The University of Sheffield

Information Security Policy

This document is uncontrolled when printed.
Before use, check to verify that this is the current version.
Compliance is mandatory.

Version and Ownership

Version	Date	Author(s)	Comments
0.1	18/04/2018	Chris Willis	Initial draft supplied to IMG for consideration
0.2	20/04/2018	Chris Willis	Incorporated initial feedback from Chair of IMG
1.0	24/04/2018	IMG	Approved by Information Management Group, IMG
1.1	07/12/2018	Sinead O'Brien	Template update and minor modifications
1.2	18/12/2018	John McAuley	Approved by Interim Director, CiCS

Introduction

Information, in all its forms, is a primary resource of the University; its effective curation and protection is critical to the effective running an reputation of the University.

The objective of the Information Security Policy (the "Policy") and supporting information management governance is to protect the University by preventing and limiting the impact of information security problems that might damage the University´s operation, reputation or business.

The Policy recognises the concepts of academic and individual freedom, and will aim to ensure that the University: employs appropriate security measures; adopts a suitable methodology for guiding the approach to managing security; and complies with all legal and contractual requirements.

Where necessary additional information governance that goes above and beyond this Policy will be put in place and must be adhered to. This is most commonly required where the data is considered to be more sensitive and/or where there is a legal, statutory or contractual requirement. 1

Scope

Information Security covers the protection of all forms of information to ensure its confidentiality, integrity and availability. This includes, but is not limited to: information stored or processed on computers, transmitted across networks, printed or written on paper, spoken directly or over a voice network, and accessed via personal devices.

The Policy applies to all University information assets and/or information systems controlled by the University.

The Policy applies to all areas of the University's business and the people and organisations involved in it

Objectives

The Policy and supporting information governance will:

- Protect the confidentiality, integrity and availability of the University's information.
- Take a considered and risk based approach to information security management.
- Establish a security aware culture within the University, ensuring that all involved have the skills and awareness to manage and secure information.
- Give assurance to the University and 3rd parties that information is appropriately protected.
- Align to recognised standards and good practice.
- Respond to, manage and learn from information security incidents in order to reduce the likelihood and impact of incidents.
- Enable continuous improvement in information security

Responsibilities

All individuals in scope of the Policy must:

- Be aware of and adhere to relevant information security policies and procedures

- Complete mandatory information security training appropriate to their role
- Ensure that information and information systems under their control are protected appropriately, seeking advice where necessary
- Report potential, suspected, or actual breaches of information security

Those with responsibility for information assets, business activities, information systems or individuals must ensure that policies and processes are disseminated appropriately and adhered to (e.g. a supervising line-manager must ensure that staff working under their direction are aware of and abide by relevant processes).

The University's Information Management Group (IMG) reports to the University Executive Board (UEB) through the Chair's line reporting. IMG provides overarching information governance for all University information assets.

Corporate Information and Computing Services (CiCS) are responsible for the development and implementation of information security policies, procedures and guidance, and will provide specialist support where needed.

Failure to comply with relevant policies and procedures by individuals and/or organizational units (e.g. departments, research groups) will be investigated in accordance with the University's Information Security Incident Policy. Where breaches of policy are confirmed action may be taken, including but not limited to; the temporary or permanent withdrawal of access to computing facilities, disciplinary action, or escalation to the IMG and in turn to UEB.

See Information Governance Roles and Responsibilities for an overview of roles and responsibilities within the wider University Information Governance landscape.

Policy Development and Implementation

This information security policy framework is in the process of being aligned to ISO 27001. New policies will be developed and existing ones reviewed under the oversight of IMG. The information security policy framework will be formally reviewed annually.

This policy is published to all members of the University, who are expected to be familiar with the key principles and to comply with them. Where possible, information systems will carry a notice to draw the users attention to appropriate policies.

The University has already developed detailed policies and procedures that in part implement the requirements of the Policy, however there are a number of areas that still require specific policies

Information Security Policy Principles

Information Security covers the protection of all forms of information to ensure its confidentiality, integrity and availability as follows;

- Confidentiality - ensuring that information is only available to authorised users
- Integrity - ensuring that information is accurate and fit for purpose
- Availability - ensuring that information is available when and where it is needed

The following principles must be adhered to:

1. **Information must be identified, assessed, classified and protected in accordance with agreed policies and standards.**

2. **Security controls must be put in place to ensure the confidentiality, integrity and availability of information is assured. Controls should be commensurate with risk but at all times they must adhere to minimum standards set by University policies and legal/regulatory standards. Security controls must be maintained when information is taken off-site or accessed from mobile technologies.**

3. **Transfers of information to third parties must adhere to policy and be authorised at an appropriate level. Minimum agreed levels of security controls must be maintained. (Transfer to third parties includes the use of cloud services by individual users).**

4. **Measures must be in place to ensure that agreed levels of availability are in place are maintained in the event of the accidental or deliberate loss of information or information systems.**

5. **All incidents involving actual or potential breaches of Information Security must be reported and managed in accordance with the Information Security Incident Policy and Procedure. The University will investigate all security incidents and take action in accordance with this policy; other related documents; University Regulations and discipline procedures; and English Law.**

Information Security Policies, Procedures and Guidance

Supporting information security policies for the principles listed above can be found at https://www.sheffield.ac.uk/cics/policies/infosec

- Information Security procedures and guidance for securing information, systems and accounts can be found at https://www.sheffield.ac.uk/cics/security
- Information Security training can be found at https://infosecurity.shef.ac.uk. The following online courses are mandatory for ALL staff;
    - Protecting personal information
    - Protecting personal data