University of South Wales
Prifysgol De Cymru

Software Policy

DOCUMENT CLASSIFICATION	PUBLIC / CYHOEDDUS
DOCUMENT REF	USW-ISMS-DOC-A12-7-EN
VERSION	1.0
DATED	17 MAY 2022
DOCUMENT AUTHOR	Rebecca Wilcox – Asset Management Lead. Ryan Tyler – Software Development and Deployment Manager
DOCUMENT OWNER	Susanne Smith – ITS Deputy Director
REVIEW BY DATE	17 MAY 2024

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
0.1	01 FEB 2022	Jon Phillips	Initial ISMS draft
0.2	30 MAR 2022	Rebecca Wilcox Ryan Tyler	ITS review draft
0.3	13 APR 2022	Jon Phillips	Final draft
1.0	17 May 2022	Ross Davies	ISSG Review

Approval

NAME	POSITION	APPROVER	DATE
ISSG	ISSG Chair	Paul Harrison	17 MAY 2022

Contents

1 Introduction

The University of South Wales uses many types of computer software to perform its teaching, learning and business operations. This software may be hosted on end-user devices, on-premises servers, or in the cloud. It is reliant upon the correct functioning and security of that software. It is imperative therefore that steps are taken to ensure that only approved software is used within the University and that no University data or service is put at risk.

1.1 Scope Statement

This policy sets out how software will be acquired, registered, installed and developed within the University of South Wales. For other elements of "software" lifecycle please refer to other relevant policies such as USW's Acceptable Use Policy and Technical Vulnerability Management Policy.

This control applies to all systems, people and processes that constitute the organization's information systems, including executive members, colleagues, students, suppliers and other third parties who have access to USW systems.

1.2 Roles & Responsibilities

IT Services Service Assurance Team: Responsible for the authoring and update of this policy. Own procedures regarding software procurement and license conformity.

IT Service Desk: responsible for enabling providing end-user guidance and first-line assistance to queries and issues in respect of their compliance to this policy and the use of software at the University.

End-users: It is the responsibility of every colleague, student, and any other person who accesses our software to comply with the provisions in the policy. End-users, including those with local administrative privileges, must not attempt to install and use software not compliant with this policy or terms of any given software licence.

2 Purchasing Software

All computer software to be used within the University must be purchased through or with the approval of the IT Services Service Assurance Team. This is necessary to ensure that:

- Licensing requirements are addressed
- The software works effectively with the standard University software images
- Use of the software can be supported by IT Services
- Best value for money is obtained in procurement
- A record is kept of installed software within the University
- The software is safely sourced and delivered to ensure the University's security posture is not jeopordised

- The software is in compliance with the UK Data Protection Act and other regulatory requirements concerned with the processing of personal data.

Under no circumstances should software be purchased independently by individuals, faculties or departments.

Software must only be procured where it is actively supported by a commercial vendor or open-source community. The release of security patches is a core component of an actively supported software package.

As part of the procurement process, software should be assessed from information compliance, security, commercial, support and deployment perspectives.

3 Software Registration

All software in use within the University must be correctly licensed and used in accordance with that licence. This is a legal requirement and compliance may be monitored by vendors and various industry bodies.

All installed software programs must be registered in the name of the University, not the individual user. Purchased software is a University asset and licenses will frequently be reused as the shape of the organisation changes.

Under no circumstances must software source files be copied (other than for authorised backups). Installation on non-University machines, such as by colleagues and students on their own devices, must only be performed where licensing allows and permitted by the University.

IT Services Service Assurance Team will maintain a register of all licensed software within the organization and licensed copies of installation media such as DVDs.

Asset management software will be used to keep track of all installed instances of software titles and regular audits will be carried out. Any user with unlicensed software installed will be asked to remove it; it is the responsibility of users to ensure that all the software on their computer equipment is licensed.

4 Software Installation

Commonly used University licensed software will typically be installed as part of the base platform deployment to devices and systems.

Software that subsets of colleagues and students ordinarily require will typically be made available via official USW-managed software portals.

