Date	Version	Author	Comments
05/2004	F01	Bridget Kenyon	Original, ratified Information Security Policy 2004
09/2008	D01	Duncan Woodhouse	Adaption and consolidation of best practices and policies
11/2008	D02	Duncan Woodhouse	Review and comments by Senior Assistant Registrar
01/2009	D03	Duncan Woodhouse	Review and comments by Deputy Registrar
06/2009	D04	Duncan Woodhouse	Review and comments by Director of IT Services subject to presentation to the Information Policy and Strategy Committee
06/2009	F01	Duncan Woodhouse	Ratified by Steering Committee
11/2009	D01	Duncan Woodhouse	Updates from the University Human Resource department and further consultation for 2010
01/2010	D02	Duncan Woodhouse	Additional wording in section 4.2 after review by IPSC in January 2010
02/2010	D03	Duncan Woodhouse	Further review by IPSC, academic departments and the Deputy Registrar
08/2012	D04	Joy Findlay	Changed author and added reference to Privacy and Electronic Communications (EC Directive) Regulations

University of Warwick Information Security Policy

1. Introduction

The University of Warwick holds a great deal of important information that is crucial to the running of the organisation. While many information systems can be recovered after an incident the business critical data that resides in electronic and paper form must be suitably protected. This involves considerations into the confidentiality, integrity and availability (CIA) of business critical and potentially sensitive data.

Information security is important to the protection of the University's reputation and the success of the academic and operational activities. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.

This document seeks to define Information Security as a top level, strategic objective that can be developed into more specific procedures.

The Policy is designed to the ISO 27001 standard and updated from BS 7799. This policy shall be reviewed regularly and updated as necessary to ensure that it remains appropriate in the light of any changes to legal, contractual or acceptable use obligations.

2. Objectives

The objective of the Information Security Policy is to provide a framework for University Members to work towards ensuring that all information and information systems upon which the University depends are adequately protected to the appropriate level.

3. Scope

The Information Security Policy applies to information in all its forms. It may be on paper, stored electronically or held on film, microfiche or other media. It includes text, pictures, audio and video. It covers information transmitted by post and by electronic means, including telephone and voicemail. It applies throughout the lifecycle of the information from creation through storage and utilisation to disposal.

The policy applies to all staff and students of the University and to other users associated with the University[1]. With regard to electronic systems, it applies to use of University owned facilities and privately/externally owned[2] systems when connected to the University network directly or indirectly.

The policy applies to all University owned/licensed data and software, be they loaded on University or privately/externally owned systems, and to all data and software provided to the University by sponsors or external agencies.

[1] 'Other users or persons' includes any individuals that need access to University systems (e.g. associates, third parties, conference guests).
[2] 'Owned' is deemed to include leased, rented or on-loan.

4. Policy Statement

The University is committed to protecting the security of information through the preservation of:

Confidentiality: protecting information from unauthorised access and disclosure.

Integrity: safeguarding the accuracy and completeness of information and processing methods.

Availability: ensuring that information and associated services are available to authorised users when required.

The University will develop, implement and maintain policies and procedures to achieve appropriate levels of information security. These will cover the range of elements that need to be addressed in the management of information security, in particular the following policy requirements:

4.1 Authorised Use

University information systems are provided to support the University's activities including learning, teaching, research, administration and approved business activities. Only staff, students and other persons authorised by an appropriate University authority[3] are entitled to use the University's information systems.

4.2 Acceptable Use

In line with our legal obligations and JANET's acceptable use of its resources:

All users have an obligation to use information and information systems responsibly.

In particular members are reminded to use University IT facilities[4]as a business resource. In short this means using these resources in a way that is appropriate for the role you are undertaking. Please consider the impact of your behaviour on your department and the University's reputation as a whole.

In particular the following is considered unacceptable behaviour:

Viewing, creating, transmitting or storing offensive, obscene, indecent or defamatory images, data or other material.

Creating or transmitting material with the intent to cause annoyance or inconvenience to others.

Create, download or transmit material that infringes on the copyright of another person or organisation.

The University recognises the above list is not exhaustive. As such the University retains the right to

[3] The University authority is deemed to be an appropriate department contact who will take responsibility for authorising the individual concerned. This in turn will allow the individual to have access to University systems.
[4] This could be (but not limited to) a managed desktop, Microsoft Outlook email account or use of shared network storage.

determine what is 'unacceptable' on a case-by-case basis in the event that individuals are investigated under disciplinary regulations.

If individuals are unsure whether their activities constitute acceptable behaviour they should consult with Human Resources or the Deputy Registrar's Office. If this is related to academic activity, or any other matter, written consent must be obtained from the Registrar or his/her nominee. This is set out in "Regulations governing the use of University Computing Facilities" section 3 (j).

4.3 Monitoring and Privacy

The University respects the privacy of its users and there is no routine monitoring of e-mail content or individual Web access. However, the University reserves the right to make interceptions in certain circumstances; examples are provided in the Appendix.

