Information Security Policy

Title:	Information Security Policy
Reference:	ISM-POL-001
Issue:	7
Document owner:	John Chapman, Director information security policy and governance
Authorised by:	Heidi Fraser-Krauss, CEO
Date:	2 October 2023

Document control

1. **Superseded documents:**
   ISM-POL-001, Issue 6, dated 31/10/22.

2. **Changes made**
   Updated to reference new Third Party use of assets policy and changed information classification to Public.

3. **Changes forecast**
   The Quality and Information Security Management Board (QISMB) will review this document at least annually to monitor its performance so that it continues to meet the needs of the organisation. The certification scope is expected to change more frequently and is documented in ISM-NOT-006.
   Jisc will be transitioning to ISO27001:2023 in 2024, which may require minor changes to this document.

Public

This document becomes UNCONTROLLED if printed or when held in any other location other than the QMS or ISMS

1. Purpose

Jisc senior management commits to security of information owned by or entrusted to the organisation and has established an Information Security Management System (ISMS) which conforms with, and exceeds, the ISO/IEC 27001:2013 standard. The standard sets out a minimum set of requirements for an ISMS, by exceeding these requirements the ISMS becomes an effective system built to meet Jisc's requirements.

Information security is defined as the appropriate protection of the confidentiality, availability and integrity of information.

- ***Confidentiality*** means that only those authorized can access and view information, preventing it from deliberate or accidental disclosure to all others.
- ***Integrity*** means protecting the accuracy and completeness of information from deliberate or accidental alteration, modification or destruction by authorized and unauthorized users.
- ***Availability*** means that information is accessible to authorized users when required.

2. Scope

The scope of the Information Security Management System covers the entire Jisc group of companies. However, the ISO 27001 certification scope is smaller than this and is detailed in ISM-NOT-006.

All employees, consultants and contractors handling information assets of the group are required to be aware of this policy.

3. Context

Jisc has considered the context and interested parties of its ISMS. The organisation must as a *minimum* meet its legal, regulatory and contractual information security requirements. In particular we must comply with current data protection legislation. More information on this can be found in QS-DOC-044.

4. Objectives

The objectives of the ISMS are set by the Quality and Information Security Management Board (QISMB) and reviewed on an annual basis as part of the ISMS management review.

5. Method

To meet these objectives Jisc will provide the means to identify, assess, evaluate, control and manage risks to the security of information in robust, repeatable and proportionate fashion. The approach will be aligned to the organisation's risk management processes and conform with the requirements of ISO 27001. The processes that support these tasks and those of the ISMS itself will be subject to continual review and improvement as required by ISO 27001 and our ISO 9001 Quality Management System. Jisc publishes policies, guidelines, work instructions and other material in support of these activities on SharePoint.

6. Responsibilities

All employees, consultants and contractors must comply with this policy and those of the ISMS. We will provide training and instruction for them to do so. Any breaches of this policy or any information security incidents must be reported to the Information Security Team as soon as is practical.

Some employees will be identified as responsible for specific risks and security activities. Jisc will provide them with training and instruction, and they are responsible for fully engaging with the ISMS.

Violations by employees can be dealt with under the disciplinary policy.

7. Suppliers, Contractors and Partners

This policy can also create requirements for our suppliers, contractors and partners. This document may be shared with them, and appropriate support and guidance provided to help find mutually acceptable solutions. Third parties are also expected to be aware of ISM-POL-009 “Third party acceptable use of Jisc’s assets policy”. For particularly sensitive activities, Jisc will only use suppliers that provide equivalent security to Jisc. Contract managers are responsible for ensuring that compliance with this policy is a requirement of contracts and for bringing this policy to the attention of any contractors. For more information see ISM-POL-007 “Information Security Policy for supplier relationships”.

8. Related Documents

ISM-POL-002 Access Control Policy

ISM-POL-003 Secure Working Practices Policy

ISM-POL-004 Cryptography Policy

ISM-POL-005 Backup Policy

ISM-POL-006 Secure Development Policy

ISM-POL-007 Information Security Policy for supplier relationships

MF-POL-060 Acceptable use of assets policy

ISM-POL-009 Third party acceptable use of Jisc’s assets policy

QS-DOC-044 Context for Jisc’s Quality and Information Security management systems

ISM-NOT-006 ISMS Certification Scope