Prifysgol Cymru
University of Wales

# Information Security Policy

Document Status Details

| | |
|---|---|
| Status | Approved |
| Version History | 3 |
| Classification | Unclassified |
| Date | 11 September 2013 |
| Author | Information Services/ Compliance |
| Implementation date | July 2002 |
| Review date | 11 September 2017 |

**1. Introduction.**

This policy sets out the approach adopted to develop, manage and improve Information Security to ensure that information assets are properly protected against loss or compromise.

Within the context of Information Security, 'information' includes data and any form of communication recorded or transmitted in transcript or verbally, manually or electronically. In terms of tangible assets, Information Security principles extend to paper documents, computer files, electronic records, CDs, disks, drives or any other storage or processing medium.

**2 Aim.**

Information Security is different to 'Information Management' which embraces a much broader set of administrative procedures necessary to manage the entire life of information from origin, through processing, to disposal. However, Information Security is an integral component of Information Management and for this to be effective, a consistent, well organised and properly administered structure must be established in all working environments throughout the organisation.

Every aspect of business will involve Information Security considerations, therefore it remains the responsibility of all people who work for or in support of the University of Wales to safeguard organisational assets and ensure that all necessary protective measures are in place.

In applying this policy it is also important that the breadth of protective security principles relating to information, IT, personnel and physical security are fully integrated to create sufficient depth and resilience to complement business continuity requirements and guard against all prevailing threats.

Finally, Information Security must take full account of a range of legislation governing the manner in which information and data is managed and protected. A common theme is 'confidentiality' and, to remain legally compliant, obligations are placed upon staff to ensure that information is protected.

**3 General Principles.**

The intention is to describe Information Security requirements and demonstrate the need for activity necessary to safeguard information, counter threats and comply with legislation.

Central to this approach is an understanding that the organisation cannot function without information, processes and networks that combine to create a complicated infrastructure. From this it is important to identify the more sensitive data, operational, financial or business assets that require specific protection and to develop measures to prevent, detect and mitigate loss or compromise.

To balance business needs with information security requirements a proportionate response is necessary and this is achieved by adopting measures that preserve:

- Confidentiality – ensuring that information is accessible only to those authorised to have access, and protecting assets against unauthorised disclosure.

- Integrity – safeguarding the accuracy and completeness of information and processing methods, and protecting assets from unauthorised or accidental modification.

- Availability – ensuring that authorised users have access to information and associated assets when required to pursue the University of Wales strategic objectives.

Another significant aim is to reinforce 'confidentiality' and 'need to know' principles. Information supplied in confidence, developed to support the operational and strategic initiatives or connected with other sensitive business activities, must be treated in a confidential manner and only imparted to others in the official course of business on a strict 'need to know' basis. This requirement is supported by legislation including:

- Data Protection Act 1998 - requires personal data to be properly safeguarded and not disclosed unless properly authorised and justified.

- Computer Misuse Act 1990 – renders it illegal to gain access to or use a computer without authority.

- Freedom of Information Act 2000 - provides for disclosure of non-personal data, subject to exemptions.

While the intention of this policy is to identify a range of protective security measures, considerably more detail is necessary to provide practitioners with clear procedural requirements and guidance. Such detail will be contained in a series of 'Information Security Policies and Procedures' that will be approved by the Nominations and Governance Committee. These will be published on the intranet and when appropriate on the internet, within the University's Publication Scheme.

Threats and Vulnerabilities - In adopting relevant protective measures, the nature of threats and vulnerabilities must be considered.

a) Some of the work of the University is of interest to others and, while the organisation must operate as a public service, it is important to protect sensitive assets and guard against infiltration by undesirable elements including terrorists, criminals, those who attack computers and, in some cases, the media.

b) As well as external vulnerabilities, the organisation must counter unauthorised or illegal internal activity including corruption or any other deliberate or accidental act or omission which could lead to loss or compromise of information.

**4. Challenges & Representations.**

Challenges and representations concerning this policy should be directed to the, Compliance and Secretariat Manager.

**5 Guidance and Procedures.**

**5.1 Confidentiality.**

Information available to staff and others who work in support of the University of Wales, is provided for official use only. Personal use or communication to unauthorised persons is not permitted.

**5.2 Need to Know.**

Knowledge and possession of sensitive information must be limited to those who have a genuine 'need to know' basis.

