Information Security Policy

Harper Adams University

Harper Adams University

INFORMATION SECURITY POLICY

The University recognises that information and information systems are valuable assets which play a major role in supporting the University's strategic objectives. Information security is important to the protection of the University's reputation and the success of academic and administrative activities. It is also an integral part of information sharing which is essential to academic and corporate endeavour. The management of personal data has important implications for individuals and is subject to legal obligations. The consequences of information security failures can be costly and time-consuming.

The Information Security Policy sets out appropriate measures through which the University will facilitate the secure and reliable flow of information, both within the University and in external communications. It comprises this document, which sets out the principles and framework, and a set of specific codes of practice and guidelines addressing individual aspects of security (available on the Portal and on the Harper Adams website.). The approach is based on recommendations contained in *British Standard 7799 - A Code of Practice for Information Security Management*.

Objectives

The objective of the Information Security Policy is to ensure that all information and information systems upon which the University depends are adequately protected to the appropriate level.

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, by electronic means and by oral communication, including telephone and voicemail. It applies throughout the lifecycle of the information from creation through storage and utilisation to disposal. 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.

The policy applies to all staff and students of the University and to other users associated with the University. With regard to electronic systems, it applies to use of University owned facilities and privately/externally owned systems when connected to the University network directly or indirectly. ('Owned' is deemed to include leased, rented or on-loan).

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.

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:

Authorised Use

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

Acceptable Use

All users have an obligation to use information and information systems responsibly. Rules are defined in the Acceptable Use Policy and Code of Practice.

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 defined in the Acceptable Use Policy and Code of Practice

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.

Retention and Disposal of Information

All staff have a responsibility to consider security when using and disposing of information in the course of their work. The University recommends retention

periods 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.

Virus Control

The University has an Anti-virus Policy and it is an offence under University regulations to knowingly introduce a virus or take deliberate action to circumvent precautions taken to prevent the introduction of a virus.

Business Continuity

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

Legal and Contractual Requirements

The University will abide by all UK legislation and relevant legislation of the European Community related to the holding and processing if information. This includes the following Acts and the guidance contained in the Information Commissioner's Codes of Practice:

- Computer Misuse Act 1990

- Copyright Designs and Patents Act (1988)

- Data Protection Act 1998

- Freedom of Information Act (2000)

- Human Rights Act (1998)

- Regulation of Investigatory Powers Act (2000)

- Counter-Terrorism and Security Act (2015)

The University will also comply with all contractual requirements related to the holding and processing of information:

- JANET Acceptable Use Policy issued by JISC

- Code of Conduct on the Use of Software and Datasets issued by JISC

- The terms and conditions of licences and contracts

- The terms and conditions of authentication systems, e.g. Athens/Shibboleth

Responsibilities

The University's Chief Technical Officer will be responsible for development of the policy, will co-ordinate implementation and dissemination, and will monitor the operation of the policy working in collaboration with other departments.

Heads of Group/Departments, with support from the Chief Technical Officer, are responsible for ensuring that information and information systems used within their department are managed and used in accordance with information security policies.

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 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 Service Desk or the Chief Technical Officer.

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

Policy Awareness and Disciplinary Procedures

The Information Security Policy will be made available to all staff and students via the web. Staff, students, authorised third parties and contractors given access to University information systems will be advised of the existence of the relevant policies, codes of conduct and guidelines. Users will be asked to confirm that they understand the policy before being given access to some systems.

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

Failure of a member of staff to comply with the Information Security Policy may lead to the instigation of the relevant disciplinary procedures as specified in their terms and conditions of employment and, in certain circumstances, legal action may be taken. Minor infringements, such as causing inconvenience to other

users, may lead to a verbal or written warning. Major infringements, such as major breach of confidentiality, harassment, or illegal activities may lead to a formal warning, suspension or termination of employment. 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.

Failure of a student to comply with the Information Security Policy may lead to the instigation of the disciplinary procedures, 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 procedures. Major infringements, such as major breach of confidentiality, harassment, or illegal activities may lead to action under the major offences procedures 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.

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

Information Security Education and Training

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. Information Services and the institution's Data Protection Officer will undertake a proactive campaign of awareness and monitor/report upon incidents.

Maintenance

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

The Chief Technical Officer will report on a summary and exception basis, will notify issues and bring forward recommendations.

Heads of Departments are required to carry out periodic risk assessments 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.

POINTS OF CONTACT

If you need assistance regarding the following topics related to Systems usage, you should initially contact the Service Desk, for additional assistance.

IT Service Desk   01952 815555   servicedesk@harper-adams.ac.uk

Related documents:

http://www.harper-adams.ac.uk/general/governance/publication-scheme.cfm

- Data Protection Policy

- Data Protection and Freedom of Information – Complaint Procedure

- Information Technology – Acceptable Use Policy

- Records Retention Guidelines