Staff Information Security Awareness Policy

Version: 1.0
Last Review Date: 14.02.2025
Last Reviewed By: Umair Ismail
Document Owner: Umair Ismail
Approver: James Smith
Document Status: Approved

1. Rationale

Appropriate security awareness and ongoing education is required to minimise the risk from the accidental introduction of security incidents to University Information Assets (UIAs) by staff.

2. Purpose

To establish appropriate levels of security awareness resources to support the Information Security Management System (ISMS) and improve the general understanding of keeping information, accounts, and devices safe.

3. Scope

Staff, including third parties acting in a staff capacity.

4. Policy

General

Appropriate training must be targeted to support the safe use of UIAs, based on role and duties and level of access. All staff must be subject to initial information security awareness training as part of any onboarding process or induction. Including:

- Training and awareness information should be delivered through various channels, Face to face training or integrated into regular meetings and workshops.
- E-Learning facilities – internal or provided by third parties.
- Regular communications such as emails, newsletters, or other briefing mechanisms.
- Visual reminders including posters, banners, or screensavers.
- Simulated phishing exercises to enhance

All training media should be readily accessible for reuse or reference as appropriate.

Determining coverage and understanding

- Formal awareness and training must be tracked to establish coverage of the programme.
- Any training provision should ideally include some measure of understanding such as quizzes or follow up reviews.
- Staff that do not have a full understanding of relevant information security topics should seek additional support and guidance.

Renewal or refresh of training

Renewal of training should be tracked to meet specific requirements, including but not limited to:

- The annual requirement for Staff Information Security Awareness training.
- Updated training to communicate changes to guidance to relevant staff.

Vendor security training
Where specific vendor training is available (e.g., cloud provider security certifications), the content and value of this training should be considered for incorporation into the awareness programme where appropriate.

New vendor best practice should be incorporated into general staff training as it introduces more secure methods of interacting with UIAs.

5. Responsibilities

CCSS	• Identification of appropriate training. • Provision of delivery mechanisms to ensure staff have access to the required training. • Provision of tracking mechanisms and reporting to monitor overall awareness program. • Alert line managers when training needs are identified, and staff would benefit from further training.
HR	• Provision and management of Learning Management System (LMS) for staff content. • Generation and distribution of regular engagement reports to line managers.
Line Managers	• Ensure that line reports complete training as part of induction within one month of their start date. • Ensure that all line reports undertake information security awareness training at least annually. • Identification of appropriate training based on role.
Information Asset Owners	• Subject Matter Expert (SME) training specific to bespoke applications and services not covered through general information security awareness.
Third Parties	• Vendor provided training for specific applications and services. • Provision of standard hosted training packages for University use. • Ensure their staff regularly undertake information security awareness training.
Document Owner	• Maintain this document. • Assure the quality of any changes. • Create major revisions following document approval.
Approver	• Understand the organisational implications of this document and support its contents.

6. Compliance
The Staff Information Security Awareness Policy shall be enforced to meet specific compliance requirements, including but not limited to:

- Cyber Essentials
- General Data Protection Regulation (GDPR)
- PCI DSS
- UK Data Protection Act 2018

7. Further Information

- Data Protection Policy
- Staff Joiners, Movers and Leavers (JML) Policy

8. Version Control

The most current version of this controlled document is stored in our document management system (DMS). Authorised reviewers are required to 'check out' documents and summarise any changes before 'check in'. Authorised reviewers may create minor revisions, e.g., 1.0 to 1.1.

Following approval, controlled documents are incremented to the next major revision, e.g., 1.1 to 2.0. As such, controlled documents with minor revisions have not been approved. Full version history is available within our DMS.