Requests for the installation of software not available via the above provisions must be made to IT Services. They will arrange for installation by the appropriate technical team or supplier upon request and once any required licenses have been purchased.

Software will not be installed prior to a valid license being obtained.

Users must not install onto University devices any software that is licensed to them personally, whether or not it is free, shareware or commercial. This includes evaluation versions of software programs.

5 Removal of software

IT Services must be informed when a software program is no longer required. The software will then be removed from the device in question and where possible the license will be re-used elsewhere within the University.

Users must not attempt to remove licensed software or associated components from their devices without informing IT Services as this potentially represents a waste of a University asset. It could also introduce an unintentional security vulnerability, particularly if the software is not fully removed in a manner compatible with the University's IT processes.

Software that becomes unsupported by a vendor or an active open-source community must be removed from USW devices and systems.

6 In-House Software Development

In rare cases, the University may develop its own software for particular purposes where a commercial package is not available or does not fulfil the identified requirements. In such cases structured and secure development methods must be used to ensure that software is developed to current standards and is tested and implemented in a managed, professional way.

Where software systems are developed and deployed by departments outside of IT Services to support operational or business-critical functions and processes, applicable IT Services policies and processes must be followed. This includes, but not limited to:

- Creation and maintenance of service design documentation.
- Adherence to current USW development standards.
- The Technical Vulnerability Management Policy.
- Registration of details on the IT Services product database.

Alterations to in-house developed software such as changes to functionality or the user interface must be managed via the IT Services Change Management Process. Changes to production-operational in-house developed software must not be made without following the change management process.

7 Modifications to software packages

Modifications (beyond "configuration" activity) to Commercial Off The Shelf (COTS) software packages will not be made unless absolutely necessary. Any such modification will need

authorisation by either an approved service design or accepted change control submission to provide the necessary management oversight and control.

Where possible and commercially viable, changes should be made by the software vendor and supplied as standard updates so as not to cause difficulties with patching and vendor support.

8 Use of software in a cloud environment

For clarity, public cloud Software as a Service (SaaS) applications are, by definition, considered to be "software" and therefore the controls presented in this policy are applicable. This is the University's preferred route for software packages.

Any applicable cloud-specific licensing requirements must be identified prior to installing software within an Infrastructure as a Service / Platform as a Service (IaaS/PaaS) cloud environment. This is particularly relevant in circumstances where the cloud service provision is elastic i.e. the processing capacity increases and decreases with demand.

9 Software Regulation

The use of illegal software and using software for illegal activities is strictly not permitted.

Use of software which tests or attempts to break University system or network security is prohibited unless the IT Service Security Team has been notified and has given prior authorisation.

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 and deactivated if necessary.

Software found on University systems which incorporates malware of any type is liable to be automatically or manually removed or deactivated.

10 ISMS Conformance

10.1 Areas of ISO/IEC 27001:2013 addressed

The following areas of the ISO/IEC 27001:2013 standard are addressed by this document:

- A.5 Information security policies
    - A.5.1 Management direction for information security
        - A.5.1.1 Policies for information security
- A.12 Operations security
    - A.12.5 Control of operational software
        - A.12.5.1 Installation of software on operational systems

    - A.12.6 Technical vulnerability management
        - A.12.6.2 Restrictions on software installation
- A.14 System acquisition, development and maintenance
    - A.14.2 Security in development and support processes
        - A.14.2.4 Restrictions on changes to software packages

10.2 Related Policies and Regulations

The following policies and procedures are relevant to this document:

- *Acceptable Use Policy*
- *Change Management Process*
- *Mobile Device Policy*
- *Technical Vulnerability Management Policy*

10.3 Compliance

Whenever any system or device connected to the University network presents a perceived risk to University infrastructure, systems or data, IT Services reserve the right to isolate that system from the network to avoid potential compromise. Such systems will be reconnected only when it can be demonstrated that they are no longer a risk.

If software is procured in a manner that is not consistent with the current processes, then it will not be deployed until the correct checks are passed and authorisations are given.