# University of Bristol
# Information Security Policy – Software Management

| | |
|---|---|
| **Title** | Software Management |
| **Reference** | ISP-13 |
| **Status** | Approved |
| **Version** | 1.2 |
| **Date** | July 2014 |
| **Review** | June 2021 |
| **Classification** | Public |

**Contents**

## 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 by IT staff and end users where necessary.

## 2. Scope

This policy applies to all University-owned systems, anyone responsible for installing and managing software on University systems, and anyone using software installed on a University system.

### 2.1. Definition

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

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

Computers - includes all University-owned devices that are able to be programmed to run logical operations or arithmetic. This includes but is not limited to tablets, smartphones, wearables, 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 themselves are responsible for that installation.

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.

Software managers are responsible for ensuring the ongoing security of their software and must apply security patches in a timely manner or with other compensatory control measures taken to mitigate risk and in accordance with prevailing University standards or framework compliances.

### 3.2. 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. These could include manual controls required during operation.

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

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 appropriate software license manager.

Automated installs should be used wherever possible - in line with current procedures.

Media and other files must be stored securely and managed.

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. Appropriate assessment or tests should be made to avoid new software causing operational problems to other systems on the network.

IT Services' Change Management processes must be followed and software catalogue maintained.

### 3.4. Software regulation

Use or installation of unlicensed software or using software for illegal activities constitutes a disciplinary offence.

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

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 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).

### 3.5. Software maintenance

All changes to computer systems are subject to IT Services' established change management processes and procedures.

Software must be actively maintained to ensure the ongoing security of the software and security patches must be applied in a timely manner, proportionate with the risk and impact, or with other compensatory control measures taken to mitigate risk.

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

### 3.6. 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 or compliance problem, which cannot be adequately mitigated, should be removed from service. IT Services' Change Management process must be followed.

When decommissioning a computer system for disposal or re-use, appropriate measures must be taken in relation to any software stored on it. Software must be removed, where not doing so could lead to breaking the terms of its licence.

### 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 Information Officer has responsibility for IT at the University and this may include the prohibition of particular software.

## 4. Further Guidance

Acceptable Use Policy (ISP-09):
http://www.bristol.ac.uk/media-library/sites/infosec/documents/ISP-09.pdf