St Hilda's College
UNIVERSITY OF OXFORD

Information Security Policy

Contents

1. Purpose

1.1. Information is critical to the collegiate university operations and failure to protect information increases the risk of financial and reputational losses. The collegiate university is committed to a systematic, risk-based approach to protecting information in all its forms from a loss of confidentiality, integrity or availability.

1.2. This policy outlines St Hilda's College's approach to information security management and provides guiding principles and responsibilities to ensure information security objectives are met, taking full account of teaching and research needs and the collegiate university's governance and management structures. Information Security is not static; it is subject to a process of continual improvement as technology changes and the threat evolves.

2. Scope

2.1. This policy is applicable to:

2.1.1. all organisations and individuals who have access to collegiate university information and technologies and all organisations and services that connect to the St Hilda's College network;

2.1.2. all facilities, technologies and services that are used to process College and University of Oxford information;

2.1.3. information processed, in any format, by the College pursuant to its operational activities;

2.1.4. internal and external processes used to process College information; and

2.1.5. external parties that provide information processing services to the College.

3. Objectives

3.1. The overall objectives for information security are that:

3.1.1. a culture is embedded to ensure all teaching, research and administration activities consider information security, including preparation for responding to cyber security events;

3.1.2. individuals are aware and kept informed of their information security responsibilities;

3.1.3. information security is managed based on an assessment of risk to information assets;

3.1.4. information assets are identified, and controls are applied proportionately to mitigate risks to a defined level of tolerance in a cost-effective manner;

3.1.5. authorised users can securely access information to perform their roles;

3.1.6. facilities, technologies, and services adequately balance usability and security;

3.1.7. contractual, regulatory, and legal obligations relating to information security are met;

3.1.8. incidents are effectively managed and resolved;

3.1.9. constituents of the College develop resilience from the effects of major cyber security incidents; and

3.1.10. information security complies with the recognised international standards ISO 27001/2 and supports compliance with other standards as demanded by collaborators such as the University of Oxford and the NHS.

3.2. These objectives must cascade into lower-level objectives. All levels and plans should be drawn up at each level to ensure they are achieved.

4. A wider framework

4.1. The information security policy is underpinned by a series of policies and procedures, to ensure that:

4.1.1. a consistent and planned approach is taken to information security;

4.1.2. information security risk is managed through risk assessments on IT systems and services, information assets and processes;

4.1.3. information security requirements are covered in agreements with third-party partners or suppliers, and these are monitored for compliance;

4.1.4. appropriate information security controls are implemented to protect all IT facilities, technologies and services used to access, process and store College and University information;

4.1.5. these controls, described in the baseline, are to be enforced by all constituents on the Oxford domain;

4.1.6. controls are monitored to ensure they are adequate and effective;

4.1.7. all information security incidents are reported in a timely manner via appropriate management channels, information systems are isolated, and incident thoroughly investigated and managed;

4.1.8. all constituents' information assets are identified, owned, classified according to how critical and sensitive they are, and rules for their use are in place;

4.1.9. business continuity and disaster recovery are planned and exercised in case of a major cyber event; and

4.1.10. communications are planned and managed.

5. Baseline Monitoring

5.1. To provide the foundation of a pragmatic information security policy, the University of Oxford maintains a target set of management and technical security requirements, representing a good level of security, referred to as the "Baseline". The Baseline will be reviewed annually to ensure it reflects changes in technology, risks and converges towards international security standards. St Hilda's College is expected to assess the information security in College with this University baseline and implement plans to close gaps in compliance.

5.2. The Baseline does not replace the need to assess and manage information security risk.

6. Responsibilities

6.1. The following bodies and individuals have specific information security responsibilities:

6.1.1. **The Governing Body** has executive responsibility for information security risk within the College.

6.1.2. **All Staff and Students and other users handling collegiate university information**, are required to complete the University of Oxford's information security awareness training including an annual refresher. They are responsible for making informed decisions to protect information, including datasets for research and teaching and all other College or university documentation. They are also responsible for reporting incidents promptly.

7. Related policies

7.1. This Policy should be read in conjunction with related College policies and procedures, including with regard to Data Protection, Mobile Devices, and Network Acceptable Use, and with University of Oxford Regulations Relating to the use of Information Technology Facilities (https://governance.admin.ox.ac.uk/legislation/it-regulations-1-of-2002).

8. Review and Development

8.1 This policy and supporting information security documentation will be reviewed annually by the IT Manager and Data Protection Officer, with any required updates to be approved by Governing Body to ensure that they remain operationally fit for purpose; reflect changes in technologies; are aligned to relevant good practice; and support continued regulatory, contractual and legal compliance.

This policy was reviewed and approved by Governing Body on 16 October 2024