1. Introduction

1.1. This information security policy document sets out principles for how University information systems are to be specified and designed to meet security requirements and manage risks. It is a sub-document of Information Security Policy (ISP-S1).

1.2. This document includes statements on:
   - Scope
   - Specification or design
   - Authorisation and assessment
   - Equipment planning
   - System access
   - Implementation
   - Documentation

2. Scope

2.1. This system planning policy relates to information systems that are used to provide services that are important to the business of the University.

2.2. This policy does not apply to deployment of additional instances of an existing tested and approved solution such as the standard CFS desktop client.

2.3. In relation to IT systems, this policy to refers to both hardware and software.

2.4. The principles covered in this policy also apply when planning for use of information systems or services provided by other organisations. See also:
   - Outsourcing and Third Party Access Policy (ISP-S4)

3. Specification or design

3.1. During specification or design of significant new information systems, or major upgrades to existing systems, information security risks should be identified and assessed. Those risk mitigation measures considered essential should then be incorporated into the specification or design.

3.2. General advice is offered by IT Services.

3.3. When planning highly sensitive, critical or specialised systems it is recommended that specialist security advice should be sought.

4. Authorisation and assessment

4.1. Projects to deliver new information systems, or significant upgrades to existing systems, should include authorisation and assessment phases:
• Before progressing from the specification or design phase into development or installation.
• As part of acceptance testing before progressing into live service.

4.2. This authorisation and assessment should include:

• Business approval – management approves the purpose and use of the system and ensures that the system is consistent with departmental strategy and any broader strategy (for systems that will provide a service beyond the department).

• Information security approval – the new system complies with relevant policies and does not adversely affect the security of existing information infrastructure.

• Technical approval – the system is approved from a technical perspective by the relevant technical managers.

4.3. Payment card processing systems must not be planned, commissioned, used or modified without consultation with and approval by the Finance Office. Refer to policy sub-document:

• Payment Card Security (ISP-I10)

5. Equipment planning

5.1. Computer 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.

5.2. Computer systems shall be given adequate protection from unauthorised access, environmental hazards and failures of electrical power and other utilities. See also:

• Operations Policy for IT Service Providers (ISP-S6)

6. System access

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

6.2. 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.

6.3. See also

• User Management Policy (ISP-S8)

7. Implementation

7.1. Following testing and approval new or upgraded systems shall be implemented and operated in accordance with University information security policies.

8. Documentation

8.1. Documentation of the planning process should include evidence that information security needs have been assessed and addressed. Findings of risk assessments and decisions taken in light of those assessments should be documented.

9. Related policy documents
9.1. From planning to providing a live service, project and system managers should be familiar with information security policy generally and in particular these documents:

- Information Asset Protection Policy (ISP-S2)
- Operations Policy for IT Service Providers (ISP-S6)
- Information Handling Policy (ISP-S7)
- User Management Policy (ISP-S8)
- Use of Computers Policy (ISP-S9)
- System Management Policy (ISP-S11)
- Network Management Policy (ISP-S12)
- Software Management Policy (ISP-S13)

Failure to comply with University Policy may lead to disciplinary action.

Document history:

14 May 2010 (C. Nelson) Began first draft.
12 July 2010 (C. Nelson) Approved.
18 May 2011 (C. Nelson) Revisions resulting from review within IT Services.

The official version of this document will be maintained on-line. Before referring to any printed copies please ensure that they are up-to-date.