

Information Security Policy

Summary

The University of Aberdeen Information Security Policy has been developed with reference to the University Colleges and Information Systems Association (UCISA) Information Security Toolkit, incorporating changes to the Compliance and Human Resources sections, following discussions with the Director of Human Resources.

Further, in response to recent high-profile events elsewhere, the Policy has been amended (at 8.15) to ensure that it addresses security risks associated with the transmission of material through the post or other means.

The inventory of major information assets referred to in Section 8, Information Handling, and guidance on implementation of the Policy will follow at a later date. Following discussions at Staffing and Development Committee on 22 January 2008, it was further agreed to develop an Executive Summary and flowchart as preface and appendix to the document before dissemination to the University community.

The Information Security Policy has been considered and for their parts approved by: the Information Strategy Committee, University Management Group, Joint Negotiation and Consultative Committee, Support Staff Liaison Committee and Staffing and Development Committee. The University Court approved the University Information Security Policy, at its meeting of 5 February 2008.

1 Introduction

1.1 What is Information Security and why do we need to think about it?

1.1.1 Information Security is the practice of ensuring that information is only read, heard, changed, broadcast and otherwise used by people who have the right to do so. It requires a range of skills and knowledge and increases in importance as the use of and reliance upon information grows.

1.1.2 All information has value. Sometimes this might be trivial but in many cases the value is substantial. Value can be measured in different ways, depending on the nature of information. In some cases, there may be a straightforward monetary value associated with given information. For others, emphasis is placed on different aspects of value, for example, the effects of unauthorised disclosure and loss of confidentiality.

1.1.3 The range of undesirable consequences associated with breaches of Information Security includes:

- Systems being unavailable
- Bad publicity and embarrassment
- Fraud
- Unauthorised access to personal data

1.2 How can information be protected?

1.2.1 Information Security is often seen as a highly technical matter that requires expensive equipment and specialist assistance. While there are many situations that do need this type of approach, the most sensible and effective first steps are based on common sense and sound management practice. Assessing and understanding the risks for the University will help to establish appropriate risk management. In turn, this should ensure appropriate incident management and recovery when security is compromised.

1.2.2 Information Security can be achieved through the following:

- A pragmatic approach to policy and standards, resulting in an Information Security Policy which is supported by realistic and workable processes and procedures.
- The rigour of security measures applicable to any information system, proportional to the assessed risk of the confidentiality, integrity or availability of its information becoming compromised.
- A 'light touch' risk assessment process which categorises the likelihood and consequences of any compromise of an information system's confidentiality, integrity or availability as being high or low.
- A well-informed, well-trained workforce exercising an appropriate (but not excessive) level of vigilance.

2 Information Security Policy and Infrastructure

Objective: To provide management direction and support for Information Security and to manage Information Security within the University.

2.1 It is the Policy of the University that information which it manages shall be appropriately secured in order to protect the University and its members from the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information. The Risk Management Committee working with the Information Strategy Committee shall ensure that appropriate risk assessments are carried out to identify the likelihood and impact of information security failures.

2.2 This Information Security Policy provides management direction and support for Information Security across the University. This Policy has been approved by the University Court. It is applicable to and will be communicated to staff, students and other relevant parties.

2.3 The Information Strategy Committee shall ensure that there is clear direction and visible management support for security initiatives.

2.4 The responsibility for ensuring the protection of information systems and that specific security processes are carried out shall lie with the Head of College, School or Section managing that information system. The implementation and ongoing monitoring of the

Information Security Policy shall be reviewed independently of those charged with its implementation, normally through the University's Internal Audit processes.

3 Business Continuity Management and Planning

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

3.1 A Business Continuity Plan will be developed for each system or activity. The nature of the plan and the actions it contains will be commensurate with the criticality of the system or activity to which it relates. All Plans will be periodically reviewed and tested. The frequency of testing will be dependent upon criticality level and will include tests to verify whether management and staff are able to put the plan into operation.

4 Compliance

Objective: To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.

4.1 All users of the University's computer based information systems are advised of their responsibilities in documentation provided by the Directorate of Information Technology (DIT). Any breach by staff may be dealt with under the University's disciplinary procedures, and by students under the Code of Practice on Student Discipline.

4.3 Guidance documents are made available to all computer users through the University's website covering the key aspects of the law in so far as they relate to the use of information systems.

4.4 The University's Data Retention Policy defines the appropriate length of time for different types of information to be held. Data will not be destroyed prior to the expiry of the relevant retention period and will not be retained beyond that period. During the retention period appropriate technical systems will be maintained to ensure that the data can be accessed.

4.5 The University will only process personal data in accordance with the requirements of the Data Protection Act and the University's Data Protection Policy. Personal or confidential information will only be disclosed or shared where an employee has been authorised to do so.

