Information Security Training Policy

1 Purpose and Scope

The University's Information Security Framework needs to be communicated to and understood by those who access information on behalf of the university and those who play a part in maintaining the technical, physical and environmental security of the university and its information. Accordingly this policy establishes a requirement for delivery of information security training to all relevant individuals as part of the Information Security Framework, and defines the objectives and scope of that training and related responsibilities.

This policy applies to members of Cardiff University as defined under Ordinance 2 - Members of the University and other workers who handle C1 and/or C2 Classified Information, as defined in the Information Classification and Handling Policy on behalf of the university, referred to below as 'relevant individuals'.

2 Policy

2.1 All staff will receive regular, mandatory training in information security which is relevant and proportionate to the type of information they are required to access and their role in maintaining the technical, physical and environmental security of the university, as set out in the attached Schedule A.

2.2 All other relevant individuals will be offered training in information security which is relevant and proportionate to the information they are required to handle on behalf of the University, as set out in the attached Schedule A.

2.3 Staff and relevant individuals will be properly briefed on their information security roles as defined in the Information Security Policy, and responsibilities prior to being granted access to Classified Information or an information system.

2.4 Staff will achieve and maintain a level of awareness on information security relevant to their roles and responsibilities; this will be measured and a record maintained.

2.5 The information security training will be tailored to the intended audience and will normally cover:

2.5.1 The need to be familiar with and comply with university information security policies as set out in the Information Security Framework in addition to all applicable laws, regulations and contracts;

2.5.2 Personal accountability for one's own actions and inactions, and general responsibilities towards securing or protecting information belonging to the university and external parties;

2.5.3 Basic information security procedures (such as information security incident reporting) and baseline controls (such as password security, malware controls and clear desks as appropriate);

2.5.4 Contact points and resources for additional information and advice on information security matters, including further information security education and training materials.

2.6 Mandatory information security training will be delivered in an accessible manner to enable all categories of staff and relevant individuals to readily access the training.

3 Roles and responsibilities

3.1 Unless otherwise stated roles and responsibilities are as set out in the Mandatory Training Policy.

3.2 The Senior Information Risk Owner (SIRO) is responsible for the university's overall information security objectives and sponsors this policy.

3.3 The Information Security Operations Group (ISOG) will be the mandatory training owner as defined under the Staff Mandatory Training Policy. The Chair of ISOG will report to the Professional Services Board, in its capacity meeting as the Compliance and Risk Group or any other successor group, on the development and delivery of the mandatory Information Security training.

3.4 Heads of Colleges/Schools/Professional Services will be responsible for ensuring that staff in the school/department/college comply with requirements for the completion of mandatory information security training and monitor compliance with this requirement in their area of responsibility, as set out in the Information Security Policy and Mandatory Training Policy

3.5 All line managers will facilitate the uptake of information security training for their staff and act on non-compliance with any mandatory requirements. *Line managers will keep records of completion of any alternative training provision for those relevant individuals who are not able to take the mandatory module via Learning Central. The relevant individuals will self-report completion.*

3.6 The Secretary to Council will ensure that lay members have undertaken the training.

3.7 The Chief Executive of the Students' Union will ensure that Students Union staff have undertaken the training.

3.8 It will be the responsibility of all staff and relevant individuals:

- to complete mandatory information security training without undue delay as soon as the modules become available to them in Learning Central (staff);
- where a specific requirement is identified to complete non-mandatory information security training activities as indicated in Schedule A.

4 Relationship with existing policies and procedures

This policy forms part of the Information Security Framework. It should be read in conjunction with:

- Information Security Policy and all supporting policies.
- Information Classification and Handling Policy
- And all Information Security Framework supporting policies

It also has a relationship with other university policies, specifically:

- Staff Mandatory Training Policy

SCHEDULE A

INFORMATION SECURITY TRAINING SCHEDULE

Category	Type of Training	Frequency
All Staff (with a record on the HR system)	On-line mandatory module provided through Learning Central with assessment test recorded in the HR system.	Within first 30 days plus annual refresh to be completed as soon as possible after release
All Staff	Live non-mandatory 'Understanding Data Protection' session, booked through HR system and co-ordinated by Staff Development	As required
All Research Staff	Live non-mandatory 'Managing Research Data' session booked through HR system and Doctoral Academy	As required
Postgraduate students	On-line module provided through Learning Central (as part of HUMRS mandatory modules for non-staff)	As required
Lay Members of University committees	In person delivery provided by Data Protection Officer	Annual
Students' Union staff	On-line module provided through Information security training - Learning materials - Intranet - Cardiff University	At induction plus annual refresher
Agency workers and other types of staff not on HR system, including student placements	On-line module provided through Information security training - Learning materials - Intranet - Cardiff	One off at commencement of role
Contractors on site: Cleaning staff Building workers IT workers Contractors Off-site: IT workers	On-line module provided through Information security training - Learning materials - Intranet - Cardiff	One off at commencement of role

Version Control	
Document Title:	**Information Security Training Policy**
UEB Policy Sponsor	Senior Information Risk Owner – University Secretary and General Counsel
Policy Owner	Senior Compliance Advisor and Data Protection Officer, University Secretary's Office
Policy Author	Senior Compliance Advisor and Data Protection Officer, University Secretary's Office
Version Number:	1.3
Equality Impact Outcome and Form Submission Date	11/05/23 – The primary impact identified was accessibility to the training module. An amendment was made to ensure the training was accessible and that line managers have a role to ensure they understand staffs' specific requirements.
Approval Date	09/02/2024
Approved By:	Senior Information Risk Owner (delegated authority from UEB)
Date of Implementation:	01/03/2024
Date of last review	November 2016
Date for Next Review:	09/02/2027
For Office Use – Keywords for search function	Information, Training