**5.3 Classification.**

Classification provides a consistent standard for marking sensitive assets. The classifications commence with **UNCLASSIFIED** and progress through **CONFIDENTIAL** and **HIGHLY CONFIDENTIAL**. It is the responsibility of the originator to classify the asset and control initial circulation which should be limited to those who 'need to know'. Thereafter, any processing or handling of a marked asset must follow approved procedures which include secure storage and disposal methods. Please refer to the Classification Procedure.

**5.4 Data Protection.**

Particular care must be taken to protect personal data and to apply the Data Protection Act principles to ensure that collection, use, retention, disclosure and disposal follow legal requirements. Please refer to the Information Protection Policy and relevant Data Protection Procedures.

**5.5 Clear Desk Practice.**

Sensitive assets including those marked with a classification must be managed in a way that prevents unauthorised access. This includes securing assets in appropriate cabinets when not in use, particularly outside normal working hours.

**5.6 Clear Screen Practice.**

Password protected screen savers must be activated when the user is away from their computer terminal to prevent unauthorised access to information or systems. In addition, the screen on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons.

**5.7 Provision of Equipment and Peripherals.**

The University provides the necessary equipment and other peripherals for use of University business only. The storage of music, personal photos and documents on such equipment is prohibited. Although equipment is normally allocated to a single member of staff, any authorised member may have access to any given item.

It is the responsibility of the individual when equipment has been allocated to ensure its safe keeping and to prevent such items being exposed to loss or theft.

The installation of any unauthorised hardware on computers or the University network is prohibited.

Email and Internet shall be used in accordance with the University's "Email and Internet Usage and Monitoring Policy's" specifically for each of these activities. Users of the University's Internet access are also bound by the JANET (The JNT Association Ltd) Acceptable Use Policy.

**5.8 System Planning, Access and Passwords**

When a new or significantly enhanced information system is planned, security, compliance, recovery and redundancy aspects shall be considered and implemented as part of the system design, system administrators and specification. For further advice and guidance please contact compliance@wales.ac.uk.

Staff, agency, contractors and consultants ("**Approved Users**") working in support of the University of Wales are only permitted access to computers and systems for which they have been specifically authorised to conduct University business.

Private use is only permitted with the authority of the line manager, with limited or restricted occasional use being permitted. It is therefore the line manager's responsibility, if permitting staff to use University equipment, to monitor on a regular basis the usage of such equipment. Please refer to the Email Usage and Monitoring and the Internet Usage and Monitoring Policies.

Access permissions include the use of personal staff secure log on details, combined with a unique password known only to the user. Passwords must not be divulged to others, nor written down, to do so could result in disciplinary action being taken. In addition, the password configuration will not permit obvious names or dates that could easily be associated with the user, and will enforce a combination of 8 or more, alpha, numeric, upper and lower case characters. Approved users will be prompted every 90 days to change their passwords, old passwords cannot be recycled to try and do so, the system will issue a warning message.

**5.9 Departmental Drives and Local Drives.**

All University departments have designated drives that have been created for the storage and back-up of work related material. Under no circumstances should work related data be stored on the local drive (known as the C drive) or the individual's H drive.

**5.10 Investigation and Audit**

From time to time, individuals within the University or the University itself may be suspected of or be in breach of internal or external policies, regulations or legislation. Depending on the nature or seriousness of the alleged breach, an appropriate level of investigation and reporting shall be carried out.

At an individual level, investigations requiring (privileged or covert) access to personal data and system logs on University systems regarding that individual will only be carried out with the express written permission of the Vice Chancellor, Deputy Vice Chancellor or the Finance and Resources Manager. Circumstances when this might apply include:

- investigating allegations of inappropriate use of Internet material, copyright infringement, identity fraud or inappropriate, offensive or defamatory communications.

Such investigations may give rise to further proceedings against individuals under the University's Disciplinary Procedure and related policies, up to and including dismissal.

At the University level or for more serious individual situations, the University shall co-operate fully and openly with the relevant regulatory or law enforcement agencies to assist with the investigation of allegations.

To ensure compliance with internal and external policies, regulations and legislation, information systems and technology shall be subject to periodic professional internal and external audit and review. The University will again co-operate fully and openly with such audits and shall receive and act upon agreed findings and recommendations arising, subject to business prioritisation and direction as may apply.

