University of South Wales
Prifysgol De Cymru

Information Security Policy

DOCUMENT CLASSIFICATION	[PUBLIC / CYHOEDDUS]
DOCUMENT REF	ISMS-DOC-05-4-EN
VERSION	3.2
DATED	31 January 2022
DOCUMENT AUTHOR	Ross Davies / Chief Technology Officer
DOCUMENT OWNER	Nath Czechowski / Chief Information Officer
REVIEW BY DATE	31 January 2024

Revision history

VERSION	ISSUE DATE	REVISION AUTHOR	SUMMARY OF CHANGES	NEXT REVIEW DATE
1.0	15/09/2015	Tony Evans	First Release	September 2016
2.0	30/08/2019	Nath Czechowski	Full Review	
3.0	04/01/2022	Ross Davies Jon Phillips	Review Period	
3.1	21/01/2022	Catherine Thomas	HR Review	
3.2	21/01/2022	Ross Davies	Implement required changes	January 2023

Approval

NAME	POSITION	APPROVER	DATE
ISSG	ISSG Chair	Paul Harrison	31/01/2022

Contents

Tables

1 Introduction

This document defines the information security policy of the University of South Wales.

Information Security covers the protection of all forms of information to ensure its Confidentiality, Integrity and Availability (CIA) as follows:

- Confidentiality - ensuring that information is only available to authorised users
- Integrity - ensuring that information is accurate and fit for purpose
- Availability - ensuring that information is available when and where it is needed

As a modern, forward-looking organisation, the University of South Wales recognises at senior levels the need to ensure that it operates smoothly and without interruption for the benefit of staff, students, partners, shareholders and other stakeholders.

In order to provide such a level of continuous operation, the University of South Wales has implemented an Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO/IEC 27001. This standard defines the requirements for an ISMS based on internationally recognised best practice.

The operation of the ISMS has many benefits, including:

- Protection of revenue streams
- Ensuring the supply of goods and services to colleagues , students and partners
- Compliance with legal and regulatory requirements
- Protecting the confidentiality, availability and integrity of information in all forms
- Increased cyber attack resilience and response to evolving security threats

The University wishes to support colleagues and students in using IT systems safely and securely, and recognises that the ability to protect systems and data is a fundamental enabler for the University's wider Digital Strategy. Promoting an effective security culture will therefore be beneficial to both the institution and the individuals within it. The policy recognises the concepts of academic and individual freedom and will aim to ensure that the University: employs appropriate, proportionate and pragmatic security measures; adopts a suitable methodology for guiding the approach to managing security; and complies with all legal and contractual requirements whilst enabling operational effectiveness.

This policy applies to all systems, assets, people and processes that constitute the organisation's information systems, including Executive Leadership, Governors, all staff who work at USW,, suppliers, students and other third parties who have access to the University of South Wales' systems.

The University of South Wales is committed to protecting information that is used for the purpose of teaching, learning, research and commercial/administrative activities. This policy applies to information in all forms, including but not limited to:

- Paper-based or stored electronically

- Text, pictures, video and audio
- Information transmitted by post, by electronic means and by oral communication, including telephone and voicemail

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

- 5 Leadership
  - 5.1 Leadership and commitment
  - 5.2 Policy
- A.5 Information security policies
  - A.5.1 Management direction for information security
    - A.5.1.1 Policies for information security

2 Information security policy

2.1 Information security requirements

A clear definition of the requirements for information security within the University of South Wales will be agreed and maintained with the institution, users and partners so that all ISMS activity is focused on the fulfilment of those requirements. Statutory, regulatory and contractual requirements will also be documented and input to the planning process. Specific requirements about the security of new or changed systems or services will be captured as part of the design stage of each project.

It is a fundamental principle of the University of South Wales' Information Security Management System that the controls implemented are driven by business needs and this will be regularly communicated to everyone who works at USW through team meetings and briefing documents.

2.2 Framework for setting objectives

A regular cycle will be used for the setting of objectives for information security, to coincide with the budget planning cycle. This will ensure that adequate funding is obtained for the improvement activities identified. These objectives will be based upon a clear understanding of the university's requirements, informed by the management review process during which the views of relevant interested parties may be obtained.

Information security objectives will be documented for an agreed time period, together with details of how they will be achieved. These will be evaluated and monitored as part of management reviews to ensure that they remain valid. If amendments are required, these will be managed through the change management process.

