THURSDAY 20 SEPTEMBER 2012 • SUPPLEMENT (1) TO NO 4998 • VOL 143

Gazette
Supplement

Information Security Policy

Contents

1 Purpose

This policy provides a framework for the management of information security throughout the University. It applies to:

(a) all those with access to University information systems, including staff, students, visitors and contractors;

(b) any systems attached to the University computer or telephone networks and any systems supplied by the University;

(c) all information (data) processed by the University pursuant to its operational activities, regardless of whether it is processed electronically or in paper (hard copy) form, any communications sent to or from the University and any University information (data) held on systems external to the University's network;

(d) all external parties that provide services to the University in respect of information processing facilities and business activities; and

(e) principal information assets including the physical locations from which the University operates.

2 Aims and commitments

2.1. The University recognises the role of information security in ensuring that users have access to the information they require in order to carry out their work. Computer and information systems underpin all the University's activities, and are essential to its research, teaching and administrative functions.

2.2. Any reduction in the confidentiality, integrity or availability of information could prevent the University from functioning effectively and efficiently. In addition, the loss or unauthorised disclosure of information has the potential to damage the University's reputation and cause financial loss. The Information Commissioner's Office (ICO) has the power to fine organisations up to £500,000 for breaches of the Data Protection Act.

2.3. To mitigate these risks, information security must be an integral part of information management, whether the information is held in electronic or hard-copy form.

2.4. The University is committed to protecting the security of its information and information systems in order to ensure that:

(a) the integrity of information is maintained, so that it is accurate, up to date and fit for purpose;

(b) information is always available to those who need it and there is no disruption to the business of the University;

(c) confidentiality is not breached, so that information is accessed only by those authorised to do so;

(d) the University meets its legal requirements, including those applicable to personal data under the Data Protection Act; and

(e) the reputation of the University is safeguarded.

2.5. In order to meet these aims, the University is committed to implementing security controls that conform to best practice, as set out in the *ISO/IEC 27002:2005 Information Security Techniques – Code of practice for information security management*. The University has drawn up an information security toolkit ("the Toolkit") in order to provide advice and guidance on the technical aspects of information security. The Toolkit is based on the information security toolkit of the Universities and Colleges Information Systems Association and adheres to the standards of ISO/IEC 27002: 2005. It is available at: www.ict.ox.ac.uk/odit/infosec-toolkit.xml.

2.6. Information security risk assessments should be performed for all information systems on a regular basis in order to identify key information risks and determine the controls required to keep those risks within acceptable limits.

2.7. The University is committed to providing sufficient education and training to users to ensure they understand the importance of information security and, in particular, exercise appropriate care when handling confidential information.

2.8. Specialist advice on information security shall be made available throughout the University.

2.9. An information security advisory group (or groups), comprising representatives from all relevant parts of the University, shall advise on best practice and coordinate the implementation of information security controls.

2.10. The University will establish and maintain appropriate contacts with other organisations, law enforcement authorities, regulatory bodies, and network and telecommunications operators in respect of its information security policy.

2.11. Breaches of information security must be recorded and reported to appropriate bodies in the University, who will take action and inform the relevant authorities (please refer to sections 6.13 and 9 for further information).

2.12. This policy and all other supporting policy documents shall be communicated as necessary throughout the University to meet its objectives and requirements.

3 Responsibilities

Council

3.1. Council has ultimate responsibility for information security within the University. More specifically, it is responsible for ensuring that the University complies with relevant external requirements, including legislation.

PRAC ICT sub-committee (PICT)

3.2. The PRAC ICT sub-committee (PICT), or any future equivalent body, is responsible to Council for:

(a) ensuring that users are aware of this policy;

(b) seeking adequate resources for its implementation;

(c) monitoring compliance;

(d) conducting regular reviews of the policy, having regard to any relevant changes in legislation, organisational policies and contractual obligations; and

(e) ensuring there is clear direction and visible management support for security initiatives.

Heads of department

3.3. Given the University's devolved structure, heads of department are responsible for information security within their departments. They must ensure that the department has in place a local information security policy to meet its own particular needs, consistent with the requirements of this overarching policy. The local information security policy should identify the department's own information security requirements and provide a management framework for meeting those requirements. 'Department' in this context includes equivalent local units, as well as divisional offices.

3.4. Specific roles and responsibilities for information security within departments should be clearly identified.

3.5. The head of department must approve the policy, and ensure that it is implemented and kept under regular review.

Users and external parties

3.6. Users of University information will be made aware of their own individual responsibilities for complying with University and departmental policies on information security.

3.7. Agreements with third parties involving accessing, processing, communicating or managing the University's information, or information systems, should cover all relevant security requirements, and be covered in contractual arrangements.

