Policy: **ISP-S13**
Title: **Software Management Policy**
Status: **Approved**

1. Introduction

1.1. This information security policy document contains high-level descriptions of expectations and principles for managing software on University computer systems. It is a sub-document of Information Security Policy (ISP-S1).

1.2. Definitions:

- Software management - any procurement, development, installation, regulation, maintenance or removal of software that takes place on University owned computers or computers permitted connection to University networks.

1.3. Software is very important to the University because it is used extensively to enhance, or enable, performance of many key activities. Software management decisions taken across the University influence efficiency, economy and information security. This document is primarily concerned with security aspects of software management.

1.4. This document includes statements on:

- General software management principles
- Managing security risks relating to software
- Permitted, regulated and prohibited use of software

2. General software management principles

2.1. All software, including operating systems and applications must be managed correctly.

2.2. There must be an identifiable individual or organisation taking current responsibility for every item of software deployed.

2.3. Those responsible for software must monitor relevant sources of information which may alert them to a need to act in relation to new security vulnerabilities.

2.4. Software is to be patched as soon as possible to remove security vulnerabilities.

2.5. Staff involved in managing software must have experience, training or qualification commensurate with the importance of the software and risk levels involved. At the minimum all staff involved must be aware of, and proactive in managing, information security related risks associated with software. University departments must support this policy by ensuring that permission and responsibility for systems and software management is delegated accordingly.

2.6. University software management procedures must incorporate measures for controlling these information security risks:

- Illegal use of software
- Use for of software for illegal purposes

- Software copyright infringement
- Inadequate control over data access by software
- Insecure software design, configuration or usage procedures
- Software network services vulnerable to attack
- Software causing operational problems to systems or network
- Untrusted mobile code, viruses, “Trojans”, worms and spyware

3. Managing security risks relating to software

3.1. Software procurement

- When business requirements for new systems or enhancements are being specified, the specification documents should describe any special or essential requirements for security controls.
- When software for use by the University is being procured there must be an assessment of whether the software incorporates adequate security controls for its intended purpose.
- It must be investigated and taken into account whether proposed new software or upgrades are known to have outstanding security vulnerabilities or issues.
- At the time of software procurement, the basis of future support and the expected supported lifetime of the product should be established. It may be important to have assurance that manufacturers will provide updates to correct any serious security vulnerabilities discovered in future.
- Consideration should be given to software escrow for mission critical applications. In a software escrow agreement the software source code is deposited into an account held by a third party escrow agent. Escrow is typically requested by a software licensee to ensure maintenance of the software. The software source code is released to the licensee if the licensor fails to maintain and update the software as promised in the software license agreement. (Expertise and advice on purchasing matters is available from the University Purchasing Office.)

3.2. Software development

- Software developed at the University must be assessed for its potential to introduce information security risks and any such risks must be adequately addressed.
- Upgrades or other changes to locally developed software must be assessed in terms of whether they may introduce an increased risk to information security. Any risks identified must be suitably addressed.

3.3. Software modification

- In-house customisation of externally written software should be avoided where it may lead to future difficulty for the University in obtaining external support. Only strictly controlled essential changes should be permitted and all changes made should be fully documented.

3.4. Software installation

- For each item of software managed by a department a master copy of any media, enabling codes and installation instruction must be stored safely in accordance with departmental procedures.
- Software must not be put into user service on University systems unless a department or group has assessed and committed to providing sufficient resourcing for its ongoing management. (Software applications and systems utilised by the University vary widely in cost, relative importance, user numbers, complexity, maintenance requirements and code quality. These factors must be taken into account when evaluating the ongoing resourcing commitment that will be required.)

3.5. Software regulation

- Use of illegal software and using software for illegal activities could be construed to be gross misconduct.
- Use of software which tests or attempts to break University system or network security is prohibited unless the Director of IT has been notified and given authorisation.
- Use of software which causes operational problems that inconvenience others, or which makes demands on resources which are excessive or cannot be justified, may be prohibited or regulated.
- Software found on University systems which incorporates malware of any type is liable to automated or manual removal or deactivation.
- Use of software that monitors the activities of other people is subject to regulation. For further information refer to :
    - Institutional IT Usage Monitoring and Access (ISP-I6)

3.6. Software maintenance

- Change control procedures, with comprehensive audit trails, must be used for all changes or upgrades to software of importance. Where correct operation of the software is itself important, or of importance to a wider system, changes must be authorised and tested before being applied to the live environment.
- Software must be actively maintained to ensure that all fixes and patches, needed to avoid significant emerging security risks, are applied as promptly as possible.
- Changing software of critical importance that is in service may sometimes be judged too risky. For example the risk of something going wrong as a result of installing a patch may seem greater than the risk associated with not installing it. It is good software management practice to assess such risks, make an informed judgement and document the reason for the decision. When it is necessary to defer installing a security fix, a less risky way or time to proceed with the installation must be sought.
- Systems running software, including the operating system, which are clearly not being maintained adequately and which may be presenting a wider risk to security are liable to have their University network connectivity withdrawn. This decision may be made by the Network Authority for the department responsible for the system; however, it may also be made by the Network Services Section of IT Services. Related information may be found in:

- Network Management Policy (ISP-S12)

3.7. Software removal

- Software that is not licence compliant must be brought into compliance promptly or uninstalled.
- Software that is known to be causing a serious security problem, which cannot be adequately mitigated, should be removed from service.
- Operating systems and application software must not be abandoned or otherwise left unmaintained for extended periods. Systems and application software that are no longer required should be decommissioned; where they will not be managed for an extended temporary period they should be removed from service.
- When decommissioning a computer system, for disposal or re-use, appropriate measures must be taken in relation to any software and data stored on it. Software must be removed, where not doing so could lead to breaking the terms of its licence. Further details relating to secure disposal or re-use of equipment may be found in:
  - Information Handling Policy (ISP-S7)

4. Permitted, regulated and prohibited use of software

4.1. The University must comply with its overriding legal and contractual obligations. Some of these obligations affect software and the uses to which it may be put. Further information may be found in:

- Compliance Policy (ISP-S3)

4.2. The Director of IT has responsibility for IT at the University and on behalf of the University is permitted to regulate or prohibit use of particular software or types of software for the overall benefit of the University. For example it may be necessary to regulate use of particular software applications or limit usage of particular types of application in order to prevent operational problems. For applicable regulations and controls that apply to the acquisition and use of software in compliance with this policy refer to:

- Software Regulations (ISP-I11)

4.3. Heads of Department may implement additional specific local policies relating to IT management, which may include further restrictions affecting software.

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

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.