Software Management Policy

1. Introduction

1.1. This policy sets out how the software which runs on the university's IT systems is managed. It includes controls on the installation, maintenance and use of software, with appropriate procedures for upgrades to minimise the risk to information and information systems.

2. Scope

2.1. This policy is applicable to all equipment that connects to the university fixed and wireless network.
2.2. This policy should be familiar to all staff involved in the specification, installation and maintenance of software.

3. Software Security Management

3.1. There must be a nominated individual or business unit responsible for every item of software deployed in the university network.
3.2. Software applications are to be managed by suitably trained and qualified staff to oversee their day to day running, and to preserve security and integrity in collaboration with nominated individual application owners.
3.3. All staff managing software applications shall be given relevant training in information security issues.
3.4. The procurement or implementation of new or upgraded software must be carefully planned and managed. Any development for or by the university must document the requirements for Information Security.
3.5. Information security risks associated with the procurement or implementation of new, or upgraded, software must use a combination of procedural and technical controls to mitigate any risks.

4. Change Control

4.1. For all university owned and managed equipment, formal change control procedures, with comprehensive audit trails, must be used for all changes or upgrades to business software.
4.2. All changes to operating systems and ancillary software must be properly authorised, and must be tested appropriately before changes are moved to the live environment to ensure there is no adverse impact on university operations or security.

5. Software Development

5.1. Modifications to vendor supplied software shall be avoided as far as possible, and only strictly controlled essential changes shall be permitted, after agreement with the vendor, and the development of interfacing software shall only be undertaken in a planned and controlled manner.
5.2. Upgrades or other changes to locally developed software must be assessed to mitigate any potential risk to information security.

6. Software Regulation

6.1. The use of illegal software and using software for illegal activities is not permitted and may lead to disciplinary action.
6.2. All software installed on University computer systems must have an appropriate licence covering its intended use.
6.3. Use of software which tests or attempts to break university system or network security is prohibited unless the Network Manager has been notified and has given authorisation.
6.4. Use of software which causes operational problems, causes inconvenience to others, or which makes demands on resources which are excessive or cannot be justified, will be prohibited.
6.5. Software found on university systems which incorporates malware of any type is liable to be automatically or manually removed or deactivated.
6.6. Any system that monitors the activities of other people for the purpose of gathering personal information is not permitted unless authorised by the Chief Information Officer in accord with the Director of People and Organisational Development.

7. Document Approval

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

8. Document History

8.1. November 2010 – 1st Draft Neil Faver
8.2. 21st February 2011 – Draft 2 Neil Faver
8.3. 10th March 2011 – Draft 3 Neil Faver
8.4. 4th April – Draft 4 – Neil Faver
8.5. 13th June 2011 – Draft 5 – Neil Faver
8.6. 5th October 2012 – Version 1 – Neil Faver