4 Risk assessment and the classification of information

Risk assessment of information held

4.1. The degree of security control required depends on the sensitivity or criticality of the information. The first step in determining the appropriate level of security therefore is a process of risk assessment, in order to identify and classify the nature of the information held, the adverse consequences of security breaches and the likelihood of those consequences occurring.

4.2. Given the devolved nature of the University's structure, the risk assessment should be carried out in the first instance by departments, as defined in paragraph 3.3 above. However, the departmental assessment must be consistent with the general principles in this section.

4.3. The risk assessment should identify the department's information assets, define the ownership of those assets and classify them, according to their sensitivity and/or criticality to the department or University as a whole. In assessing risk, departments should consider the value of the asset, the threats to that asset and its vulnerability. (An example of a risk assessment is in the appendix to this document.) Further guidance on risk assessment and the classification of information is available in the Toolkit[1].

4.4. Where appropriate, information assets should be labelled and handled in accordance with their criticality and sensitivity.

4.5. Rules for the acceptable use of information assets should be identified, documented and implemented. The University's regulations and policies applying to all users of University ICT facilities are available from www.ict.ox.ac.uk/oxford/rules.

4.6. Information security risk assessments should be repeated periodically and carried out as required during the operational delivery and maintenance of the University's infrastructure, systems and processes.

Personal data

4.7. Personal data must be handled in accordance with the Data Protection Act 1998 (DPA) and in accordance with the University's policy and guidance on personal data[2].

4.8. The DPA requires that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

4.9. A higher level of security should be provided for 'sensitive personal data', which is defined in the DPA as data relating to ethnic or racial origin, religious beliefs, physical or mental health, sexual life, political opinions, trade union membership, or the commission or alleged commission of criminal offences.

5 Protection of information systems and assets

5.1. Having completed a risk assessment of their information assets, departments should draw up their own information security policy, setting out appropriate controls and procedures, in accordance with the Toolkit. Information owners must be satisfied that the controls will reduce any residual risk to an acceptable level, in line with the practices outlined in the Toolkit.

5.2. Confidential information should be handled in accordance with the requirements set out in section 6 below.

6 Protection of confidential information

Identifying confidential information is a matter for assessment in each individual case. Broadly, however, information will be confidential if it is of limited public availability; is confidential in its very nature; has been provided on the understanding that it is confidential; and/or its loss or unauthorised disclosure could have one or more of the following consequences:

(a) financial loss (eg the withdrawal of a research grant or donation, a fine by the ICO, a legal claim for breach of confidence);

(b) reputational damage (eg adverse publicity, demonstrations, complaints about breaches of privacy); and/or

(c) an adverse effect on the safety or well-being of members of the University or those associated with it (eg increased threats to staff or students engaged in sensitive research, embarrassment or damage to benefactors, suppliers, staff and students).

6.1. Storage

6.1.1. Confidential information should be kept secure, using, where practicable, dedicated storage (eg file servers) rather than local hard disks, and an appropriate level of physical security.

6.1.2. File or disk encryption should be considered as an additional layer of defence, where physical security is considered insufficient.

6.2. Access

6.2.1. Confidential information must be stored in such a way as to ensure that only authorised persons can access it.

6.2.2. All users must be authenticated. Authentication should be appropriate and, where passwords are used, clearly defined policies should be in place and implemented. Users must follow good security practices in the selection and use of passwords.

6.2.3. Where necessary, additional forms of authentication should be considered.

6.2.4. To allow for potential investigations, access records should be kept for a minimum of six months, or for longer where considered appropriate.

6.2.5. Users with access to confidential information should be security vetted as appropriate, in accordance with existing policies.

6.2.6. Physical access should be monitored, and access records maintained.

6.3. Remote access

6.3.1. Where remote access is required, this must be controlled via a well-defined access control policy and tight access controls provided to allow the minimum access necessary.

6.3.2. Any remote access must be controlled by secure access control protocols using appropriate levels of encryption and authentication.

6.4. Copying

6.4.2. The number of copies made of confidential information, whether on portable devices or media or in hard copy, should be the minimum required, and, where necessary, a record kept of their

distribution. When no longer needed, the copy should be deleted or, in the case of hard copies, destroyed (see 6.12.5).

6.4.3. All copies should be physically secured, eg stored in a locked cupboard, drawer or filing cabinet.

6.5. Disposal

Policies and procedures must be in place for the secure disposal/destruction of confidential information. The University's policy on the disposal of old computers can be found at www.ict.ox.ac.uk/oxford/disposal.

