WEDNESDAY 20 JULY 2016 • SUPPLEMENT (1) TO NO 5140 • VOL 146

Gazette Supplement

UNIVERSITY OF OXFORD

Information Security

Information Security Policy

Approved by Council on 11 July 2016

The following policy supersedes the existing Information Security Policy (Supplement (1) to *Gazette* No 4998, 20 September 2012).

Purpose

This policy outlines the University's approach to information security management and provides the guiding principles and responsibilities to ensure the University's information security objectives are met.

Scope

This policy is applicable across the University and individually applies to:

- all individuals who have access to University information and technologies;
- all facilities, technologies and services that are used to process University information;
- information processed, in any format, by the University pursuant to its operational activities;
- internal and external processes used to process University information; and
- external parties that provide information processing services to the University.

Objectives

The University's objectives for information security are that:

- a culture is embedded to ensure all teaching, research and administration activities consider information security;
- individuals are aware and kept informed of their information security responsibilities;
- information risks are identified, managed and mitigated to an acceptable level;
- authorised users can securely access information to perform their roles;
- facilities, technologies and services adequately balance usability and security;
- implemented security controls are pragmatic, effective and measurable;
- contractual, regulatory and legal obligations relating to information security are met; and
- incidents are effectively managed and resolved, and learnt from to improve our control environment.

Information Security Policy Framework (ISPF)

Information is critical to University operations and failure to protect information increases the risk of financial and reputational losses. The University is committed to protecting information, in all its forms, from loss of **confidentiality**, **integrity** and **availability** ensuring that:

- all staff complete information security awareness training;
- information security risk is adequately managed and risk assessments on IT systems and business processes are performed where appropriate;
- all relevant information security requirements of the University are covered in agreements with any third-party partners or suppliers, and compliance against these is monitored;
- appropriate information security controls are implemented to protect all IT facilities, technologies and services used to access, process and store University information;
- all information security incidents are reported in a timely manner via appropriate management channels, information systems are isolated, and incident properly investigated and managed;
- Information Asset Owners are identified for all University information assets, assets are classified according to how critical and sensitive they are, and rules for their use are in place; and
- information security controls are monitored to ensure they are adequate and effective.

To provide the foundation of a pragmatic information security framework, the University will define and implement a set of minimum information security controls, known as the baseline, set out in topic specific information supporting documentation. Where research, regulatory or national requirements exceed this baseline, there is flexibility to increase control at a departmental or project level. The baseline will support the University in achieving its information security objectives.

The policy and the baseline shall be communicated to users and relevant external parties, and are available via the information security website.

Responsibilities

The following bodies and individuals have specific information security responsibilities:

- **Council** has executive responsibility for information security within the University. Specifically Council is responsible for determining the system of internal controls operated by the University and for monitoring the adequacy and effectiveness of the control environment. The Security Subcommittee of the General Purposes Committee has responsibility for overseeing the management of the security risks to the University's staff and students, its infrastructure and its information.
- **Joint Information Security Advisory Group** (JISAG) has the responsibility to develop and maintain the information security policy framework, review reports on compliance, provide support and guidance, escalate risks and issues, and provide recommendations to the University.

- **Chief Information Security Officer** (CISO) is responsible for establishing and maintaining the University's information security management framework to ensure the availability, integrity and confidentiality of the University's information. The CISO will define and implement the University's information security strategy and lead operational and improvement programmes.
- **Information Security Team** is responsible for maintaining and monitoring compliance against the University's information security policy framework. The Information Security Team will provide services to the University to support a collaborative approach to reducing risks associated with processing University information. The Information Security Team will create and maintain topic specific information security content to support the implementation of information security controls in accordance with the policy framework.
- **Heads of Division** are responsible for the oversight of information security arrangements for departments or faculties within their division in order to ensure that they are functioning in accordance with this policy.
- **Heads of Department and Faculty Board Chairs** are responsible for the effective implementation of this information security policy, and supporting information security rules and standards, within their department or faculty.
- **Users** are required to complete information security awareness training and are responsible for making informed decisions to protect the information that they process.

Compliance

The University shall conduct information security compliance and assurance activities to ensure information security objectives and the requirements of the ISPF are met. Wilful failure to comply with the policy and baseline will be treated extremely seriously by the University and may result in enforcement action on a department and/or an individual.

Review and Development

This policy, and supporting ISPF documentation, shall be reviewed and updated by JISAG on an annual basis to ensure that they:

- remain operationally fit for purpose;
- reflect changes in technologies;
- are aligned to industry best practice; and
- support continued regulatory, contractual and legal compliance.

Information Security Strategic Plan

Vision

The implementation of this Strategic Plan will enable the development and operation of a fit-for-purpose and effective information security framework that enables the University to deliver against its strategic aims by:

- managing information security risk, legal and external compliance requirements to protect the University's brand and reputation;
- supporting the delivery of the IT Strategic Plan and the implementation of the University's strategy to enable staff and students to use IT and other services with confidence;
- using information security as an enabler to develop and sustain strong industry partnerships and collaboration with other institutions;
- emphasis on information security service excellence to provide a pragmatic, flexible capability and capacity to service the University's requirements and facilitate the ease of implementation of IT projects and services; and
- widening engagement to build relationships across the sector and broader community and supporting the University's focus on apprenticeships.

Staff and students will have the support and resources to allow information security to be easily implementable and greater support to resolve queries and issues. Obtaining data from external sources will be straightforward as the University can easily demonstrate the robustness of its information security arrangements.

These features combine to result in an improved student and staff experience, reflecting the need for research collaboration and increasing compliance requirements, and the confidence to implement new and emerging technology and ways of working in an internationally leading University.