4.6 All University systems will be operated and administered in accordance with the documented procedures. Regular checks will be carried out through a process of Internal Audit to verify this compliance.

5 Outsourcing and Third Parties

Objectives: To maintain the security of the University's information processing facilities and information assets accessed by third parties;

To maintain the security of information when the responsibility for information processing has been outsourced;

To ensure the correct and secure operation of information processing facilities;

To maintain the security of application system software and information.

5.1 External suppliers who are contracted to supply goods or services to the University should, as appropriate, be informed of the University's Information Security policy and may be required to agree to observe that policy. A summary of the Information Security Policy will be provided to any such supplier, prior to any supply of services. The University may require external suppliers of services to sign a non-disclosure agreement to protect its information assets.

6 Human Resources

Objectives:

To reduce the risks of human error, theft, fraud or misuse of facilities;

To ensure that users are aware of Information Security threats and concerns, and are equipped to support organisational security Policy in the course of their normal work;

To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents.

6.1 All members of the University must comply with the Information Security Policies of the University. Any Information Security incidents resulting from non-compliance may result in disciplinary action.

6.2 Where necessary employees may be required to sign a formal undertaking concerning the need to protect the confidentiality of information, both during and after their employment with the University. Non-disclosure agreements should be used in all situations where the confidentiality, sensitivity or value of the information being disclosed is important.

6.3 An appropriate summary of the Information Security Policies must be delivered to, and accepted in writing by, all staff as part of the normal recruitment and appointment process.

6.4 New staff will receive Information Security awareness training as part of induction. Where staff change jobs, their Information Security needs must be re-assessed and any new training

provided. The University will provide training to all users of new systems to ensure that their use is both efficient and does not compromise Information Security.

6.5 Access privileges of staff will normally be terminated on their last day of employment with the University. Access may be extended on application by the relevant Head of School, Head of Section to the Director of Human Resources who will refer the matter to the Director of Information Technology. Such application should be made in advance of the last day of employment.

7 Operations

Objectives:

To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents;

To prevent unauthorised physical access, damage and interference to business premises and information;

To ensure the correct and secure operation of information processing facilities;

7.1 Areas and offices where sensitive or critical information is processed shall be given an appropriate level of physical security and access control. Staff with authorisation to enter such areas are to be provided with information on the security risks and the measures used to control them.

7.2 Duties and areas of responsibility must be segregated to reduce the risk and consequential impact of information security incidents.

7.3 Procedures must be established and widely communicated for the reporting of security incidents and suspected security weaknesses in business operations and information processing systems.

7.4 Procedures are established for the reporting of software malfunctions and faults in the University's information processing systems. Faults and malfunctions are logged and monitored and timely corrective action taken.

7.5 Changes to operational procedures must be controlled and must have management approval.

7.6 Development and testing facilities for business critical systems must be separated from operational facilities and the migration of software from development to operational status must be subject to formal change control procedures.

7.7 Acceptance criteria for new information systems, upgrades and new versions must be established and suitable tests of the systems carried out prior to migration to operational status.

8 Information Handling

Objectives:

To maintain appropriate protection of all the University's information assets and to prevent loss, damage or compromise of assets and interruption to business activities;

To prevent compromise or theft of information and information processing facilities;

To maintain the integrity and availability of information processing and communication services;

To prevent loss, modification or misuse of information exchanged between organisations and user data in application systems.

8.1 An inventory is maintained of all the University's major information assets and the ownership of each is clearly stated. Within the inventory, each information asset is classified according to sensitivity using the University's agreed information security classification scheme. Classified information and outputs from systems handling classified data are appropriately labelled according to the output medium.

8.2 When permanently disposing of equipment containing storage media all sensitive data and licensed software must be deleted before the equipment is moved off site using procedures authorised by the Director of Information Technology. Damaged storage devices containing sensitive data must undergo appropriate risk assessment, to determine if the device should be destroyed, repaired or discarded.

8.3 The University encourages a clear desk and screen policy when employees are absent from their normal work place and outside normal working hours. In addition, screens 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.

8.4 Removal off site of the University's sensitive information assets, either printed or held on computer storage media, must be properly authorised by the appropriate Head of School, Head of Section or line manager.

8.5 Information owners must ensure that appropriate backup and system recovery procedures are in place. The Head of College, School or Section is responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of the business.

8.6 The archiving of information and documents must take place with due consideration for legal, regulatory and business issues, with liaison between technical and business staff, and in keeping with the University's Data Retention Policy. Storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must also be carefully considered, especially where proprietary formats are involved.