In accordance with ISO/IEC 27001 the reference controls detailed in Annex A of the standard will be adopted where appropriate by the University of South Wales. These will be reviewed on a regular basis in the light of the outcome from risk assessments and in line with information security risk treatment plans. For details of which Annex A controls have been implemented and which have been excluded, please see the Statement of Applicability.

In addition, enhanced and additional controls from the following codes of practice will be adopted and implemented where appropriate:

- ISO/IEC 27002 – Code of practice for information security controls
- ISO/IEC 27017 – Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27035 – Information Security Incident Management

The adoption of these codes of practice will provide additional assurance to our customers and help further with our compliance with international data protection legislation.

2.3 Continual improvement of the ISMS

The University of South Wales' policy regarding continual improvement is to:

- Continually improve the effectiveness of the ISMS
- Enhance current processes to bring them into line with good practice as defined within ISO/IEC 27001 and related standards
- Achieve ISO/IEC 27001 certification and maintain it on an on-going basis
- Increase the level of proactivity (and the stakeholder perception of proactivity) with regard to information security
- Make information security processes and controls more measurable in order to provide a sound basis for informed decisions
- Review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data
- Obtain ideas for improvement via regular meetings and other forms of communication with interested parties
- Review ideas for improvement at regular management meetings in order to prioritise and assess timescales and benefits

Ideas for improvements may be obtained from any source including students, colleagues, partners, suppliers, IT team members, risk assessments and service reports. Once identified they will be recorded and evaluated as part of management reviews.

2.4 Information security policy areas

The University of South Wales defines policy in a wide variety of information security-related areas which are described in detail in a comprehensive set of policy documentation that accompanies this overarching information security policy.

Each of these policies is defined and agreed by one or more people with competence in the relevant area and, once formally approved, is communicated to an appropriate audience, both within and external to, the organisation.

The table below shows the individual policies within the documentation set and summarises each policy's content and the target audience of interested parties.

POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
Mobile Device Policy	Care and security of mobile devices such as laptops, tablets and smartphones, whether provided by the organisation or the individual for business use.	Users of company-provided and BYOD (Bring Your Own Device) mobile devices
Teleworking Policy	Information security considerations in establishing and running a teleworking site and arrangement e.g. physical security, insurance and equipment	Management and colleagues involved in setting up and maintaining a teleworking site
Access Control Policy	User registration and deregistration, provision of access rights, external access, access reviews, password policy, user responsibilities and system and application access control.	All users
Anti-Malware Policy	Firewalls, anti-virus, spam filtering, software installation and scanning, vulnerability management, user awareness training, threat monitoring and alerts, technical reviews and malware incident management.	Colleagues responsible for protecting the organisation's infrastructure from malware
Logging and Monitoring Policy	Settings for event collection. protection and review	Colleagues responsible for protecting the organisation's infrastructure from attacks
Software Policy	Purchasing software, software registration, installation and removal, in-house software development and use of software in the cloud.	All colleagues
Technical Vulnerability Management Policy	Vulnerability definition, sources of information, patches and updates, vulnerability assessment, hardening and awareness training.	Colleagues responsible for protecting the organization's infrastructure from malware and local administrators
Network Security Policy	Network security design, including network segregation, perimeter security, wireless networks and remote access; network security management, including roles and responsibilities, logging and monitoring and changes.	Colleagues responsible for designing, implementing and managing networks
IP and Copyright Compliance Policy	Protection of intellectual property, the law, penalties and software license compliance.	All colleagues and students
Records Retention and Protection Policy	Retention period for specific record types, use of cryptography, media selection, record retrieval, destruction and review.	All colleagues
Privacy and Personal Data Protection Policy	Applicable data protection legislation, definitions and requirements.	All colleagues
Clear Desk and Clear Screen Policy	Security of information shown on screens, printed out and held on removable media.	All colleagues
Social Media Policy	Guidelines for how social media should be used when representing the organisation and when discussing issues relevant to the organisation.	All users
Information Management Policy	Applying a classification degree of sensitivity and criticality to the information created, collected, and disseminated within the University and placing	All colleagues

POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
	controls relating to the type of information and its need to remain confidential and secure.	

Table 1: Set of policy documents

2.5 Application of information security policy

The policy statements made in this document and in the set of supporting policies listed in Table 1 have been reviewed and approved by the Executive and/or the Information Security Steering Group (as appropriate) of the University of South Wales, and must be complied with. Failure by a colleague to comply with these policies may result in disciplinary action.

Questions regarding any University of South Wales policy should be addressed in the first instance to the colleague's line manager.