Software Management Policy (ISP-13)

1. Introduction

This Software Management policy is a sub-policy of the Information Security policy (ISP-01) and sets out the principles and expectations for the security aspects of managing software.

2. Scope

This policy applies to all University-owned systems and any third party systems managed on behalf of the University, anyone responsible for installing and managing software on University systems, and anyone using software installed on a University system.

2.1 Definitions

Software management - any procurement, development, installation, regulation, maintenance or removal of software that takes place on systems owned by, managed by or for the University.

Software asset - all software, software licences, support and maintenance agreements used within the University.

Software manager - Any individual installing software on University systems is considered a Software Manager.

University systems - includes all University-owned devices that are able to be programmed to run logical operations or arithmetic. This includes but is not limited to laptops, desktops, tablets, smartphones, wearables, physical and virtual servers and network infrastructure, on or off premises.

3. Policy

3.1. General Software Management Principles

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

There must be an identifiable individual and deputy, or organisational unit, taking current responsibility for every item of software formally deployed.

Individuals installing software from non-University managed software repositories are responsible for the active management of that software instance.

Those responsible for software must monitor relevant sources of information that may alert them to a need to act in relation to new security vulnerabilities. This may include instruction from IT Services. Failure to act may result in removal of the software, isolation of the device or removal of privileged access.

Software managers are responsible for ensuring software remains compliant with University standards and relevant security frameworks.

Installation, maintenance and removal of software should follow IT Service Management processes.

3.2. Software Procurement

Due diligence for software procurement should be conducted in accordance with the Outsourcing and Third Party Compliance Policy (ISP-04).

At the time of software procurement, the basis of future support and the expected supported lifetime of the product should be established. It is important to have the assurance that manufacturers will provide updates to correct any serious security vulnerabilities discovered in future.

3.3. Software Installation

Checks should always be made that there is a valid licence before installing software and users advised of any special conditions regarding its usage. All software licenses must be notified to the to the IT Software Licensing Team.

Managed installs should be used wherever possible - in line with current procedures to ensure software is maintained and use of individual administrative privilege is limited.

Software assets and other software files must be stored securely and managed effectively.

Software must not be put into active use on University systems unless a department or group has assessed and committed to providing sufficient resourcing for its ongoing management. Appropriate assessments or tests should be made to avoid new software causing operational problems to other systems on the network.

3.4. Software Regulation

Use or installation of unlicensed software or using software for illegal activities constitutes a disciplinary offence as detailed in the Acceptable Use Policy (ISP-09) section ‘3.8 Penalties for Misuse’.

Use of software that tests or attempts to compromise University system or network security is prohibited unless authorised by the Chief Information Security Officer for the duration of those tests.

Use of software that causes operational problems that inconvenience others, or that makes demands on resources that are excessive or cannot be justified, may be prohibited or regulated.

Software found on University systems that incorporates malware of any type, or that does not conform to the restrictions outlined in this policy, is liable to automated or manual removal or deactivation.

The installation and use of software will be monitored by IT Services to ensure we are fulfilling our licencing obligations. The University needs to ensure it is maximising the value of its software assets.

For further guidance on the use of University software and other facilities, refer to the Acceptable Use Policy (ISP-09) and the Compliance Policy (ISP-03).

3.5. Software Maintenance

Software managers are responsible for maintaining the integrity of software by applying security patches in a time period proportionate to the criticality of those patches. If patches cannot be applied for whatever reason, other compensatory control measures must be taken to mitigate the risk.

Systems running software, including the operating system, which are not being maintained adequately and which may be presenting a wider risk to University networks and data, are liable to have their connectivity restricted.

3.6. Software Removal

Software that cannot be made compliant (for example software for which security patches cannot be applied and any unlicensed or incorrectly licensed software) must be removed from service or the host device moved to an autonomous or isolated network. The IT Service Management process must be followed.

When decommissioning a University system, or a system managed on behalf of the University, licensed software must be removed to prevent any breach of licensing conditions.

3.7. Permitted, Regulated and Prohibited Use of Software

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. The Chief Digital and Information Officer has overall accountability for IT at the University and has the authority to prohibit use of software. This may include, but is not limited to software that poses a risk to confidentiality, integrity or availability of University data.

4. Further Guidance

Acceptable Use policy (ISP-09)

Outsourcing and Third Party Compliance Policy (ISP-04)

Compliance Policy (ISP-03)

IT Service Management Process

Title	Network Management Policy
Reference	ISP-13

Status	Approved
Version	4.0
Date Created	July 2013
Last Reviewed	September 2024
Next Review	September 2025
Classification	Public
PDF Policy Link	ISP-13 Software Management (PDF,144kB)