induction and Exit Process Owner
		>90% of staff read and acknowledge ISMS documents within 1 month of notification.	ISM
		All staff have completed Data protection training within 1 month of start date or renewal	TRE Information Governance Process Owner
2	Take reasonable measures to prevent unauthorised access to the TRE	No more than 3 events specific to physical security are reported every 2 months.	ISMS Event and Incident Management Process Owner
3	Maintain confidentiality of information	Assessment completed for all data imports and exports prior to use to prevent the disclosure of personal or identifiable information via linkage of information	TRE Information Governance Process Owner
4	Integrity of imported information will be maintained	Checksum (file signature) tests are completed for all new raw datasets prior to use	ISM
5	Deliver services that meet the needs of our users	Availability – TRE service availability 99% Mon-Fri 09:00 to 17:00 (excluding planned outages)	ISM
		All user queries to TRE support receive an initial acknowledgement within 2 working days (*currently not measured*)	ISM
6	Manage all security events to minimise impact on the TRE	All security event assessments completed within 2 days	ISMS Event and Incident Management Process Owner
		Security event action stages are closed within agreed timescales	ISMS Event and Incident Management Process Owner

4.3. Resources needed to meet objectives and contingencies

Measure	Task	Who does this now	Contingency
1: All new staff complete their CHI induction within 1 month of start date.	New starter completes induction	Line Manager and CHI Onboarding Manager	There is a rota to ensure someone is always present to oversee induction
1: >95% of staff read and acknowledge ISMS documents within 1 month of notification.	Document Distribution & Acknowledgment	ISMS Documentation process owner	Staff Training and Competency process owner
1: All staff have completed Data protection training within 1 month of start date or renewal	Completion of training activity	Staff Training and Competency process owner	UoM/Faculty IG guardian will resume their monitoring
2: No more than 3 security events specific to physical security are reported every 2 months.	Conduct regular inspections of the physical security controls at Vaughan House	ISM	The ISM can delegate the monitoring to another member of the TRE service team
3: Assessment completed for all data imports and exports within 2 weeks of request to prevent the disclosure of personal or identifiable information via linkage of information	Monitoring service inbox for new requests, reviewing requests against any existing data sharing agreements, and conducting TRE Data import and export content checking	TRE Operations	There are 3 people within the TRE Operations team who can conduct content checking, and 2 people who can perform data transfers
4: Checksum (file signature) tests are completed for all new datasets	File integrity checks conducted and recorded in the asset register	TRE Data Management process owner	TRE System Administrator
5: Availability – TRE service availability 99% Mon-Fri 09:00 to 17:00 (excluding planned outages)	Each morning check to see that care TRE service are running OK	TRE Operations	There are 3 people within the TRE Operations team who can conduct these checks
5: All user queries to TRE support are acknowledged within 2 working days	Check the TRE-Support mail box each morning, making initial response to TRE User within 2 working days and making sure	TRE Operations	There are 3 people within the TRE Operations team who can conduct these checks

	there is ownership of the user's query		
6: All security event assessments completed within 2 days	Completing the triage process for new events	CHI-Incident Response Team	There is a rota to ensure someone is always present to conduct these reviews
6: Security event action stages are closed within agreed timescales	Making sure event actions stages are assigned to someone who has the necessary competency to resolve the issue, and that they are available to complete this task within the required timescale.	CHI-Incident Response Team	There is a rota to ensure someone is always present to conduct these reviews

5. Cross-referenced ISMS Documents

Number	Type	Title
ISMS-02-10	ISMS\Policy & Guidance\ISMS Management - policy & guidance	ISMS Manual
ISMS-02-10	ISMS\Policy & Guidance\ISMS Management - policy & guidance	ISMS Manual
ISMS-04-01	ISMS\Policy & Guidance\ISMS Improvement - policy & guidance	ISMS Management Review
SOP-04-04	ISMS\SOP\ISMS Improvement - SOP	ISMS Measurement and Monitoring

6. Appendices

None