8.7 All users of information systems must manage the creation, storage, amendment, copying and deletion or destruction of data files in a manner which safeguards and protects the confidentiality, integrity and availability of such files.

8.8 Day to day data storage must ensure that current information is readily available to authorised users and that archives are both created and accessible in case of need.

8.9 Highly sensitive or critical documents should not rely upon the availability or integrity of data files over which the author may have no control. Key documents and reports should normally be self-contained. Hard copies of sensitive or classified material must be protected and handled according to the distribution and authorisation levels specified for those documents.

8.10 All users must be aware of the risks of breaching confidentiality associated with the photocopying (or other duplication) of sensitive documents. All information used for, or by the University, must be filed appropriately and according to its classification.

8.11 All signatures authorising access to systems or release of information must be properly authenticated.

8.12 All hardcopy documents of a sensitive or confidential nature must be disposed of when no longer required, in line with the University's Data Retention Policy and policy on sustainability.

8.13 Any third party used for external disposal of the University's obsolete information-bearing equipment or hardcopy material must be able to demonstrate compliance with the University's information security.

8.14 Prior to sending sensitive information or documents to third parties, not only must the intended recipient be authorised to receive such information, but the procedures and information security measures adopted by the third party must also be seen to continue to assure the confidentiality and integrity of the information.

8.15 Sensitive data or information, may only be transferred across networks, transmitted by post or other similar means or copied to other media, when the confidentiality and integrity of the data can reasonably be assured.

8.16 Email addresses and faxes should be checked carefully prior to dispatch, especially where the information content is sensitive.

8.17 The identity of recipients or requesters of sensitive or confidential information over the telephone must be verified and they must be authorised to receive it.

8.18 Staff authorised to make payment by credit card for goods ordered over the telephone or Internet, are responsible for safe and appropriate use.

8.19 Email should only be used for business purposes in a way which is consistent with other forms of business communication. Information received via email must be treated with care due to its inherent information security risks. File attachments should be scanned for possible viruses or other malicious code.

9 User Management

Objectives: To control access to information;

To ensure that access rights to information systems are appropriately authorised, allocated and maintained.

9.1 Procedures for the registration and de-registration of users and for managing access to information systems shall ensure that users' access rights match their authorisations. Users shall have a unique identifier (user ID) for their personal and sole use for access to University information services. The user ID must not be used by anyone else and associated passwords shall not be shared with any other person for any reason. Password management procedures shall ensure the implementation of the requirements of the Information Security policies and assist both staff and students in complying with best practice guidelines.

9.2 Access control standards must be established and reviewed regularly for all information systems, at an appropriate level for each system, to minimise Information Security risks and yet allow the University's business activities to be carried out without undue hindrance.

9.3 Access to all systems must be authorised by the manager responsible for the system and a record must be maintained of such authorisations, including the appropriate access rights or privileges granted. Users' access rights must be adjusted appropriately, and in a timely manner, whenever there is a change in business need, staff change their role, or staff or students leave the University.

10 Use of Computers

Objectives:

To protect the integrity of software and information from damage by malicious software;

To maintain the integrity and availability of information processing and communication services;

To prevent loss, modification or misuse of information exchanged between organisations;

To prevent unauthorised user or computer access.

10.1 Equipment must be safeguarded appropriately - especially when left unattended.

10.2 Files downloaded from the Internet, including files attached to electronic mail, must be treated with the utmost care to safeguard against both malicious code and inappropriate material. Such files, or any others not known to come from a trusted source, must be scanned for possible malicious code before being opened.

10.3 Electronic mail must not be used to communicate confidential or sensitive information unless appropriate measures have been taken to ensure authenticity and confidentiality, that it is correctly addressed and that the recipients are authorised to receive it.

10.4 Any essential information stored on a laptop or on a PC's local disk must be backed up regularly. It is the responsibility of the user to ensure that this takes place on a regular basis.

10.5 Sensitive or confidential data should only be accessed from equipment in secure locations and files must never be printed on a networked printer that does not have adequate protection or security. Utmost care must be used when transporting files on removable media (e.g. disks, CD-ROMs and USB flash drives) to ensure that valid files are not over-written or incorrect/ out-of-date information is not imported.

11 System Planning

Objectives:

To manage information security within the University.

To minimise the risk of systems failure.

11.1 New information systems, or enhancements to existing systems, must be authorised jointly by the manager(s) responsible for the information and the Director of Information Technology. The business requirements of all authorised systems must specify requirements for security controls.

11.2 The implementation of new or upgraded software must be carefully planned and managed, to ensure that the information security risks associated with such changes are mitigated using a combination of procedural and technical controls. The information assets associated with any proposed new or updated systems must be identified, classified and recorded, in accordance with the Information Handling Policy, and a risk assessment undertaken to identify the probability and impact of security failure.

