Information Security Policy

Version Number:	2
Document Status:	Approved
Date Approved:	19 April 18
Approved By:	Data & Information Management Oversight Group
Effective Date:	19 April 18
Date of Next Review:	March 2020

1 PURPOSE AND SCOPE

1.1 The purpose of this policy is to set out the University's aims and objectives for the management of information security throughout the University. Information Security is defined as the preservation of confidentiality, integrity and availability of information. Further definitions of all key terms are found in section 5.

1.2 The scope of the Information Security Policy covers the storage, access, transmission and destruction of information in the course of Cardiff University business. It therefore applies to the conduct of staff, students and others with access to that information (wherever the information or they are located) as well as the applications, systems, equipment and premises that create, process, transmit, host, or store information, whether in-house, personally owned or provided by external suppliers.

2 RELATIONSHIP WITH EXISTING POLICIES

This policy provides the overarching approach to the management of information security at Cardiff University and is the master policy document of the information security framework. All related policies shall be consistent with this policy.

3 POLICY STATEMENT

Cardiff University is committed to preserving the confidentiality, integrity and availability of all its key information assets in order to maintain its competitive edge, legal and contractual compliance and reputation. The information security framework (comprising this policy, supporting policies, processes and tools and the requisite management and decision-making structures) shall be an enabling mechanism for information sharing and for reducing information-related risk to acceptable levels.

4 INFORMATION SECURITY AIMS & OBJECTIVES

4.1 The information security framework will deliver a compliant and enabling environment that balances information security with appropriate accessibility and provides the optimum level of risk management to support achievement of the University's strategic goals.

4.2 Information security is included within wider activity of data and information management. The University organises the management of its information assets by using the following categories:

- Data Domains;
- IT Systems;
- End user devices;
- People.

Under the Data & Information Governance Framework each of the above has an identifiable responsible owner and information security controls are applied across all four areas.

4.3 The University will protect the security of its information assets in order to:

- maintain the integrity and quality of information, so that it is accurate, up to date and 'fit for purpose';
- make information available to those who need it and ensure there is no disruption to the business of the University;
- ensure that confidentiality is not breached, so that information is accessed only by those authorised to do so;

thereby ensuring that the University meets its legal and regulatory obligations with respect to information handling, that business is conducted efficiently, that intellectual property is protected and that the reputation of the University is safeguarded.

4.4 Information Security Objectives

4.4.1 The University will manage the risks it faces in relation to information security, keeping its risk exposure to acceptable levels as defined by the University's risk appetite. The governance structure shall include allocation of ownership of information security risks and information assets to provide accountability, and the establishment of risk assessment policy and processes.

4.4.2 The risk assessment method shall provide a consistent and systematic approach to estimating the magnitude of risks and the process of comparing the estimated risks against risk acceptance criteria to determine the significance of the risks and any changes to risk over time.

4.4.3 The framework will create consistency of approach and clarity by ensuring that information security roles and responsibilities are defined and clearly articulated via policy documents, contracts and job descriptions and that understanding is reinforced through monitored training, documented procedures, probation and annual performance development reviews, such that all individuals understand their role and responsibility with respect to information security.

4.4.4 The University will ensure that information security knowledge is shared and appropriate information security controls applied in the most efficient, effective and economical manner by maintaining high level oversight via a co-ordinating body; by embedding information security considerations into service design, transition, and delivery; and by making the necessary tools and advice on information security available throughout the University, such that all individuals can access the relevant advice, policy, procedure, training or tools in a timely manner.

4.4.5 In order to reduce the number and severity of information security incidents, and to ensure that appropriate steps are taken with respect to reporting to relevant external authorities, information security incident recording, reporting and management system will be implemented and monitored, with outcomes informing future risk assessments.

4.4.6 A supportive culture for information security will be created within the University through clear management direction and demonstrated individual management commitment to the information security framework, including acknowledgement and explicit assignment of information security responsibilities, commitment to training uptake and reporting of security incidents.