6.6. Use of portable devices or media

6.6.1. Procedures should be in place for the management of removable media in order to ensure that they are appropriately protected from unauthorised access.

6.6.2. The permission of the information owner should be sought before confidential information is taken off site. The owner must be satisfied that the removal is necessary and that appropriate safeguards are in place (eg encryption). For further information, please see the Toolkit[1].

6.6.3. In the case of personal data, the ICO recommends that all portable devices and media should be encrypted where the loss of the data could cause damage or distress to individuals.

6.6.4. The passphrase of an encrypted device must not be stored with the device (see also section 6.8.2).

6.7. Exchange of information and use of email

6.7.1. Controls should be implemented to ensure that electronic messaging is suitably protected.

6.7.2. Email should be appropriately protected from unauthorised use and access.

6.7.3. Email should only be used to send confidential information where the recipient is trusted, the information owner has given their permission, and appropriate safeguards have been taken (eg encryption).

6.7.4. Further guidance on managing the risks associated with the use of email is available on the University website[3] and in the Toolkit.

6.8. Cryptographic controls

6.8.1. Procedures should be in place to support the use of cryptographic techniques and to ensure that only authorised personnel may gain access to confidential information.

6.8.2. University guidance, provided via the Toolkit, on cryptographic policy and key management should be followed to ensure that data are appropriately secured and that all legal and regulatory requirements have been considered.

6.9. System planning and acceptance

A risk assessment should be carried out as part of the business case for any new ICT system that may be used to store confidential information. The risk assessment should be repeated periodically on any existing systems.

6.10. Backup

Information owners should ensure that appropriate backup and system recovery procedures are in place. Backup copies of all important information assets should be taken and tested regularly in accordance with such an appropriate backup policy.

6.11. Further information

The Toolkit provides further guidance on the matters covered in 6.1 to 6.10 above.

6.12. Hard Copies

Protective marking

6.12.1. Documents containing confidential information should be marked as 'Confidential' or with another appropriate designation (eg 'sensitive' etc), depending on the classification system adopted by the department.

Storage

6.12.2.

(a) Wherever practicable, documents with confidential information should be stored in locked cupboards, drawers or cabinets. Where this is not practicable, and the information is kept on open shelving, the room should be locked when unoccupied for any significant length of time.

(b) Keys to cupboards, drawers or cabinets should not be left on open display when the room is unoccupied.

Removal

6.12.3. Confidential information should not be removed from the University unless it can be returned on the same day or stored securely overnight, as described in section 6.12.2 above.

Transmission

6.12.4.

(a) If confidential documents are sent by fax, the sender should ensure they use the correct number and that the recipient is near to the machine at the other end ready to collect the information immediately it is printed.

(b) If confidential documents are sent by external post, they should ideally be sent by a form of recorded delivery. The sender must ensure that the envelope is properly secured.

(c) If confidential documents are sent by internal post the documents should be placed in an envelope marked 'Confidential' with the addresse's name clearly written on it.

Disposal

6.12.5. Confidential documents must be shredded in a confidential manner prior to disposal.

6.13. Enforcement

6.13.1. There must be a written policy in place at the local level for the handling of confidential information, whether electronic or hard copy, and a copy of the procedures must be provided to every user so that they are aware of their responsibilities.

6.13.2. Any failure to comply with the policy may result in disciplinary action.

6.13.3. Any loss or unauthorised disclosure must be promptly reported to the owner of the information.

6.13.4. Computer security incidents involving the loss or unauthorised disclosure of confidential information held in electronic form must be reported to Oxford University Computer Emergency Response Team (OxCERT) – security@oucs.ox.ac.uk – and investigated.

6.13.5. If the loss or unauthorised disclosure involves personal data, whether electronic or hard copy, the University's Data Protection Officer must also be informed, either by email (data.protection@admin.ox.ac.uk) or by phone ((2)70002).

7 Compliance

7.1. The University has established this policy to promote information security and compliance with relevant legislation, including the DPA. The University regards any breach of information security requirements as a serious matter, which may result in disciplinary action.

7.2. Compliance with this policy should form part of any contract with a third party that may involve access to network or computer systems or data.

7.3. Relevant legislation includes, but is not limited to:

- The Computer Misuse Act 1990
- The Data Protection Act 1998
- The Regulation of Investigatory Powers Act 2000
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- The Freedom of Information Act 2000
- The Special Educational Needs and Disability Act 2001.

