Information Security Policy

Systems Planning Policy

1 Introduction

1.1 This Policy sets out how Information systems are to be specified and designed and includes processes for identifying requirements and risks, designing appropriately configured systems to meet them and assigning responsibility for their security.

2 Objectives

2.1 To achieve and maintain appropriate protection of the University's assets.

2.2 To prevent unauthorised physical access, damage and interference to the University's premises and information.

2.3 To prevent loss, damage, theft or compromise of assets and interruption to the University's activities.

2.4 To minimise the risk of system failures.

2.5 To prevent unauthorised access to operating systems and information held within information systems.

3 Scope

3.1 This policy applies to managers with responsibility for planning, procuring or commissioning of information systems.

3.2 Information systems should be understood to mean the critical information systems that serve the core purpose of the University, e.g. Library systems, Financial systems, Student systems, Research Systems, E-learning systems, Email, Web servers etc.

4 Policy

4.1 New information systems, or enhancements to existing systems, must be authorised jointly by the manager(s) responsible for the information and the Director of IT Services. The business requirements of all authorised systems must specify requirements for security controls.

4.2 Before any new systems are introduced, a risk assessment process will be carried out which will include an assessment of the legal obligations that may arise from the use of the system. These legal obligations will be documented and a named system controller, with responsibility for updating that information, will be identified.

4.3 The information assets associated with any proposed new or updated business system must be identified, classified and recorded in accordance with the Information Handling Policy, and a risk assessment undertaken to identify the probability and impact of failure in system confidentiality, integrity or availability. Where there is the potential for the system to impact on the privacy of individuals, a privacy impact assessment shall be undertaken to identify and appropriately mitigate such risks. The information security risk assessment and the privacy impact assessment may be combined in a single process.

4.4 Equipment supporting business systems shall be planned to ensure that adequate processing power, storage and network capacity are available for current and projected needs, all with appropriate levels of resilience and fault tolerance. Equipment shall be correctly maintained.

4.5 Equipment supporting business systems shall be given adequate protection from unauthorised access, environmental hazards and failures of electrical power or other utilities.

4.6 The implementation of new or upgraded software associated with information systems shall be carefully managed according to the Software Management Policy.

4.7 Access controls for all information and information systems are to be set at appropriate levels in accordance with the value and classification of the information assets being protected.

4.8 Access to operating system commands and application system functions is to be restricted to those persons who are authorised to perform systems administration or management functions. Where appropriate, use of such commands should be logged and monitored.

4.9 Prior to acceptance, all new or upgraded systems shall be tested to ensure that they comply with the University's information security policies, access control standards and requirements for ongoing information security management.

4.10 Where a system is to be provided as a managed service, or operated on infrastructure provided or operated by a third party, particular attention shall be paid to the legal, security and privacy requirements in:

- specifying the service provision requirements;
- designing the provider selection process;
- drawing up the contract for the provision of the service;
- setting up and maintaining joint operational processes;
- reviewing the service provision at regular intervals.

5 Related Policies

5.1 This policy should be read alongside the Software Management Policy, the Operations Policy, the Systems Management Policy and the Third Party Access Policy.

Ownership:

Owner	Department/Team
Director ITS	ITS

Authors:

Author(s)	Department/Team
Jerry Niman	Consultant

Contributors and Reviewers:

Contributor/Reviewer	Department/Team
Matthew Trump	Information Service Assurance Manager

Revision History:

Version Number	Status D/R/A/I[1]	Date Issued	Reason for Issue	Issued by
0.21	R	19/1/2010	Updated following ISWG Discussion	
1.0	A	25/1/2010	Final Version	
1.1	D	9/1/2015	Added privacy consideration to 4.3, added 4.10 and added Third Party Access Policy to 5.1	SR
1.2	R	23/02/2015	Issued to ISC for Approval	PD
1.3	I	3/3/15	Approved by ISC for issue	PD
1.4	I	20 June 2017	Minor Amendments	MT

[1] D = Draft; R= Ready for approval; A = Approved for issue; I = Issued