London Business School

Information Security Policy

Audience: This document is for anyone who stores, handles, or processes London Business School information or data or uses the School's technology or systems.

Document Owner: Information Security Manager

Release Date: v.2.0, February 2024

Contents

1. Introduction

Information is a critical asset to London Business School. Regardless of the form it takes, or how it is stored or shared, it should always be appropriately protected. This applies to information in many different forms; electronically stored or transmitted, printed, shown in presentation and video, online or spoken in conversation. The confidentiality, integrity, and availability, of the School's information is essential to the success of its academic and administrative activities.

The purpose of this policy is to outline the information security requirements and objectives for protecting the School's systems, information, and data.

2. Scope

This policy covers all information assets and IT resources used by the School.

The policy applies to all faculty, staff, participants, students, and alumni, and any individual or third-parties contracted by the school to provide services or who handles or processes School data.

The policy relates to the use of IT devices, when connected to the School's network directly or indirectly; to all School-owned information assets or those on private systems, and to all information services provided to or by the School, by or for external agencies.

Supporting policies, standards, and procedures are considered part of this information security policy suite and have equal authority. Guidelines are provided for additional information.

3. Information Security Objectives

The School's objectives for information security are based on the requirements of ISO27001 along with recommended industry practise. This policy, together with the procedures and controls that support it, provides the framework for an information security management system (ISMS) that:

- Protects the confidentiality, integrity and availability of information and data appropriately for the purpose of London Business School.
- Meets regulatory, legal, and contractual requirements.
- Is committed to and supported by the School's management, regularly reviewed, and continuously improved.

Information security policy and related topic-specific policies and standards shall be defined, approved by management, published, communicated to, and acknowledged by, relevant personnel and relevant interested parties, and reviewed at planned intervals or sooner if significant changes, or security related incidents occur.

All faculty, staff, participants, students and relevant third parties are to apply information security practices in accordance with the established information security policy, related topic-specific policies, standards, and procedures of the organisation.

4. Information Security Policy

The following section outline's the School's information security policy:

4.1 Information Security Governance

4.1.1 Information security objectives are defined and supported by management.

4.1.2 A framework for the management of information security is defined and embedded.

4.2 Compliance & Assurance

4.2.1 Regulatory, legal and compliance requirements for information security are identified and communicated.

4.2.2 Assurance activities are undertaken to ensure information security objectives are met.

4.3 Employee Security

4.3.1 Information security roles and responsibilities are documented and compliance with them is a contractual obligation.

4.3.2 Employees, contractors and relevant third parties are subject to pre-employment screening and must complete mandatory information security training.

4.4 Asset & Data Management

4.4.1 All data and information processing systems and services must have an identified owner who is accountable for ensuring that data is processed, and the service is operated in accordance with the School's legal, regulatory and compliance requirements.

4.4.2 There is a documented approach to data asset identification, data classification and information handling.

4.4.3 Data is protected within its information system boundaries by technical controls and cryptographic controls in accordance with the classification scheme.

4.4.4 Assets storing School information are securely wiped prior to re-use and are disposed of securely when no longer required.

4.4.5 Data is protected and handled in compliance with applicable laws, regulations, and contractual requirements.

4.4.6 Inventories for the management of the School's information and other associated assets are maintained.

4.4.7 Individuals must return to the School all School-owned equipment, information, and data assets in their possession upon change or termination of their employment, contract, or agreement.

4.5 Third Party Security

For the purposes of this policy, third parties include, but are not limited to, service providers (including 'cloud' service providers'), contractors providing services to the School, either individuals or corporate, research partners and collaborators, and others.

4.5.1 Processes and procedures to manage information security risks associated with the use of third-party products or services are documented and implemented.

4.5.2 Third party management processes and procedures ensure products and services are monitored and managed throughout the contract lifecycle and meet information security requirements.

4.5.3 Third-party contractual arrangements meet the School's legal, regulatory and compliance requirements.

4.6 Physical & Environmental Security

4.6.1 The School's physical environment has security measures in place to protect all systems and data from unauthorised access or damage.

4.6.2 All IT facilities and equipment are protected by appropriate environment and physical security arrangements, and are maintained to ensure the confidentiality, integrity, and availability of information.

4.7 Incident Management

4.7.1 Information security management procedures are implemented to ensure incidents are detected and reported.

4.7.2 Information security incident response procedures are implemented to ensure incidents are assessed and handled to reduce their impact and to ensure they are communicated appropriately.

4.7.3 Information security incidents are reviewed to strengthen and improve information security controls.

4.8 Identity and Access Management

4.8.1 Rules to control physical and logical access to information and other associated assets are established and implemented based on the principle of least privilege and business and information security requirements.

4.8.2 There are processes and procedures in place to manage and audit identities and authentication information throughout their lifecycle.

4.8.3 Secure authentication technologies and procedures are implemented.

4.9 Network & Secure Configuration

4.9.1 Networks and network devices are secured, managed, and controlled to protect information in systems and applications.