4.4.7 The University will ensure that its information security framework is fit for purpose by utilising ISO/IEC 27001:2013 Information Security Management Systems Requirements, conducting regular audits and by a process of continual improvement, benchmarking itself with respect to information security against comparator institutions where possible.

5 RESPONSIBILITIES

5.1 Council

Council has ultimate accountability for information security activities within the University. More specifically, it protects institutional reputation by being assured that clear regulations, policies and procedures that adhere to legislative and regulatory requirements are in place, ethical in nature, and followed. Council needs to be assured that there are effective systems of control and risk management, and that governance structures and processes are fit for purpose by referencing them against recognised standards of good practice.

5.2 University Executive Board

The University Executive Board is responsible via the Vice-Chancellor to Council for:

- leading and fostering a culture that values, protects and uses information for the success of the University and benefit of its members;

- defining the University's information security risk appetite in the context of the prevailing legal, political, socio-economic and technological environment and external standards;
- ensuring that a fit for purpose and adequately resourced information security framework is in place, including this policy as the top level reference document.

5.3 Senior Information Risk Owner

A Senior Information Risk Owner (SIRO) for the University's overall information security objectives shall be designated by the Vice-Chancellor. The SIRO shall be a member of the University Executive Board. The key responsibilities of the SIRO shall be to:

- ensure that this policy and the information security objectives are compatible with the strategic direction of the University;
- ensure that data and information assets are identified; that the top level data and information governance roles are allocated and that the post-holders are appropriately briefed on their information security roles and carry out their functions with due diligence;
- own the risks associated with the information security objectives and ensure that control action owners are identified;
- ensure that exception procedures are in place to authorise at an appropriate level acceptance or mitigation of significant information security risks that deviate from agreed standards;
- determine when and by whom breaches of information security shall be reported to relevant external authorities;
- ensure there is clear direction and visible management support for security initiatives and promote continual improvement;
- ensure the Vice-Chancellor and Council are adequately briefed on risk management issues.

5.4 Data & Information Management Oversight Group

The Data & Information Management Oversight Group is responsible for providing strategic direction and focus to the activities of data and information management across the University. The scope includes information security and data quality.

The Data and Information Management Oversight Group provides assurance to the University Executive Board via the Senior Information Risk Owner/Chief Operating Officer who shall chair the Data and Information Management Oversight Group. The terms of Reference are set out in Annex A.

5.5 Data & Information Governance Roles

Supporting Data & Information Governance roles shall be established by the Senior Information Risk Owner (Annex B)

5.6 Heads of Schools/Departments/Colleges

Responsible for:

– ensuring that staff are aware of the need to adhere to this policy and associated information security policies;
– reporting non-compliance via the defined and approved channels.

5.7 All users

All individual users of University information systems and those handling or having access to University information outside of those systems shall be responsible for:

- complying with all relevant information security, policies, practices and procedures including any external accountability;
- ensuring that they request, where necessary, and receive adequate and relevant information security awareness training to enable them to undertake their roles; and
- reporting information security incidents via the defined and approved channels.

6 BREACHES OF POLICY

Breaches of the Information Security Policy may be treated as a disciplinary matter dealt with under the University's staff disciplinary policies or the Student Disciplinary Code as appropriate.

7 DEFINITIONS

Availability	Having appropriate access to Information Assets as and when required in the course of University business
Confidentiality	The restriction of information to those persons who are authorised to receive or access it
Information	Data that has a meaning or can be interpreted. It can be held as an electronic record or in a non-electronic format such as paper, microfiche, photograph
Information Asset	Information that has value to the University. Key Information Assets are the most important types of information required for achievement of the University's strategic aims
Integrity	The completeness and preservation of information in its original and intended form unless amended or deleted by authorised people or processes
Quality	The state of completeness, validity, consistency, timeliness and accuracy that makes data appropriate for both operational and strategic use.

ANNEX A

Data and Information Management Oversight Group Terms of Reference

The Data and Information Management Oversight Group is responsible for providing strategic direction and focus to the activities of data and information management across the University. The scope includes information security and data quality.

The Data and Information Management Oversight Group provides assurance to the University Executive Board via the Senior Information Risk Owner/Chief Operating Officer who shall chair the Data and Information Management Oversight Group.

