Information Security System Controls Policy

Version Control

Version Number	UEB Sponsor	Approval Body/Officer	Date of approval
1.0	Chief Digital and Information Officer	University Executive Board	05/05/2026

For queries on this policy please contact:

IT Support:

- Email: it-support@cardiff.ac.uk
- Tel: 02922 511111 (ext. 11111 internally)

Purpose and Scope

This policy exists to meet the requirement of the Information Security Policy to ensure that adequate controls are operated to protect the confidentiality, integrity, and availability of digital systems.

The purpose of this policy is to establish a baseline level of security controls to be applied to all digital systems (including, but not limited to, university hosted, cloud services, Software-as-a-Service platforms, and third-party hosted systems) holding university information.

The policy requires that responsibility for the security controls applied to all systems holding university information be explicitly allocated, and that controls are properly considered and are regularly reviewed in line with the University's risk management appetite.

The security controls applied to all systems holding confidential or non-classified university information shall be the responsibility of named individuals in accordance with the roles established in the Information Security Policy. They shall be documented, approved, and reviewed regularly, taking a risk assessment approach, to ensure that the confidentiality, integrity and availability of that information is appropriately managed on behalf of the University.

Related Policies and Procedures

This policy forms part of the Information Security Framework and should be read in conjunction with the Information Security Policy and all supporting policies (https://www.cardiff.ac.uk/public-information/policies-and-procedures/information-security).

The Information Security Classification and Handling Policy includes key information including the definition of Classified and Non-Classified.

The Software Update Policy includes key information on management of software vulnerabilities and maintaining software support.

Policy

1. The Senior Business Owner is accountable for security controls and authorising access to systems within their area of responsibility.

2. Where systems are shared or ownership is ambiguous, the SIRO shall determine the Senior Business Owner.

3. Assurance of systems controls will be documented as part of system design. This documentation will be maintained to ensure accuracy as part of systems lifecycle (upgrades, maintenance etc.).

4. University IT will define a minimum set of security controls and make available a template to support documenting control implementation and system design as outlined in Appendix A.

5. A repository shall be maintained centrally, by University IT, and will be managed under change control.

6. Controls are subject to periodic audit, and any deficiencies in controls shall be subject to a remediation plan under ownership of the Senior Business Owner.

7. The Chief Digital and Information Officer or their nominated delegate shall have the authority to agree to exceptions to the requirements of this policy.

Roles and Responsibilities

The roles and responsibilities defined within the policy are complementary to those described in the Information Security Policy.

Chief Digital and Information Officer is the sponsor for this policy, and responsible for approving the need to develop or substantively amend the policy, for presenting the final draft to the approving body, considering exceptions, and for ensuring that their policy-making documents comply with and are monitored and reviewed in line with the Cardiff University Policy for the Development of Policy-making Documents.

Senior Business Owners are accountable for information security controls for information systems used within their business area, or for which they are the nominated by the SIRO as the Senior Business Owner for information systems that cross multiple business areas. The Senior Business Owner must nominate Business Owners for dedicated information systems.

Business Owners are responsible for information system specific controls to ensure security of information as outlined in the Information Security Policy.

The **Senior Technical Owner** is accountable for technical aspects of information systems to ensure security and integrity of data. The Senior Technical Owner must nominate a Technical Owner.

Technical Owners are responsible for building and maintaining technical aspects of information systems to meet agreed design.

Information Security Oversight Group (ISOG) will review exceptions and outcomes of security control reviews from an information security risk perspective.

Technical Design Authority (TDA) will conduct an initial assessment of exceptions and proposed remediations, followed by periodic reviews to evaluate their ongoing suitability.

Monitoring and Review

This policy shall be reviewed every three years, at minimum.

Information captured as part of system design will be reviewed annually for accuracy, or during system changes (upgrades, maintenance etc.).

University IT, in partnership with Compliance and Risk, shall provide a template to record and report ownership of datasets and systems, in accordance with the policy roles.

University IT shall, wherever practicable, use automated methods to test, validate, and report on adherence of systems to the policy requirements.

Breaches of this policy may be treated as a disciplinary matter, dealt with under the University's staff disciplinary procedures or the student disciplinary procedures as appropriate.

Appendix A - Controls

The outlined controls represent the minimum level of controls for consideration. Where required, it is expected that additional controls will be implemented to ensure that systems and data are adequately protected.

1. Types of information held (including but not limited to Research, Staff, Student, Financial, Education), the classification of information held, and whether the system holds Personal Data (information about a living identifiable individual).

2. Intended users of systems, including the rationale for their level of access (e.g., all staff, all staff in a particular department/team).

3. The mechanism used to verify the identity of users authorised to access systems.

4. The mechanism used to ensure that access to information is appropriate to role.

5. Processes to manage the approval and removal of access across all roles (users, administrators, superusers). Processes shall include any pre-requisites such as training or vetting required.

6. Processes to remove access to systems when it is no longer required; supported by periodic review to ensure allocated access is appropriate.

7. Assurance that access to systems by privileged users (as defined in the IT Regulations) will be limited to authorised devices and connection methods.

8. Defining and implementing a backup and disaster recovery plan consistent with the business requirements for recovery time and retention.

9. Protection to limit impact of malware and software vulnerabilities.

10. Cryptographic measures to ensure confidentiality of information is maintained in transit and at rest, where appropriate.

11. Systems capacity management to ensure the allocation of resources is proportionate to the business requirements.

12. Systems monitoring for anomalous behaviour, with actions taken to investigate and remediate detected events. The integrity and availability of event and log data shall be preserved consistent with retention requirements, and as requested sharing data with University IT.

13. An authoritative time source used for clock synchronisation.