Responsible organization (Technology Organizational Unit) OneTrust ID 732

POLICY ON INFORMATION SECURITY MANAGEMENT

VERSION 1.0

APPROVED BY THE
EXECUTIVE COMMITTEE
ON 29 OCTOBER 2024

Università
Bocconi
MILANO

Guiding Principles of the Information Security Management

Bocconi University is committed to establishing, implementing, maintaining and continuously improving an Information Security Management System that is consistent with the University's strategic goals and processes. This system is developed in line with the ISO/IEC 27001 international standard, as well as current GDPR regulations and Legislative Decree 231/2001.

This document describes the objectives pursued, the manner in which the system has been developed, and the basic principles and rules for the control and management of information security. It also represents the University's commitment to protecting information with clearly identified and defined responsibilities and security measures.

This commitment helps to strengthen and maintain the University's credibility and reputation with its students, alumni, employees, donors and other business partners and stakeholders, including the public administration with which it interacts in continuous exchanges of data and information.

The principles that Bocconi University aims to adhere to, through its Information Security Management System, include:

- Ensuring the confidentiality of data so that it is available only to the processes and/or resources entitled to use it;
- Ensuring the integrity of information, applications, systems and networks by preventing unauthorized or accidental modifications;
- Ensuring the availability of information according to specific needs, enabling the continuity of processes.

These principles are set out in goals specified in dedicated documents, which are to be monitored and measured in order to ensure the Management System’s effectiveness.

The Management System complies with ISO27001 requirements and is structured through:

- The identification of roles and responsibilities involved in information asset protection activities;
- The adoption of a process to identify, assess and periodically monitor information security risks due to changes that have occurred in the internal and external technical-organizational environment, also in order to retrace the reasons for choices made over time;
- The definition of security protocols for asset and configuration management in order to ensure access to data according to the principle of least privilege;
- The establishment of guidelines for the protection of physical access to university premises and in particular to areas where servers and technical-information infrastructure are kept;
- The definition of logical security safeguards through a Security by Design process used while conducting various project initiatives;
- The definition of how to detect and manage possible information asset security incidents;
- The definition of useful safeguards to ensure continuity of the technology services provided in IT;

- The definition of instructions aimed at managing information security in accordance with operational requirements, business procedures and relevant external regulations including, but not limited to, GDPR, Legislative Decree 231/2001, etc.;
- The definition of a process to assess the suitability of third parties and the instructions and clauses to be included in agreements stipulated with them;
- The categorization and classification of information for the purpose of efficient planning of efforts and investments according to an objective, shared priority order;
- The definition of ways to raise awareness of behavior that affects information security, at the level of the university's senior management, directors and their collaborators.

These provisions are a point of reference for other lower-level regulatory documents that, in compliance with the principles outlined above, describe the precise security objectives, the organizational context of reference, the control principals provided by the ISO/IEC 27001 standard applicable to the University, and the Information Security Management System Manual in detail, as suggested by the best practices of reference to the standard itself. In addition, the Information Security Management System consists of additional detailed operational documents.

Scope of Application

The scope of the Information Security Management System (ISMS) includes the processes and activities managed by the university’s Staff Organizational Units reporting to the Managing Director. These processes and activities include management of the technical-application infrastructure, governance of processes and resources used in administrative activities, and also the conduct of processes to support teaching, learning, research and the third mission.

This provision covers all personnel, as well as the collaborators and suppliers involved in the specified activities. This document is distributed internally within the university and made available to stakeholders through the institution's internal and external communication channels. In addition, the document is subject to periodic revisions to ensure that it is always adequate, appropriate and effective with respect to the university's needs and to developments in the external environment.

With reference to activities related to academic production, these are decided under the full autonomy and self-regulation of the faculty that operates outside the scope of the Managing Director. In this context, the Information Security Management System is configured for faculty as a set of guidelines that – while needing to be respected – cannot be directly controlled by administrative Organizational Units that are subordinate to the Managing Director, in observance of the academic freedoms guaranteed to faculty.

Information Security Management System Leadership

The university's Information Security Management System is structured around two main areas of action:

- **Technical-Application Infrastructure Security**. This area focuses on protecting the IT infrastructure, including critical assets such as servers, networks and devices such as university-owned smartphones and laptops. Security measures applied include, for example, standards for setting and changing passwords, advanced authentication policies (e.g. multi-factor), network and communication security management, firewall configuration, secure information system development and controlling access to information systems.
- **Security Governance**. This area establishes personnel roles and responsibilities in the safe use of university-owned applications and assets, defining rules of conduct and organizational and process controls operated by University Staff Organizational Units. For example: verification of IT skills at the hiring stage, a ban on credential sharing, the requirement of accessing data and features only for work purposes, a ban on using unauthorized storage solutions, a ban on installing applications not authorized beforehand by the University and the requirement of adopting cryptographic measures when handling sensitive data.

Responsibility for promoting and developing the Management System, as well as for pursuing the actions described, lies with the Managing Director, who is also responsible for developing a culture of security in the Organizational Units that report to the same. This responsibility extends to all University administrative activities as specified in the Scope of Application.

The Managing Director makes use of the Organizational Units reporting to the same to implement the areas of action, assigning specific responsibilities by area of competence, particularly the Technology Organizational Unit which is responsible for the execution of any technological obligations. In this context, the Managing Director appoints an Information Security Management System Manager who will serve as a point of reference for the Technology Organizational Unit and other impacted Organizational Units, ensuring the effective development, monitoring and updating of the system.

The University is committed to promoting the continuous improvement of the ISMS by regularly reviewing and updating the system, policies and risk assessment procedures in response to any significant changes or the emergence of new security needs, thereby ensuring the adequacy and effectiveness of the system over time.

It is the responsibility of all personnel, as well as the collaborators and suppliers involved in the specified activities to act in accordance with the security requirements expressed in the Security Management System.

Disclosure to University Governance Bodies

The University Board, the Supervisory Body, and the Board of Auditors are periodically informed about the progress of activities, risk assessments and the implementation of safeguards put in place to mitigate them. The University Board is promptly informed in the event of any particular critical issues that jeopardize information security, business continuity or non-compliance with relevant regulations, including maintaining ISO 27001 certification.

The Supervisory Body, in particular, is informed in the event of any critical issues related to the risk of cybercrimes under Legislative Decree 231/2001 for circumvention of or failure to apply the safeguards defined by the Information Security Management System.