11.3 Equipment supporting business systems shall be planned to ensure that adequate processing power, storage and network capacity are available for current and projected needs, all with appropriate levels of resilience and fault tolerance and are given adequate protection from unauthorised access, environmental hazards and electrical power failures.

11.4 Access controls for all information and information systems must be set at appropriate levels in accordance with the value and classification of the information assets being protected. Access to operating system commands and application system functions is restricted to those persons who are authorised to perform systems administration or management functions. Where appropriate, such commands should be logged and monitored.

11.5 Prior to acceptance, all new or upgraded systems shall be tested to ensure that they comply with the University's information security policies, access control standards and requirements for ongoing information security management.

12 System Management

Objectives:

To protect the integrity of software and information from damage by malicious software;

To prevent unauthorised computer access;

To detect unauthorised activities.

12.1 The University's systems and business applications must be managed by suitably trained and qualified staff to oversee their day-to-day running and to preserve security and integrity in collaboration with individual system or application owners.

12.2 Access controls shall be maintained at appropriate levels for all systems and any changes of access permissions must be authorised by the manager of the system or application. A record of access permissions granted must be maintained. Access to all information services must use a secure log-on process and all access will be logged and monitored to identify potential misuse of systems or information..

12.3 Access to operating system commands is restricted to those persons who are authorised to perform systems administration or management functions. Use of such commands is logged and monitored.

12.4 The implementation of new or upgraded software must be carefully planned and managed. Formal change control procedures, with audit trails, shall be used for all changes to systems.

12.5 Capacity demands of systems supporting business processes must be monitored and projections of future capacity requirements made to enable adequate processing power, storage and network capacity to be made available.

12.6 Security event logs, operational audit logs and error logs must be reviewed and managed by qualified staff.

12.7 System clocks must be regularly synchronised between the University's various processing platforms.

13 Network Management

Objective: To prevent loss, damage or compromise of assets and interruption to business activities.

13.1 The University's network must be managed by suitably authorised and qualified staff to oversee its day-to-day running and to preserve its security and integrity in collaboration with individual system owners.

13.2 The network must be designed and configured to deliver high performance and reliability to meet the University's needs whilst providing a high degree of access control and a range of privilege restrictions. The network must be segregated into separate logical domains with routing and access controls operating between the domains.

13.3 Networks and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorised intrusion.

13.4 Moves, changes and other reconfigurations of users' network access points will only be carried by staff authorised by the Directorate of Information Technology according to procedures laid down by them.

13.5 Access to the resources on the network must be strictly controlled to prevent unauthorised access and access control procedures must provide adequate safeguards through robust identification and authentication techniques. Access to all computing and information systems and peripherals will be restricted unless explicitly authorised.

13.6 Remote access to the network will be subject to robust authentication.

14 Software Management

Objectives:

To ensure that security is built in to information systems;

To maintain the security of application system software and information.

14.1 The University's business applications must be managed by suitably trained and qualified staff to oversee their day to day running and to preserve security and integrity in collaboration with nominated individual application owners.

14.2 The procurement or implementation of new, or upgraded, software must be carefully planned and managed and any development for or by the University must always follow a formalised development process. Information security risks associated with such projects must be mitigated using a combination of procedural and technical controls.

14.3 Business requirements for new software or enhancement of existing software must specify the requirements for information security controls.

14.4 Formal change control procedures, with comprehensive audit trails, must be used for all changes or upgrades to business software. All changes must be properly authorised and all software, including that which interacts with the amended software, must be tested before changes are moved to the live environment.

14.5 Modifications to vendor supplied software shall be discouraged, only strictly controlled essential changes shall be permitted and the development of interfacing software shall only be undertaken in a planned and controlled manner.

14.6 The implementation, use or modification of all software on the University's business systems shall be controlled. All software shall be checked before implementation to protect against malicious code.

15 Mobile Computing

Objective: To ensure information security when using mobile computing facilities.

15.1 Users of mobile computing equipment must comply with guidelines on the use of such equipment advising them on how use these in ways that conform to the University's Information Security Policy and other good practices.

16 Teleworking

Objective: To ensure information security when using teleworking facilities.

16.1 Persons who undertake part or all of their work using dedicated equipment in a fixed location outside the University (teleworking) must be authorised to do so

16.2 Teleworkers must be provided with appropriate computing and communications equipment and so far as practicable should use only this equipment for teleworking. All teleworking agreements must include rules on the use of equipment provided for teleworking.

First Draft

PJM/mg

22 September 2005

Second Draft

BFR

3 October 2006

Third Draft

PH

9 October 2006

Fourth Draft

May 2007

Final Revisions Nov / Dec 2007