Information Security Strategic Plan

The Information Security Strategic Plan sets out the three-year vision of how information security will support the University in delivering its objectives in a secure manner. The Information Security Strategic Plan covers the following areas:

- research and teaching;
- administrative systems and IT infrastructure;
- widening engagement; and
- information security service excellence.

For each area within the Information Security Strategic Plan there is a set of objectives. Given the rapidly evolving nature of information security risk together with rapid change in IT technologies and an evolving legislative landscape, it is not possible to predict everything we might need to achieve within a four-year period and hence the objectives are purposely set at a high level. An annual review of the Information Security Strategic Plan should not change the objectives, but is likely to adapt and add to the activities that have been identified through consultation with the collegiate University.

We will monitor progress against our objectives using relevant performance indicators, benchmarks and targets. This will ensure we maintain focus on the Information Security Strategic Plan so that it continues to meet academic needs, enables us to respond to the changing external environment and is updated as appropriate. The Information Security Strategic Plan will support, and be supported by, the IT Strategic Plan.

Objectives and Activities

RESEARCH AND TEACHING

Increasingly, research is performed by interdisciplinary teams, often distributed across institutions or countries. The information, in any format, used or produced as part of research activity may include sensitive data or intellectual property that must be stored, processed and transferred securely.

The security of digital technologies that are used for the planning, sharing and communication of teaching materials, delivery of lectures and tutorials and support of learning activities is essential to ensure staff and students have confidence in the technologies used.

Objectives

1. To enable secure IT infrastructure and tools that allow researchers to be compliant with regulatory requirements and enable them to share and store electronic research outputs securely.

2. To support the secure development and adoption of new technologies and tools to support Oxford's teaching practices.

3. To facilitate the secure delivery of the University's Digital Strategy.

Activities

1. Develop an information security management system, based on international good practice, to enable the University to easily respond to legal, regulatory, research and funding requirements.

2. Create pragmatic, academic-focused tools and collateral that allow staff to operate in a secure manner both globally and locally.

3. Generate confidence in technology and new ways of working through improvement in security, privacy standards and the provision of robust information security services and related training.

4. Create a secure staff and student experience, including distance and remote learners.

5. Enable the identification, classification and protection of research and teaching information assets.

6. Provide information security support and guidance that encourages and supports innovation in research and teaching.

ADMINISTRATIVE SYSTEMS AND IT INFRASTRUCTURE

The University administrative systems provide a technology platform that enables administrative support for all functions of the University. These systems contain sensitive information and require robust information security arrangements. A secure IT environment will enable the University to deliver robust and resilient services to students and staff and achieve its compliance requirements.

Objectives

4. To enable secure and easily used IT infrastructure and services that allow both the secure management and sharing of information across the University.

5. To be responsive to the information security requirements of the University.

Activities

1. Embed security by design in to all IT projects and services.

2. Provide information security guidance, tools and technologies that encourage confidence in University systems.

3. Improve IT security controls across the University to enhance the security of information systems and IT infrastructure.

4. Implement appropriate information security arrangements in key administrative functions including but not limited to purchasing, finance and personnel.

5. Enable the identification, classification and protection of administrative information assets.

6. Support the response to, and management of, the University's legal and regulatory information security compliance requirements.

WIDENING ENGAGEMENT

Widening engagement is a priority within the University Strategic Plan. A major aspect of the Information Security Strategic Plan is collaborative working with a range of organisations including other Universities, cyber security research groups, industry and the wider community. Additionally, the Information Security Strategic Plan will facilitate greater engagement with the public and local community.

Objectives

6. To build and leverage strong information security relationships with a range of organisations in Higher Education, the information security industry and the wider community.

7. To support the sharing and dissemination of information security knowledge and good practice across the information security community.

8. To support the University in developing a stronger and more secure digital presence.

Activities

1. Develop strong relationships and collaborative working with other information security teams in the Higher Education and wider information security sectors.

2. Introduce information security apprenticeships to both provide jobs and training and ensure the ongoing development of information security resource for the University and wider community.

3. Provide confidence in the University's digital presence by securing online and social media channels.

4. Collaborate with IT support staff at other collegiate Universities, Russell Group incident response teams, cyber security research groups and the wider information security community to share information security knowledge and good practice.

INFORMATION SECURITY SERVICE EXCELLENCE

The University desires a culture that drives excellence in information security and ensures that information security is embedded in day-to-day activities across the University. Information security is an enabler that that will help IT Services and the wider University deliver services that are efficient, robust, secure, fit for purpose and ensure that the University meets its compliance requirements.

Objectives

9. To ensure information security is an enabler, supporting the delivery of University objectives and initiatives.

10. To develop an information security function that has the capability and capacity to deliver information security service excellence.

11. To develop a strong information security culture across the University through education, awareness and collaboration.

Activities

1. Establish a highly visible information security team that is recognised as a centre of excellence within the University and that provides responsive information security services.

2. Recruit and retain specialist technical and non-technical information security staff and build and develop management and leadership capability.

3. Improve information security services through engagement with staff, students and the wider information security community, and build an information security network across the collegiate University.

4. Demonstrate value for money in terms of team and service efficiency and effectiveness.

5. Promote personal responsibility for information security through education and awareness training.

6. Provide information security input to positively impact on non-academic IT and business process decision making.

7. Develop a proportionate, pragmatic and flexible approach to information security which facilitates the delivery of University objectives.

8. Improve Oxford Computer Emergency Response Team (OxCERT) capability thorough the implementation of improved threat intelligence, network monitoring, incident response, reporting and forensic capabilities to improve the detection, response and reporting of information security incidents.