8 Other relevant University policies or guidance

- Computer disposal: www.ict.ox.ac.uk/oxford/disposal
- Data protection: www.admin.ox.ac.uk/dataprotection
- Email management: www.admin.ox.ac.uk/dataprotection/oxonly/staffguide/#d.en.43187
- Freedom of information: www.admin.ox.ac.uk/foi
- Handling of illegal material: www.ict.ox.ac.uk/oxford/rules/soaguidelines.xml
- Privacy policy: www.admin.ox.ac.uk/dataprotection/privacypolicy
- Records management: www.admin.ox.ac.uk/lso/statutes/recordsmanagementpolicy
- Regulations relating to the use of information technology facilities: www.admin.ox.ac.uk/statutes/regulations/196-052.shtml

9 Contacts for further information

Name	Office	Email	Tel	Further info
Jonathan Ashton	Information Security Officer	infosec@it.ox.ac.uk		Information security
Robin Stevens	OXCERT	security@it.ox.ac.uk	82222	Security incidents
Paul Jeffreys	Director of IT Risk Management	infosec@it.ox.ac.uk		Information security
Max Todd	Council Secretariat	data.protection@admin.ox.ac.uk	80299	Data protection

[1] www.ict.ox.ac.uk/odit/infosec-toolkit.xml

[2] www.admin.ox.ac.uk/dataprotection

[3] www.admin.ox.ac.uk/dataprotection/oxonly/staffguide/#d.en.43187

Appendix

Sample Risk Assessment

For more detailed guidance see: www.ict.ox.ac.uk/odit/infosec-toolkit.xml.

SCOPE, CRITERIA AND ORGANISATION

Scope

Criteria

RISK IDENTIFICATION AND ANALYSIS

Assets

An example of one way to record assets is given here:

Asset	Type	Value	Owner	Vulnerabilities	Vulnerability type	Likelihood of being exploited	Impact

Threats and Risks

An example method for listing threats is given here:

Threat	Type	Extent	Likely Frequency

One possible threat rating tool is given here:

Threat Rating	Guide
Low	Incidents occur less than once a year
Medium	Incidents occur at least once a year
High	Incidents occur at least once a month

Vulnerabilities

A possible vulnerability rating tool is given here:

Vulnerability	Guide
Low	<33% chance of worst case scenario in the event of an incident
Medium	33%-66% chance of worst case scenario in the event of an incident
High	>66% chance of worst case scenario in the event of an incident

Example Risk Matrix

One possible technique is to use the following risk matrix:

	Threat	Low			Medium			High		
	Vulnerability	L	M	H	L	M	H	L	M	H
Asset	0	0	1	2	1	2	3	2	3	4
Value	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Glossary

Access control – ensures that resources are only granted to those users who are entitled to them

Appropriate – suitable for the level of risk identified and justifiable by risk assessment

Asset – anything that has a value to the University

Audit – information gathering and analysis of assets to ensure such things as policy compliance and security from vulnerabilities

Authentication – the process of confirming the correctness of a claimed identity

Best Practice – current standard advice for implementing security controls. Synonymous with 'good practice'

Confidentiality – the need to ensure that information is disclosed only to those who are authorised to view it

Control – a means of managing risk by providing safeguards. This includes policies, procedures, guidelines, other administrative or technical controls or management controls

Data – information held in electronic or hard copy form

DPA – Data Protection Act 1998

External party – *see* Third party

ICO – Information Commissioner's Office (www.ico.gov.uk)

Information – any communication or representation of knowledge such as facts, data or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative or audiovisual

Information owner – synonymous with 'information risk owner'. This is the person who is responsible for accepting any residual risk

Information security – preservation of confidentiality, integrity and availability

Information security toolkit – collection of guidelines, policies, interpretation, technical guidance and example solutions

Information systems – any system, service or infrastructure used to process information or the physical locations housing them. This includes critical business environments, business processes, business applications (including those under development), computer systems and networks

ISO/IEC 27002:2005 – information security code of practice published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), entitled 'Information technology – Security techniques – Code of practice for information security management'

OxCERT – Oxford University's Computer Emergency Response Team (www.oucs.ox.ac.uk/network/security/about)

Personal Data – any data held in a system, whether electronic or hard copy, that identifies a living individual (for a legal definition, see Data Protection Act 1998)

Policy – overall intention and direction as formally expressed by management

Risk – the potential for an unwanted event to have a negative impact as a result of exploiting a weakness. It can be seen as a function of the value of the asset, threats and vulnerabilities

Risk Assessment – overall process of identifying and evaluating risk

Third party – person or body that is recognised as being independent of the University

Threat – something that has the potential to exploit a weakness to result in some form of damage. Threats can be environmental, deliberate, accidental, logical or technical

UCISA – Universities and Colleges Information Systems Association (www.ucisa.ac.uk)

Vulnerability – weakness of an asset or group of assets that may be exploited by a threat