Information Security Specification (Systems Level) Policy

Version Number:	2.0
Document Status:	Approved
Date Approved:	19th April 2018
Approved By:	Data & Information Management Oversight Group
Effective Date:	19th April 2018
Date of Next Review:	March 2020

1 Purpose

The purpose of this policy is to ensure that responsibility for the security controls applied to individual information systems holding Classified University Information, or Non-Classified datasets that are critical to the University's functions, has been explicitly allocated and that those controls have been properly considered, appropriately documented in a Specification and approved, and that such Specifications are regularly reviewed.

2 Scope

This policy covers all information systems holding Classified University Information (e.g. Student Information Management System, Core HR, IT network, University email and the internal postal system). It covers both paper filing systems and electronic systems where they fall under the above scope. (For further detail see Definitions in section 8 below).

3 Relationship with existing policies

This policy forms part of the Information Security Management Framework. It should be read in conjunction with the Information Security Policy and all other supporting policies.

4 Policy statement

The security controls applied to all systems holding Classified University Information or Non-Classified critical datasets shall be the responsibility of named individuals. They shall be documented, approved and reviewed regularly, taking a risk assessment approach, in order to

ensure that the confidentiality, integrity and availability of that information is appropriately managed on behalf of the University.

5 Policy

5.1 The Senior System Owner (Technical) for all IT systems holding Classified University Information or Non-Classified critical datasets shall be the Chief Information Officer.

5.2 All such systems shall also have a Senior System Owner (Business) and a documented Information Security Specification. The Information Security Specification shall identify the System Owner (Business) and System Owner (Technical) and include a description of:

- How it is determined which users and administrators will be authorised to access the system, who authorises the initial access, who determines the appropriate level of access and any pre-requisites in terms of training or vetting required
- How the authorised users' identities are verified when accessing the system (including any relevant password policy) and whether any means of access (e.g. off campus, remote access, personal device) will be prohibited and if so how this will be achieved
- The levels of security within the system in relation to the user and administrator types, the classification of the information to which they have access and the type of access (read/write/edit/etc)
- Any physical/technological controls to prevent removal or copying of data from the system
- How the system will be backed up including frequency and responsibility
- What are the permitted uses of the information in the system and how this is communicated to the users/administrators (and any data subjects in terms of data protection notices where relevant)
- Which other systems will feed data into this system
- Which other systems will receive data from this system
- What audit trails are in place to record user/administrator actions
- Whether any compulsory user/administrator, induction or refresher training is required and how this will be enforced
- How changes to access rights for users and administrators (including removal of rights) will be instigated, applied and authorised

5.3 Existing Data Systems – All IT systems holding Classified University Information or Non-Classified critical datasets shall document an Information Security Specification with supporting documented procedures within a timescale approved by the Senior Information Risk Owner.

5.4 All IT system Information Security Specifications shall be reviewed by the IT Technical Design Authority every two years. Additional triggers for these reviews shall include the annual information asset risk assessments and any proposed architectural changes to existing systems that are referred to the Technical Design Authority.

5.5 New data transfers between systems – whenever a need is identified to re-use data from an existing system the Data Re-use Authorisation Procedure (see Annex A) should be followed to ensure that key stakeholders are consulted/notified and that appropriate authority is in place

relating to the data flows and security of the assets during transfer and in any new system and environment. The Procedure will require the development of an Information Security System Specification and that the Technical Design Authority review the Information Security Specification as part of the procedure.

5.6 New IT Systems – All new IT Systems holding Classified University Information or Non-Classified critical datasets shall have an Information Security Specification documented as part of their development. Information Security Specifications for such new IT systems shall be reviewed by the Technical Design Authority as part of the approval process. An approved Information Security Specification shall be a requirement of any IT release gate and no information system shall 'go live' without an approved Information Security Specification in place.

6 Responsibilities

6.1 The System Owners (Business) shall be responsible for ensuring that the Information Systems Security Specifications are complete, up to date and accurate. The System Owners (Business) shall, in liaison with the System Owner (Technical) and the Technical Design Authority, review the Specifications whenever there is a proposed change to the system that may affect the controls applied (including their necessity) and following the annual information asset risk assessment exercise to determine whether *associated* changes to the Specification are required.

6.2 The relevant Senior System Owner (Business) shall approve the Information Security Specifications for the dedicated systems holding that data, taking a risk assessment approach, informed by the Technical Design Authority's findings and the University's acceptable level of risk. The relevant Senior System Owner (Business) shall also approve any changes or amendments to a Specification in the same manner.

6.5 The Technical Design Authority shall be responsible for reviewing the Information Security System Specifications in line with the policy requirements set out above, and for providing advice to the System Owners and Senior System Owners on any areas of weakness and/or outstanding risks.

6.6 The Senior System Owner (Technical) shall ensure that a register is kept of all approved IT system Information Security Specifications and that all new IT systems have an approved Information Security Specification prior to 'go live'.

6.7 The Data and Information Management Oversight Group shall consider Information Security System Specifications referred to it by one or more Senior System Owners (Business or Technical), by the Technical Design Authority or by the Senior Information Risk Owner and advise the Senior Information Risk Owner on areas of weakness and outstanding risks.

6.8 The Senior Information Risk Owner shall have the authority to approve a deviation from the recommended level of information security controls.

7 Compliance

Breaches of this policy should be reported to the Senior Information Risk Owner and may be treated as a disciplinary matter dealt with under the University's staff disciplinary policies.

8 Definitions

University Information: any information (in any format) that the University acquires, creates, modifies or stores in connection with its own business purposes. Such information is categorised into Classified (Highly Confidential or Confidential) and Non-Classified. University Information Classification categories can be found at: *http://sites.cardiff.ac.uk/isf/handling/*

Senior System Owner (Business): The Senior System Owners (Business) are accountable for defining the business needs to be met by the system and for the on-going management of the system within the policy context to meet those needs. The Senior System Owner (Business) takes a governance role, ensuring that the system is managed to meet the needs of the business and that it supports data quality requirements.

System Owner (Business): System Owners (Business) are responsible to the Senior System Owner (Business) for defining the business requirements to be delivered by the system and for system specific controls to ensure the quality of the data. This role is performed by staff nominated by the Senior System Owner (Business). These are staff who have management responsibilities with respect to the processes that the system delivers or supports. The role of the System Owner (Business) includes understanding what information is held, what is added and what is removed, how information is moved, who has access and why.

Senior Systems Owner (Technical): The Senior Systems Owner (Technical) is accountable for defining and assuring the technical standards, controls and operations required to maintain the data on IT systems, in accordance with business requirements. This role is performed by the Chief Information Officer.

System Owner (Technical): System Owners (Technical) are responsible to the Senior Systems Owner (Technical) for maintaining the data and implementing technical controls on IT systems, in accordance with business requirements. This role will focus on system data collection methods, system processes and system security. This role is performed by staff nominated by the Senior Systems Owner (Technical), normally IT Services staff and/or contractors.

Senior Information Risk Owner: The Senior Information Risk Owner for the University's overall information security objectives is designated by the Vice-Chancellor. The Senior Information Risk Owner shall ensure that the University's information security objectives are compatible with the strategic direction of the University and shall own the associated information security risks.

Technical Design Authority: The Technical Design Authority is a group within Portfolio Management and IT Services responsible for guiding, evaluating and approving high-level architectural designs and identifying appropriate technical resource to carry these forward to

implementable designs, as well as agreeing and enforcing technical standards and strategies, and approving any exceptions to those technical standards.