Regular audit programmes will be conducted by the Network and Systems Manager either remotely or within the Registry building. Audit reports will be made available to the Finance and Resource Manager, Compliance and Secretariat Manager and any necessary Manager of the University.

**5.11 Corporate Software**

The downloading of unauthorised software onto any University of Wales systems, whether part of the network or a standalone facility is prohibited without the prior permission of the Network and Systems Manager. This includes, but is not an exhaustive list, any executable program, screen saver or macro program. In addition approved software loaded onto the University systems must not be downloaded or copied.

Corporate software is provided for approved users for the use in accomplishing their duties and conducting University business only.

**5.12 Mobile Computing**

Mobile computing devices such as Personal Digital Organisers (PDAs), portable memory devices, laptop computers and Blackberry/mobile telephones that belong to the University of Wales, or contain the University data, must be properly secured at all times. Access control (e.g. PIN) must be activated and particular care taken to safeguard equipment when travelling or in a public place. Unless equipment includes specific security measures, such as encryption, then classification of data contained on these devices must not exceed **UNCLASSIFIED.**

If such mobile devices are being used to process data, it is critical to the operation of the University that data is not stored on the hard drive (C drive).

Approved users of the University traveling to India, China, Singapore and Malaya must ensure that the necessary permits have been obtained prior to departure to enable entry into that country with an encrypted device; or to make the necessary arrangements within their department to use a "clean" laptop, (no classified data and un-encrypted data has been stored on this device).

**5.13 Removal of Assets from University Premises**

Authority is required from line managers for any asset to be removed from University premises. For assets classified **CONFIDENTIAL** or higher, specific authorisation is required together with arrangements to ensure that material is properly secured and safeguarded.

**5.14 Oversight, Eavesdropping and Social Engineering**

When discussing or processing issues of a sensitive nature on University premises or in public, extra care must be taken to avoid oversight of mobile computing devices, or eavesdropping.

***Social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures.***

Care must be taken when confirming details with individuals over the phone to ensure that the necessary validation checks have been conduct to prevent any social engineering. In some instances the smallest piece of personal information can be used to give an air of credibility to individuals (e.g. a date of birth, details of school attended, workplace) and the increasing popularity of Facebook and the naivety of many users when publishing personal information about themselves, has been a source of information for fraudsters looking for information to gain them a 'foot in the door'.

**5.15 'Cloud', hosted or Shared Service Systems**

The use of such services are discouraged, however if the need arises the same principles apply throughout to the data or information that may be placed or reside in systems external to the University, such as explicitly externally hosted, 'co-located' or shared service systems; or in distributed, effectively location-less, 'cloud' systems and services, including web-based systems such as Drop Box.

It remains the responsibility of the approved user to ensure that safeguards are in place to protect data in accordance with this policy and the Information Protection Policy. Contractual terms with the service provider should be used to ensure data confidentiality, security and integrity. For advice and guidance please contact compliance@wales.ac.uk .

**5.16 Disposal**

Information assets of a sensitive nature, and particularly those containing a classification, must be destroyed using approved methods. UNCLASSFIFIED and CONFIDENTIAL material can be placed in confidential waste bins, whereas HIGHLY CONFIDENTIAL material must be shredded. Please refer to the Disposal Procedure which can be found on the Intranet.

**5.17 Breaches of Information Security**

The monitoring of Internet and email use will be conducted as a matter of routine by the Information Services Department, and if any unauthorised use is identified the appropriate line manager will be informed.

Any security incident or occurrence that has the potential to compromise the organisation, staff, departmental information or other assets, must be reported to the Compliance and Secretariat Manager for assessment and decision regarding further action. This can be done by using the Security Incident Form, shown in Appendix 1.

If an approved user believes that there has been a security breach which may have compromised personal data, the Compliance and Secretariat Manager must be notified immediately, or no later than 72 hours of that breach being identified.

**5.18 Awareness and Disciplinary Procedures**

A copy of the Information Security Policy will be given to all new members of staff as part of the University's Induction process, and is available on the University's intranet. Existing staff and agency workers of the University, authorised third parties and contractors given access to the University network will be advised of the

existence of this policy and the availability of the associated policies and guidelines on the University intranet. Reminders of the existence and nature of the policy will be issued at least annually by the Information Services Department. The failure of a member of staff to comply with this policy may lead to the instigation of the relevant disciplinary procedures and, in certain circumstances, legal action may be taken. Failure of a contractor to comply could lead to the cancellation of a contract.