1. review and approve the University's portfolio of data and information management policies to ensure that it continues to align with the University's strategic objectives
2. monitor and review the University's risk exposure in the areas of data and information governance;
3. provide strategic focus for the application of data and information quality and security controls across information and assets, based on a risk assessment approach;
4. ensure standards are set and periodically reviewed
5. consider requests for exceptions and provide authority where appropriate
6. communicate and promote value of data and information assets
7. ensure that adequate training is in place to support the University's data and information management objectives
8. monitor and review the University's response to information security incidents;
9. review data and information governance audit findings and recommendations.

ANNEX B: Supporting Data & Information Governance Roles

ROLE	LEVEL	RESPONSIBILITIES
Senior Information Risk Owner	**Executive Board member**	Accountable for ensuring that data management and information security policy and the associated objectives are compatible with the strategic direction of the University; own the risks associated with the associated objectives and ensure that control action owners are identified, including identifying key Information Assets, nominating Data Leads and Senior System Owners; authorise acceptance or mitigation of significant information security risks that deviate from agreed standards; determine when and by whom breaches of information security shall be reported to relevant external authorities; ensure there is clear direction and visible management support for data management and security initiatives and promote continual improvement; ensure the Vice-Chancellor and Council are adequately briefed on risk management issues. Senior Liaison Contact for HESA.
Data Lead	**Professional Services Directors**	Accountable for quality of data within their domain; Ensure data within the domain is fit for operational and strategic use; Determine conditions under which data may be used (taking account of any legal obligations applying to that type of data), in order to safeguard confidentiality, integrity, availability and quality; Confirm classifications of data entities within the domain; Confirm data requirements for business purposes.
Senior System Owners (Business)	**Directors**	Confirm business purposes and required outcomes of systems; Accountable for system specific policy controls to ensure security and quality of data including compliance with the terms of any 3rd party license or other contractual terms applying to the University's access to, or permitted use of, the system; Nominate System Owners (Business) for dedicated systems; Confirm service level agreement requirements re availability of the system.
Senior Systems Owner (Technical)	**Chief Information Officer**	Accountable for technical aspects of systems to ensure security and integrity of data; Nominate System Owners (Technical)

University Data Steward	**Director Strategic Planning & Governance**	Be final arbiter over decisions affecting relationships between data fields and objects; Be final arbiter over decisions affecting transformations of data objects; Strategic co-ordination of external data reporting; Oversight of the implementation of the data management and information security frameworks (including information security incident management), ensuring they are reviewed periodically and remain fit for purpose.
System Owner (Technical)	**Snr Manager (IT)/Service supplier**	Build and maintain system to meet agreed design; Set up and maintain data transfers; Implement authentication and access permission controls; Implement antivirus and malware controls; Implement back-up and restore capability; Implement user attribute technical controls; Implement auditing capability and produce monitoring reports as required; Implement system retention and disposal requirements; Implement data quality system controls; Provide metrics for risk assessment; Develop information security and data quality technical procedures.
System Owner (Business)	**Snr Managers**	Responsible for system specific policy controls to ensure security and quality of data; Define required data needs and outputs from applications/systems; Balance the confidentiality, integrity and availability needs of the information under their control in the best interests of the University and in line with agreed risk acceptance; Confirm system user groups/roles with associated permissions; Define appropriate access environments and user attributes; Define appropriate back-up and restore requirements; Document an Information Security Specification for each system; Document an Information Security Specification for each system; Define system auditing and monitoring report requirements; In association with the Data Lead nominees define retention and disposal requirements for system records; Assess risks to data security within systems; In association with the Data Lead nominees, define system specific data quality and security processes and procedures.
Data Stewards	**Snr Managers**	Work with System Owners to ensure the quality of the data entities is sufficient to meet the requirements for both operational use and strategic business intelligence use; Define the meaning of data entities; Confirm and review classifications of data entities; Assess risks to data quality and advise relevant System Owners; Determine required data quality checks and controls and advise System Owners; Change management where data definitions change; Define retention requirements for data entities