University of South Wales
Prifysgol De Cymru

University of South Wales: Information Security Policy

Introduction

Information is the lifeblood of a successful organisation. Without it they cannot operate. Equally, if it is untrustworthy, every activity is suspect, and reliable decisions are difficult to make. Information must therefore be readily available in a trustworthy manner to those that need it.

This information security policy defines the framework within which information security will be managed across the University of South Wales and sets out management direction and support for information security throughout the University of South Wales. This policy is the primary policy under which all other Information compliance, and Information Security Management Systems reside.

Although Information Security is often considered to be the realm of the IT Services department, everyone has a role to play.

This Policy and the associated Information Security Management System[1](ISMS) are grounded on the three principles of Confidentiality, Availability and Integrity of information.

Together they set out how the University will protect itself and its participants from any actual or perceived threat, thereby adding an acceptable degree of confidence to those with a vested interest in the institution.

Within the overall framework more specific Information Security policies and procedures are defined and maintained, including those based on ISO/IEC 27001:2013 (information technology – Security techniques – information security management systems – requirements). These include those that safeguard the physical and environmental security of the University's ICT assets, enable business continuity, and ensure compliance with legal requirements. Access to some of these documents are restricted due to the nature of their information and the potential risk of security from getting in the wrong hands.

Governance of information security

Overall responsibility for Information Security lies with the Vice-Chancellor's Executive Board (VCEB) and its sub-group for ICT (VCEB ICT). These groups receive regular reports from the Director of IT Services and the University Secretary's Office on information security matters together with proposals for improving the University's security controls. The objective of VCEB in this respect is to ensure that there is clear direction and visible management support for security initiatives and to promote security through appropriate commitment and adequate resourcing.

The University Secretary's Office is responsible for ensuring that the University complies with legislation relating to the use of information, and for promoting good practice in the management of

[1] ISO/IEC 27001 international standard describing the creation and maintenance of information security management system (ISMS).

information. Further supporting policies and procedures relating to this office can be found here http://uso.southwales.ac.uk/ig/.

The Information Governance Team, part of the University Secretary's office, has responsibility for ensuring compliance with data protection legislation within the University. These staff ensure that the appropriate policies and procedures are in place, provide training, guidance and advise University employees on matters relating to data protection.

Within IT Services, an ICT Security Management Group has the responsibility to respond and review security incidents as well as to develop the University's security controls, both in terms of defence mechanisms and of the policies and procedures within the ISMS. Links to these documents can be found here http://its.southwales.ac.uk/it-regulations/.

It is the responsibility of all line managers to implement this policy within their area of responsibility and to ensure that all staff for which they are responsible are:

1) made fully aware of the policy;
2) given appropriate support and resources to comply.

It is the responsibility of each member of staff to adhere to this policy.

The IT Services Information Security Management Group (ISMG) will report all information or IT security incidents, or other suspected breaches of this policy. They will follow the procedures for the escalation and reporting of security incidents. Any data breaches that involve personal data will subsequently be reported to the University's Data Protection Officer.

Policy Statement

The University of South Wales is committed to protecting the security and integrity of its information and information systems. It is also committed to a policy of education, training and awareness for information security and to ensuring the continued business of the university.

It is the University of South Wales's policy that the information it manages shall be appropriately secured to protect against breaches of confidentiality, failures of integrity or interruptions to the availability of that information and to ensure appropriate legal, regulatory and contractual compliance.

To determine the appropriate level of security control that should be applied to information systems, a process of risk assessment shall be carried out in order to define security requirements and identify the probability and impact of security breaches.

Specialist advice on information security shall be made available and advice can be sought via the University Secretary's Office and the IT Services Information Security Management Group (ISMG).

Failure to comply with this policy through deliberate, malicious or negligent behaviour, may result in disciplinary action.

Policy Objectives

The objectives of this policy are:

1. To protect University and personal information, in whatever form, from unauthorised access by malicious or accidental means;
2. To ensure that the confidentiality of the University's information can be assured;
3. To ensure consistency and continuity of service and availability of information to users;
4. To maintain the integrity of all University data;
5. To meet all the University's contractual, legislative, privacy and ethical requirements with regard to the security of information.

The University is prepared to use all reasonable, appropriate, practical and effective measures to ensure that these objectives will continue to be met.

Controls

Through the governance process, and guided by the UCISA[2] Information Security Toolkit, a set of ICT security related policies and procedures are maintained to provide the necessary controls to protect the University's information assets.

To determine the appropriate levels of security measures applied to information systems, a process of risk assessment is carried out for each system to identify the probability and impact of security failures.

The University will exercise its right under applicable law to intercept and monitor electronic communications, covering but not limited to the monitoring of criminal or unauthorised use.

Communication

Both the IT Services department and the Information Governance team offer specialist advice on information security to all students and staff, and have a responsibility to establish and maintain appropriate contacts with other organisations, law enforcement authorities, regulatory bodies, and network and telecommunications operators in respect of the University's information security policy.

Through their relevant groups they regularly review the policies and procedures for the University and submit revisions and additions to the VCEB group for approval and subsequent implementation.

All new and amended policies will be published on the appropriate system(s), either the University's web site, the student portal and/or the staff portal. A news item announcing the release will also be posted to the appropriate portal.

[2] UCISA – Universities and Colleges Information Systems Association, www.ucisa.ac.uk

Your Responsibilities

These responsibilities apply to all staff and students of the University and all other authorised users.

1. Your principal responsibility is to maintain an awareness of existing policies/regulations and to comply with their requirements.
2. If you handle personal, confidential or sensitive information, you must take all reasonable steps to safeguard it and you must observe the University's Data Protection Policy and all Information Security policies and guidance available, particularly with regard to removable media, mobile and privately owned devices, and paper records.
3. Members of staff developing new systems or using systems outside of the control of the University must seek advice to ensure that the appropriate safeguards are in place to ensure the security of that information.
4. You will have been provided with a University username and password, it is a breach of the IT Computing Regulations to share these with anyone else. Care must also be taken to ensure your username and password are not accidentally shared or disclosed with anyone else, such as when using computers in public places and responding to unsolicited email.
5. You must not infringe copyright, or break the terms of licences for software or other material.
6. You must not attempt to access, delete, modify or disclose information belonging to other people without their permission, or explicit approval from the Director of IT Services or their deputy.
7. You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening or discriminatory.
8. You must abide by the University's Social Media policy when using the IT facilities to publish information.
9. You must at all times comply with applicable law.
10. If you become aware that there has been or is likely to be a breach of information security that you suspect has hitherto been unreported, you should report it to your Head of Faculty/Department.

Title: Information Security Policy					
Version	**Issue Date**	**Revision Description**	**Author**	**Approved By & Date**	**Next Review Date**
0.1	26/2/15	First draft	Tony Evans		
0.2	3/8/15	First revision	Alan Davies		
0.3	15/9/15	Second revision for VCEB ICT feedback.	Tony Evans	Approved by VCEB ICT 04/09/15	04/09/16