System Planning and Management Policy

1. Introduction

The System Planning and Management Policy sets out how university information systems are specified, designed and managed. It includes processes for identifying requirements and risks, and designing appropriately configured systems to meet them. It also covers assigning responsibility and required behaviour of those managing university computer systems, including requirements on the maintenance and management of information systems and the software and services they run.

2. Scope

2.1. This policy relates to information systems that are used to provide services that are important to the business of the University.
2.2. In relation to IT systems, this policy refers to both hardware and software.
2.3. The principles covered in this policy also apply when planning for use of information systems or services provided by other organisations.
2.4. This policy applies to all staff that use administrator privileges on any University owned or managed multi-user computer or software application service.

3. Planning Authorisation and Assessment

3.1. A management approval process for new systems, or upgrades to existing systems, is in place to ensure that the development is for a clear purpose, will provide an adequate level of security protection, and will not adversely affect the security of the existing university information systems.
3.2. Business approval – each development should have appropriate management approval, authorising its purpose and use.
3.3. Information security approval – each development must specify the requirements for security controls and must also comply with all relevant university security policies.
3.4. Technical approval – each development must be approved by the designated faculty and department technical managers.

4. System Managers

4.1. University computer systems must be managed by suitably trained and qualified staff to oversee day to day running and to preserve security and integrity with nominated individual system owners.
4.2. System managers have a key role to play in ensuring confidentiality, integrity and availability of University information and information systems. They are responsible for endeavouring to ensure correct and secure operation of computers in accordance with both university level policies and any relevant departmental policies.
4.3. System managers are required to be familiar with all university Information Technology and IT Security policies. They must be familiar with this document and other documents which are of particular relevance to system managers, including:

- Network Management Policy
- Information Handling Policy

- Software Management Policy
- Use of Computers Policy

4.4. System managers must take into account the confidentiality and value of the information they are managing, and the impact that a serious incident (such as hardware failure, information loss and user account misuse) may have when determining what security controls and risk mitigation measures to use.

4.5. System managers are required to be proactive in liaising with information owners to help and ensure that security requirements, expectations and limitations are understood.

5. Access Control

5.1. Administrative access to all university information services shall use a secure logon process and access to high risk systems shall, where appropriate, also be limited by time of day or by the location of the initiating terminal or both.

5.2. Access controls shall be maintained at appropriate levels for all systems by ongoing proactive management and any changes of access permissions must be authorised by the manager of the system or application. A record of access permissions granted must be maintained and made available to the IT Governance Manager on request.

5.3. Inactive terminals in high risk locations or serving high risk systems shall shut down after a defined period of inactivity to prevent access by unauthorised persons.

5.4. Password management procedures shall be put into place to ensure the implementation of the requirement of the Principal Information Technology and Security Policy and to assist users in complying with best practice guidelines. See also:

- User Management Policy

6. Planning and Monitoring System Activity

6.1. Capacity demands of systems supporting business processes shall be monitored and projections of future capacity requirements made to enable adequate processing power, storage and network capacity to be made available.

6.2. All access to IT services will be logged and monitored to identify potential misuse of systems or information.

6.3. Security event logs, operational audit logs and error logs must be properly reviewed and managed by qualified staff.

6.4. Access to operating system commands 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.

7. Importing Files

Software and data files intended for installation on critical business systems should be downloaded or installed into a secure environment, scanned for malicious software and where possible and tested in a test environment before deployment in a live environment.

8. Data Backup

To ensure that data and software can be recovered following a media failure or computer disaster, backup copies of all essential data and software must be regularly taken. The backup requirements for each system or business application will vary and need to be defined and regularly reviewed in accordance with the Information Handling Policy. Backup arrangements for individual systems must also meet the

requirements of business continuity plans and backup data should be regularly tested, where practicable, to ensure that it can be relied upon for emergency use when necessary.

9. System Clocks

System clocks must be regularly synchronised between the university's various processing platforms.

10. Document Approval

Approved by: Kathryn Arnold CIO
Approved Date: October 5th 2012
Review Date: October 5th 2013
Reviewer: IT Governance Manager

11. Document History

11.1. 10th March 2011 – Draft 1 Neil Faver
11.2. 13th June 2011 – Draft 2 Neil Faver
11.3. 22nd March 2012 – Draft 3 Neil Faver
11.4. 5th October 2012 – Version 1 Neil Faver