**6. Compliance**

This Information Security Policy sets out the responsibilities of all approved users, including those based at collaborative partner institutions, in relation to their use of the University information systems and data. Any individual who access the University systems and / or data agrees, in doing so, to comply with the Information Security Policy, and where appropriate their compliance maybe monitored.

All activities of the University must be conducted in accordance with current legislation. Line managers are responsible for ensuring that any approved users whose duties require it receives specific guidance on legal compliance. If any approved user is unsure as to their responsibilities in relation to the law, they should seek advice from their line manager.

The use of information is governed by a number of different Acts of Parliament, together with various statutory and other pieces of legislation. These currently include, but are not limited to:

Copyright, Design And Patents Act 1988
Data Protection Act 1998
Human Rights Act 1998
Computer Misuse Act 1990
Regulation of Investigatory Powers Act 2000
Freedom of Information Act 2000
Electronic Communications Act 2000
Digital Economy Act 2010
Defamation Act 1996

Before any new system is introduced, a risk assessment process will be carried which will include an assessment of the legal obligations that may arise from the use of the system. These legal obligations will be documented and have a named service manager, with responsibility for updating that information.

The acceptable use policies specify any uses of the University information systems that are prohibited and in relation to which disciplinary action may be taken.

Information will be retained for appropriate periods of time that are consistent with the business needs and relevant legislation and the (Joint information Systems Committee (JISC) Retention Schedule. During retention periods appropriate technical systems will be maintained to ensure that data can be accessed.

The University will only process personal data in accordance with the requirements of data protection legislation. Personal or confidential information will only be disclosed or shared where a member of staff has been authorised to do so.

The University reserves the right to access data within information systems where this is necessary for management purposes. In cases where investigation of traffic or content of users' accounts is necessary, Information Services technical staff will carry out such work under the direct instruction from the Vice-Chancellor following authorisation from the Head of Finance and Resources. The University will involve the police in all cases where it believes that illegal activity may have taken place.

All of the University's information systems will be operated and administered in accordance with relevant procedures, and the University may at any time monitor compliance with written authorisation from the Vice-Chancellor.

**7. Discrimination**

The University's policies are not to discriminate against any persons on the ground of age, disability, gender reassignment, marriage and civil partnership, race, religion or belief, sex and sexual orientation.

**8. Compliance with the Welsh Language Scheme**

This Policy aims to comply with the organisation's Welsh Language Scheme in terms of dealing with the Welsh speaking public, impact upon the public image of the organisation and the implementation of the Language Scheme.

**9. Implementation Timescales**

New policies and procedures should be applied immediately following formal adoption and communicated to all members of staff.

**10. Guidance**

Queries of requests for guidance on any aspect of this policy can be obtained from the University's Compliance and Secretariat Manager: compliance@wales.ac.uk

**Appendix 1 University of Wales Information Security Incident Form**

| | |
|---|---|
| **To** | **Secretariat and Compliance Manager, The Registry, Cathays Park Cardiff** |
| **From / Title** | |
| **Location** | |
| **Email address** | |
| **Telephone/Mobile** | |
| **Asset Number, if known** | |
| **Date and time of incident (if known)** | |
| **Loss of Physical Asset (accidental or theft)** | |
| **Has any physical asset been lost?. Give details including circumstances. Value, if known** | |
| **Have the Police been informed? If so which force and what is the crime number?** | |
| **Data compromised (lost and / or breach of confidentiality )** | |
| **Has any data been lost, disclosed or maliciously corrupted? Where was it stored? What were the circumstances of the loss?** | |
| **Is identity theft, impersonation or compromise involved?** | |
| **Has any breach of the confidentiality taken place? How has it occurred?** | |
| **Describe the nature of any data loss or compromise?** | |
| **System attack – virus alert or other instance of malicious activity** | |
| **Has a virus alert or other attack been noted? Was there a message? Did you see the virus name?** | |
| **Other information** | |
| **Record any other incident or information regarding the University's information system security having been compromised.** | |

**Signed**_____ **Date**_____