4.4 Protection of Software

All users must comply with the Copyright, Designs and Patents Act 1988 under which it is an offence to copy software or licensed products without the permission of the owner of the copyright.

Warwick University holds a number of copyright licenses, details of which are available at:

http://www2.warwick.ac.uk/services/gov/legalservices/whentouse/copyright

4.5 Use and disposal of Information

All staff have a responsibility to consider security when using and disposing of electronic and paper information in the course of their work.

Users will need to be familiar with the guidelines set out in the Data Retention Policy[5], particularly to ensure data is not kept for longer than is necessary.

Where users are handling data in relation to CCTV systems they must be familiar with the University of Warwick CCTV Code of Practice and Operational Procedures Manual 2009.[6]

For confidential paper information, members should cross shred onsite and additionally put into the confidential waste stream.

For confidential, electronic information:

- DVDs/CDs should be shredded and then put into the recycling stream.
- Computer hard drives and external storage media (such as USB sticks) should be wiped with a suitable software tool. No unencrypted data should be left on these types of media before re-using/recycling/disposal.
- Media that cannot be wiped initially will need to be sufficiently protected before being overwritten e.g. storage tapes in a locked safe.

[5] Available on http://www2.warwick.ac.uk/services/gov/informationsecurity/policies/.
[6] This was developed and is distributed by the Head of Security Services. Available on http://www2.warwick.ac.uk/services/gov/informationsecurity/policies/.

The University will determine retention periods[7] for certain kinds of information and departments should establish procedures appropriate to the information held and processed by them, and ensure that all staff are aware of those procedures.

4.6 Virus Control[8]

University members will take reasonable steps to ensure their machines are virus protected.

It is an offence under the Computer Misuse Act 1990 to knowingly introduce a virus or take deliberate action to circumvent precautions taken to prevent the introduction of a virus.

For staff and student members, ITS can provide advice on anti-virus licensing and use. Currently the University has a site license for Kaspersky anti-virus which can be used for any University owned machines.

Some departments manage their own computers and responsibility for virus protection on these computers lies with the Department. This includes installing antivirus products, keeping them up to date, giving advice on their use, removing any viruses found and applying any updates necessary to defend against possible threats. The Head of Department must ensure that these responsibilities are allocated to an appropriate member of staff. Assistance on this area can be obtained from the Deputy Registrar's Office and IT Services.

For student members of the University care must be taken when using the Campus LAN and RESNET[9] facilities.

For further details on acceptable use on the RESNET facilities please refer to:

http://www2.warwick.ac.uk/services/its/servicessupport/resnet/rules/aup/

4.7 Password protection[10]

University members should take reasonable precautions to protect their Warwick passwords and create strong passwords where necessary. Advice on password creation and best practice is available in the Appendix.

4.8 Business Continuity

The University will implement, and regularly update, a business continuity management process to counteract interruptions to normal University activity and to protect critical processes from the effects of failures or damage to vital services or facilities.

5. Legal and Contractual Requirements

[7] Please see the Data Retention Policy.
[8] This section incorporates the Anti-virus Policy 2002.
[9] RESNET has a specific Acceptable Use Policy which is strictly enforced to adhere to JANET's Acceptable Use Policy.
[10] This section incorporates the Password Policy ratified 28/06/2006.

The University will abide by all UK legislation and relevant legislation of the European Community related to the holding and processing of information. This includes the following Acts and mandatory requirements:

- Copyright Designs and Patents Act 1988
- Computer Misuse Act 1990
- Data Protection Act 1998
- Human Rights Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Payment Card Industry Data Security Standards 2007
- Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (previously Privacy and Electronic Communications (EC Directive) Regulations 2003)

The University will also comply with all contractual requirements related to the holding and processing of information:
• JANET Acceptable Use Policy.[11]
• The terms and conditions of licences and contracts.
• The terms and conditions of authentication systems, e.g. Athens.

6. Responsibilities

The Information Policy and Strategy Committee[12] is responsible for the Information Security Policy.

The University has established a strategic information security, risk management and business continuity function within The Deputy Registrar's Office. The Deputy Registrar's Office will be responsible for the development of the Information Security Policy. The Deputy Registrar's Office will co-ordinate implementation and dissemination, and will monitor operation.

Heads of Departments, with support from the Deputy Registrar's Office, are responsible for ensuring that information and information systems used within their department are managed and used in accordance with the Information Security Policy.

Everyone granted access to University information systems has a personal responsibility to ensure that they, and others who may be responsible to them, are aware of and comply with the policies, codes of conduct and guidelines.

Each individual is responsible for protecting the University's information assets, systems and infrastructure, and will protect likewise the information assets of third parties whether such protection is required contractually, legally, ethically or out of respect for other individuals or organisations.

All staff, students and other users should report immediately any observed or suspected security incidents where a breach of the University's security policies has occurred, any security weaknesses

[11] http://www.ja.net/documents/publications/policy/aup.pdf
[12] On behalf of SENATE.

in, or threats to, systems or services. Reports should be made to the Head of Department, the owner of the information, or, where the IT infrastructure is involved, IT Services Help Desk.

