

Information Security Policy

1. Introduction

This is the top level Information Security policy in the British Library, and forms part of the Library's Information Risk Management framework. The guiding principles and axioms described in this policy will provide the basis for the Library's development of more detailed information security policies, procedures and guidelines designed to manage specific security issues as they arise.

2. Definitions

- **CIGG** – the Library's Corporate Information Governance Group – this Group is charged with the task of raising the profile of, and coordinating, the Library's work on information governance. This includes information security.
- **Information Asset** - includes information itself in the form of computer data and print/non-print written materials. Also includes our IT systems and networks that store, process and communicate the electronic information that we hold.
- **Information Asset Owners** - managers held accountable for the protection of particular Information Assets.
- **Information Security** - the protection of information assets against threats to their confidentiality, integrity and/or availability.
- **ISO/IEC 27000 series** – this comprises information security standards published jointly by the International Organisation for Standardisation and the International Electrotechnical Commission.
- **ISO/IEC 27002** – this standard was originally published as ISO/IEC 17799:2000. It was subsequently renumbered ISO/IEC 27002:2005 in July 2007, bringing it into line with the other ISO/IEC 27000-series standards. It is entitled '*Information technology – security techniques – Code of practice for information security management*'. The current standard is a revision of the version first published by ISO/IEC in 2000, which was a copy of the British Standard 7799-1:1999.
- **Systems Development Life Cycle** – the process of creating or altering IT or information systems, and the models and methodologies that people use to develop those systems.

3. Guiding principles

Seven fundamental information security principles underpin our approach to information security:

- A. Our approach to information security management conforms to accepted best practice as defined by the ISO/IEC 27000-series and other relevant information security standards.
- B. Information is a critical business asset of the British Library and must be protected to a degree appropriate to its vulnerability and its importance or value to the Library.
- C. Information security controls are necessary to protect our information assets against unacceptable risks to their confidentiality (e.g. preventing unauthorised disclosure of sensitive corporate or personal information), integrity (e.g. ensuring that human errors and programming bugs do not reduce the completeness or accuracy of our data) and availability (e.g. minimizing unplanned system downtime consequent interruption of critical business processes).

- D. We invest wisely in proven information security controls where justified on the basis of lifecycle cost-benefit assessment and risk analysis. Our goal is not completely to eliminate information security risks but to minimize them in the most cost-effective manner, offsetting the cost of controls against the anticipated reduction in losses due to avoiding or mitigating security incidents.
- E. Information security is pervasive throughout the entire organisation. It is an inherent part of our IT architecture and a component of our operational and management processes. In short, we are *all* responsible for information security.
- F. Information security is a core element of corporate governance. It is closely related to aspects such as IT management, physical site security, risk management, legal and regulatory compliance and business continuity. It supports various obligations to our employees, business partners and to the community at large.
- G. Information security is a business enabler that allows us to enter more confidently into and maintain business relationships, markets and situations that would otherwise be too risky. By minimizing net losses resulting from information security incidents, it supports our financial bottom line. It also enhances our image as a trustworthy, open, honest and ethical organisation.

The scope of this policy excludes managing the security of the Library's Collections, which is the responsibility of the Collection Security Group. This policy nonetheless recognises that there are substantial overlaps between the security of the Library's own information as recorded in our electronic systems and the security of the Collection Items that we hold in trust for the nation, particularly in the digital domain. The security of any information systems holding digital Collection Items will by default be managed in accordance with this policy and with other policies specifically related to the ingest, storage, access and preservation of digital Collection Items.

4. Axioms

The following 39 information security axioms correspond directly to the 39 control objectives identified in ISO/IEC 27002:2005.

- Axiom 1: Information Security policies, procedures and guidelines provide a framework for managing information security risks. Their purpose is to communicate management's policies for the protection of information assets and to promote the consistent and appropriate application of information security throughout the organisation.
- Axiom 2: A structured management framework is needed to direct, monitor and control the implementation of information security as a whole within the Library
- Axiom 3: Third party access to the Library's facilities and information assets must be restricted to authorised hardware, software, organisations, people and purposes
- Axiom 4: Information Asset Owners must be identified to be held accountable for the protection of all significant information assets
- Axiom 5: Information assets must be risk assessed according to the British Library's information security requirements
- Axiom 6: Information security responsibilities must be addressed during pre employment screening, included in employment contracts, and monitored by management during an individual's employment
- Axiom 7: Workers must be made aware of and motivated to comply with their obligations under these information security policies plus the associated standards, procedures, guidelines, laws and regulations
- Axiom 8: A worker's exit from, or change of status within, the Library must be properly managed and controlled such that information assets are retrieved and information access rights are promptly revoked where no longer justified
- Axiom 9: Information assets must be housed securely and protected against identified risks