4.9.2 Security mechanisms, service levels and service requirements of network services are identified, implemented, and monitored.

4.9.3 Networks are segregated according to service and information sensitivity and criticality.

4.9.4 Rules for the effective use of cryptography, including cryptographic key management, are defined, and implemented.

4.9.5 Configurations, including security configurations, of hardware, software, services, and networks is established, documented, implemented, monitored, and reviewed.

4.10 Logging, Monitoring & Alerting

4.10.1 Audit logs of events that could help to detect, understand, or recover from an incident are collected, protected, managed, and analysed.

4.10.2 There are defined and implemented procedures for the identification, collection, acquisition, and preservation of evidence related to information security events.

4.10.3 Access logs from physical buildings, offices and other premises are captured and monitored for unauthorised physical access.

4.10.4 Networks, systems, and applications are monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.

4.11 Secure Development

4.11.1 Information security requirements are identified, specified, and approved in the lifecycle of development.

4.11.2 Secure development standards and practices are defined and implemented.

4.11.3 Security testing processes and procedures are defined and implemented in the development life cycle.

4.12 Change Management

4.12.1 Changes to information processing facilities and information systems are subject to change management procedures.

4.13 Backup, Disaster Recovery and Business Continuity

4.13.1 Backup copies of information, software and systems will be maintained and tested in accordance with service requirements.

4.13.2 Business continuity plans and IT disaster recovery plans are maintained and tested in accordance with service requirements.

4.14 Threat and Vulnerability Management

4.14.1 All systems are under security support from the manufacturer or developer, or their approved partners.

4.14.2 There are processes and procedures to identify, evaluate and remediate IT vulnerabilities.

4.14.3 Information relating to information security threats is collected and analysed to produce threat intelligence.

4.15 Remote Working Device Management

4.15.1 Security measures are implemented to protect information accessed, processed, or stored outside the organisation's premises.

4.15.2 Security standards are applicable to all systems and devices with access to School information, including personally owned devices.

5. Roles and Responsibilities

Chief Digital and Information Officer (CDIO)

- The CDIO has accountability for the Information Security Management System (ISMS) and this supporting Information Security Policy. They must ensure compliance is met throughout the organisation.

Information Security Manager

- The Information Security Manager will have ultimate ownership of this policy and for ensuring that appropriate controls are defined and implemented throughout the organisation. The Information Security Manager will work closely with IT Services, Data Protection, HR, Finance, and other operational leadership to ensure the policy statements and supporting standards are both appropriate for the organisation and implemented throughout. The Information Security Manager will ensure that any exceptions to this policy, and associated

risks are documented but may not be responsible for the mitigation and remediation of those risks; that may lie with the operational leadership team(s).

Senior Data Privacy Manager

- Information Security has the guiding principles of protecting the Confidentiality, Integrity, and Availability of data. The Senior Data Privacy Manager is responsible for ensuring that this policy services the needs of protecting data in relation to privacy and the rights of faculty, staff and students but also ensuring that business critical data is protected.

Data Privacy & Security Committee

- Led by the CDIO this is a multi-disciplinary group that reviews, endorses, and supports the implementation of changes to the Information Security Policy and related standards and processes.

All LBS Employees, Faculty, Contractors, Students, Participants and Alumni

- All School Employees, Faculty, Contractors, Students, Participants and Alumni are responsible for complying with this policy.
- They are required to complete any training required to support the policy and are responsible for making informed decisions to protect London Business School's information and data assets.
- Line managers are responsible for ensuring that their staff adhere to this policy and to support them in doing so.

6. Compliance and Exemptions

Exemptions to this policy may be granted subject to the approval of the CDIO. All exemption requests shall be recorded along with their outcome.

London Business School shall conduct appropriate compliance and assurance activities to ensure objectives are being met. Reports may be made to the Management Committee, Senior Management Team, Management Board, Audit and Risk Committee and/or Governing Body, as required.

Non-compliance with this policy will be recorded, and remedial action will be taken, including but not limited to re-training, possibly including removal of access to IT assets, or disciplinary proceeding, up to and including termination of employment. Serious breaches may lead to criminal or civil proceedings.

7. Review and Continual Improvement

This policy shall be reviewed periodically by the CDIO and Data Privacy & Security Committee when there has been a significant change to the environment or business process to ensure that they:

- Remain operationally fit for purpose.
- Reflect changes in technologies or business processes.
- Are aligned to industry good practice; and
- Support continued regulatory, contractual, and legal compliance.

8. Document Control

Document Information

Title	LBS Information Security
Author	Information Security Working Group
Approver	Chief Digital & Information Officer; Data Privacy & Security Committee
Owner	Information Security Manager

Version History

Version	Date	Summary of Changes
Published	September 2021	Approved and published policy
2.0	February 2024	Full policy refresh