Those responsible for information or information systems, for example database and IT systems administrators, must ensure that appropriate security arrangements are established and maintained.

7. Policy Awareness and Disciplinary Procedures

The Information Security Policy will be made available to all staff and students via the web as part of the Governance site, maintained by the Deputy Registrar's Office, dedicated to the explanation and promotion of the policy. Staff, students, authorised third parties and contractors given access to the University information systems will be advised of the existence of the relevant policies, codes of conduct and guidelines.

Failure to comply with the Information Security Policy may lead to suspension or withdrawal of an individual's access to information systems.

Members of staff

Failure of a member of staff to comply with the Information Security Policy may lead to the instigation of the relevant disciplinary procedures[13] as specified in their terms and conditions of employment and, in certain circumstances, legal action may be taken.

Student members

Failure of a student to comply with the Information Security Policy may lead to the instigation of the disciplinary procedures specified in Regulation 23[14], and, in certain circumstances, legal action may be taken.

Minor infringements, such as causing inconvenience to other users, may lead to disciplinary action under the Minor Offences Procedure (Regulation 23 Subsection 6 and 7).

Major infringements, such as major breach of confidentiality, harassment, or illegal activities may lead to action under the Major Offences Procedure (Regulation 23 Subsections 8 and 9). This is not an exhaustive list of possible offences and the University will determine whether a case is minor or major having regard to all the circumstances of each incident.

University contractors

Failure of a contractor to comply could lead to the cancellation of a contract and, in certain circumstances, legal action may be taken.

8. Information Security Education and Training

[13] Further information on the University's staff disciplinary procedure is available on: http://www2.warwick.ac.uk/services/humanresources/newpolicies/disciplinary/

[14] Further information on the University's student disciplinary procedure is available on: http://www2.warwick.ac.uk/services/gov/calendar/section2/regulations/disciplinary

The University recognises the need for all staff, students and other users of University systems to be aware of information security threats and concerns, and to be equipped to support University security policy in the course of their normal work. Appropriate training or information on security matters will be provided for users and departments will supplement this to meet their particular requirements. The Deputy Registrar's Office will undertake a proactive campaign of awareness and monitor/report upon the type and frequency of incidents.

9. Maintenance

The Information Security Policy will be monitored by Information Policy and Strategy Committee and reviewed as necessary. Revisions will be subject to appropriate consultation.

The Deputy Registrar's Office will report on a summary and exception basis, will notify issues and bring forward recommendations.

Heads of Departments should carry out periodic risk assessments[15] and establish and maintain effective contingency plans. They are also required to carry out regular assessment of the security arrangements for their information systems.

Those responsible for information or information systems must carry out periodic risk assessments of their information and the security controls in place. They must take into account changes in business requirements, changes in technology and any changes in the relevant legislation and revise their security arrangements accordingly.

10. Related Policies

- Use of University computing facilities is covered by Regulation 31 - Regulations governing the use of University Computing Facilities available on the Governance website.
- The University has a separate Regulation of Investigatory Powers Act Statement available on http://www2.warwick.ac.uk/services/gov/informationsecurity/policies/
- Data Protection Act issues are also dealt with in the Data Retention Policy guidelines on the Governance website.
- Incidents related to bullying and harassment are covered in the Dignity at Work and Study Policy at http://www2.warwick.ac.uk/services/humanresources/newpolicies/dignity

[15] For help with risk assessments please see: http://www2.warwick.ac.uk/services/gov/riskmanagement/

Appendix

Monitoring and Privacy related to point 4.3

Examples in which the University could expect to investigate user activity:

- Under the terms of the Regulation of Investigatory Powers Act.[16]
- Where there is evidence to suggest legal, contractual or acceptable use obligations have been broken.
- In investigating abnormal system behaviour.[17]

Password protection related to point 4.7

Where University Members are responsible for data the following must apply:

- Never give a password (yours or someone else's) to anyone.
  Even IT Services doesn't need to know your password to be able to help you.
  If anyone asks you for your password, refuse to give it to them, regardless of who they are.
- Never store your password on a computer in an unencrypted form, e.g. not in a Word or text document on your H: drive.
- Avoid writing down your password. If you have no alternative, store the written information out of sight in a secure (locked) location.
  Inappropriate locations include: under a mouse mat or keyboard, on your desk, and attached to a monitor.
- Never send your password via email.
- Make no attempt to learn anyone else's password.
- Never use anyone else's password.
- Inform IT Services immediately if you have reason to believe that a password is known by anyone other than the person authorised to use it.

Passwords **should**:

- Be at least 8 characters long
- Contain at least three of the following four types of character:

[16] A separate statement is available detailing this Act and its use at Warwick.
[17] This could mean the degradation of network services for other users due to activity such as volume file sharing.

  - letters in lower case
  - letters in upper case
  - numbers
  - symbols (e.g. “£$%^&*)

- Be changed every six months for a new password (more often for systems requiring greater security)