Departmental Information Security Policy

Purpose

The Department of Statistics' computer and information systems underpin all departmental activities and are essential to our research, teaching, and administration. The department recognises the need for its members, employees, and visitors to have access to the information they require to carry out their work and the role of information security in enabling this.

The departmental Information Security Policy relates to information stored and processed digitally, as well as hard copy information storage and processing. Information security must therefore be an integral part of the department's management structure to maintain continuity of its business, legal compliance, to avoid financial and reputational losses, and adhere to the University's central Information Security Policy.

The departmental information security policy defines the framework within which information security will be managed across the department and demonstrates management direction and support for information security throughout the department. This policy is the primary policy under which all other technical and security related polices reside.

Scope

This policy is applicable to:

- all departmental staff, students, and other relevant parties;
- visitors and contractors;
- external parties that provide information processing services to the department;
- Internal and external processes used to process departmental information;
- all facilities, technologies and services that are used to process departmental information;
- information processed in any format by the department.

Objectives

The overall information security objectives are that:

- the department is committed to protecting the security of its information and information systems;
- the department is committed to a policy of education, training, and awareness for information security;
- business continuity is ensured;
- appropriate legal, regulatory, and contractual compliance is ensured;
- authorised users can securely access information to perform their roles;
- incidents are effectively managed and resolved.

Procedures and practices

To determine the appropriate level of security control that should be applied to information systems, a process of risk assessment shall be carried out to define security requirements and identify the probability and impact of security breaches. Specialist advice on information security shall be made available throughout the department and advice can also be sought via the University's Information Security Team.

Information security requirements are covered in agreements with third-party partners or suppliers, and these must be monitored for compliance by the IT team or the owners of the business.

Reporting

It is the department's policy to report to the Head of Department all information security or IT security incidents, or other suspected breaches of this policy. The department will follow the University's advice for the escalation and reporting of security incidents and data breaches that involve personal data will subsequently be reported to the University's Data Protection Officer. Records of the number of security breaches and their type should be kept and reported on a regular basis to the Computing Manager and Chair of the IT Committee.

Systems security

All systems within the Department must comply with the University's 'baseline' information security standards. Additional controls must be implemented where confidential information is stored or processed.

Any IT facilities within the department must have appropriate environmental and physical security arrangements in place. All departmental computing systems must be regularly kept up to date and have appropriate anti-malware software installed. To comply with the University's Security Policy, all laptops bought through the department will be encrypted.

The department also requires that Sophos Endpoint and Tanium are installed on machines containing information relating to employment by the University.

Account Access

All IT user accounts should have appropriately strong passwords and should not be automatically logged on. User accounts, including email logins, must not be shared between users. Failure to comply will result in account suspension. If passwords are to be stored, these must be kept in secure Password Managers or Password Vaults. As far as can be implemented, access credentials must be secured with appropriate Multi-Factor Authentication (MFA) methods. Risks associated with any services that are accessible by non-MFA credentials, including local VPN services must be managed and minimised.

Email is not a secure form of communication. If confidential data is to be sent, then extra precautions are required, such as using encryption and password protection. Passwords must be shared by an alternative method to email, e.g. Microsoft Teams, phone, or SMS.

Access to Files

Users of the computing facilities of Department of Statistics may not access other the files of other users without explicit permission from the owner of the files. All users' files are considered private to them in this respect, even from system administration and Departmental staff except as indicated below.

Systems Administration or Departmental Staff are authorised to look at any files owned by any user of departmental facilities under their control when investigating a breach, or suspected breach, of the relevant law and regulations such as the Data Protection Act, the Computer Misuse Act, or any other such Act or Rule, or when required to do so for legal reasons. Such access will be made with the knowledge of the owners of the files where possible except in emergencies. The Head of Department should be urgently contacted and kept informed.

Security Incidents

All information security incidents must be reported immediately via appropriate management channels, information systems must be isolated, and the incident thoroughly investigated and managed. Two people should be present for any investigation involving a suspected data breach. OxCERT should also be contacted immediately to ensure they are aware and to provide advice and guidance. If you suspect a breach involving personal data has occurred then email the Information Compliance Team (ICT). You should do this **in addition** to contacting OxCERT, not instead of doing so.

Using your own device

If you wish to use your own device for purposes related to University business, then you must follow the central IT team's advice. In particular, your system must be kept up to date, with an appropriate firewall and virus protection software, and you should take reasonable precautions to prevent malicious code from being run.
This Information Security policy will be reviewed annually to ensure it reflects changes in technology, risks and converges towards international security standards.

Responsibilities

The following bodies and individuals have specific information security responsibilities:

- **Head of Department** is responsible for the effective implementation of this policy and for compliance within the department.
- **IT Committe** are responsible for reviewing this policy on an annual basis. They will provide clear direction, visible support and promote information security through appropriate commitment and adequate resourcing.
- **Department Computing Manager** and **computing staff** are responsible for the management of information security and, specifically, to provide advice and guidance on the implementation of this policy, and

to support a unified and collaborative approach to reducing risks to personal information, research data, operational systems around.

- **Line managers and supervisors** are responsible for the implementation of this policy within their area of responsibility and to ensure that all staff and students for which they are responsible are 1) made fully aware of the policy; and 2) given appropriate support and resources to comply.
- **Staff and students** each have the responsibility to adhere to this policy, and to complete the mandatory Information Security and Data Protection training course, annually, to ensure the department and the University are compliant with UK Data Protection legislation. They are responsible for making informed decisions to protect information, including datasets for research and teaching and all other university documentation. They are also responsible for reporting incidents promptly.

Compliance

This policy should be read in conjunction with related policies and regulations, including:

- Data Protection Policy
- University central Information Security Policy
- Laws and regulations relating to the use of Information Technology facilities.

Enforcement

Failure to comply with this policy that occurs as a result deliberate, malicious, or negligent behaviour, may result in disciplinary action.

Review and Development

This policy will be reviewed and updated by the IT Committee annually. The next review is due in Michaelmas 2025