- Axiom 10: IT equipment and storage media must be physically protected from security threats and environmental hazards to prevent loss, damage or compromise of information assets and interruption to business activities
- Axiom 11: Responsibilities and procedures for the management of all information processing facilities must be documented to ensure the correct and secure operation of information processing facilities
- Axiom 12: IT outsourcing contracts must address the risks, security controls and procedures for information systems and the associated operating procedures
- Axiom 13: Management of information systems must ensure the availability of adequate capacity and resources
- Axiom 14: Information systems, software and data must be protected against the risks relating to malicious software
- Axiom 15: Routine backup procedures and controls must maintain the integrity and availability of IT services, and protect the confidentiality of data on backup media
- Axiom 16: The British Library's networks must be protected from unauthorised access and other information security risks to confidentiality, integrity and availability
- Axiom 17: Data storage media must be suitably protected against damage, theft or loss
- Axiom 18: Information exchanged with other organisations must be protected against unauthorised access or disclosure and must comply with relevant legislation and regulations
- Axiom 19: The particular information security requirements relating to e-commerce must be taken into account
- Axiom 20: Systems must be monitored to detect and record security events and trigger suitable responses
- Axiom 21: Access to information assets must be granted to authorised persons based on business and security requirements
- Axiom 22: Access to networks, systems and applications must be authorised based on business need and security requirements throughout the Systems Development Life Cycle
- Axiom 23: Users are responsible for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment
- Axiom 24: Access to the British Library's network must be limited to authorised users according to business need and information security policies
- Axiom 25: Operating system security facilities must be used to authenticate users and control access to information assets
- Axiom 26: Logical security controls within application systems must restrict access to data and program functions to authorised users
- Axiom 27: The British Library's information assets must be protected when outside the premises, or when accessed remotely
- Axiom 28: Information security must be taken fully into account throughout the entire Systems Development Life Cycle
- Axiom 29: Suitable controls must be designed into applications to ensure the completeness, accuracy and integrity of data, satisfying information security requirements
- Axiom 30: Cryptographic controls must protect the confidentiality and/or integrity of information not adequately protected by other controls
- Axiom 31: Access to system files and program source code must be limited according to legitimate business needs
- Axiom 32: All system changes must be reviewed before implementation to verify that changes do not compromise the confidentiality, integrity and availability of information and systems. All support access must be based on business need and least privilege.
- Axiom 33: Technical vulnerabilities in operating systems and applications must be managed systematically
- Axiom 34: Security incidents must be reported promptly through the correct management channels and resolved by suitable professionals
- Axiom 35: Information security incidents and improvement suggestions should be managed consistently and effectively, using forensic evidence where necessary

- Axiom 36: Systems should be sufficiently resilient to ensure the continuity of critical business processes despite minor incidents, and should have proven disaster recovery arrangements in place to minimize the business impacts of serious incidents
- Axiom 37: The British Library must comply with all applicable legal, regulatory and contractual obligations relating to information security
- Axiom 38: The security of information systems must be regularly reviewed to ensure compliance of systems with the British Library's information security policies and standards
- Axiom 39: IT audits must be performed by independent and competent auditors.

5. Roles and responsibilities

The British Library Board is ultimately accountable for corporate governance as a whole. The management and control of information security risks is an integral part of corporate governance. In practice, however, the Board explicitly delegates executive responsibilities for most governance matters to the Executive Team, led by the Chief Executive.

The Executive Team has appointed a Senior Information Risk Officer (SIRO). The SIRO is responsible for leading the work of the Corporate Information Governance Group which is charged with the task of raising the profile of, and coordinating, the Library's work on information governance.

This policy applies throughout the British Library as part of the library's Information Risks Management framework. It applies to all of our employees and those of third party organisations acting in a similar capacity (e.g. working on site on joint projects or maintenance and support activities), whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of acceptable behavior) to comply with our information security policies.

A related document 'Organisation of Information Security' provides full details about roles and responsibilities related to information security.

Review

The Executive Team is responsible for the review of the Information Security Policy. This policy will be reviewed every three years.