Do Good.
Do Better.

esade

www.esade.edu

Policy on Information Security and the Protection of Processed Personal Data

Do Good. Do Better.

Version tracking

Version	Date	Author	Revised by	Changes
2.0	September 2023	Technical Team, Security and Privacy Committee	Legal Services	Scope review

Approval

Governing body	Institution	Date	Signature
Director General's Office	Fundació Esade	September 2023	Approved by the Executive Committee

Content

1. Document objective

This document aims to provide norms and guidelines that the entire Esade community has to comply with in order to ensure the security of our information and protect the personal data processed by Fundació Esade from any possible incidents and a wide variety of security and privacy threats. Specifically, the objective is to:

→ Ensure the security of the operations carried out via Esade's IT systems;

→ Minimize the risk of damaging the information and data and prevent any undue access to personal data;

→ Ensure Esade's objectives are met; an

→ Ensure all currently valid norms and legislation are complied with.

Fundación Esade aims to ensure that data security and privacy policy principles are an integral part of its corporate culture. For this reason, it has implemented an Information and Privacy Security Management System (referred to collectively hereafter as "Information Management System" or IMS) based on the internationally recognized ISO27001 standard and its extension for privacy, the ISO27701 standard.

2. Scope

All Fundació Esade personnel, including employees, suppliers and executives have to be familiar with and duly comply with this Policy.

This Policy will be implemented by means of norms, procedures, instructions, guides, manuals and any other organizational tools deemed useful to achieve its objectives.

3. Legal Framework

This Policy meets all the requirements established in norms ISO 27001 and ISO 27701, section N05.1

4. Definitions

To ensure this Policy is interpreted correctly, the following definitions apply:

→ Information: Meaningful data in any format and included in any storage device; it refers to the content of all types of communications or representation of knowledge.

→ Personal data: Information which identifies individuals or makes it possible to identify them.

→ Information system: This refers to a set of related resources which are structured and organized to process data depending on certain procedures, whether computerized or manual.

5. Policy on Information Security and the Protection of Processed Personal Data

5.1 Policy objective

The primary objective of drafting and implementing this Information Security and the Protection of Processed Personal Data Policy is for Fundació Esade Management to guarantee to the users of its services that access to data and the latter's processing are secure and that respect for privacy is maintained for the services needed to carry out all that agreed on between the parties. Similarly, it also aims to avoid serious losses or alterations of the information as well as any unauthorized access to the latter. For this it will:

- → Develop policies, norms, procedures and operational guidelines to support the Information Security and the Protection of Processed Personal Data Policy.
- → Duly identify the information that has to be protected;
- → Establish a risk management system in line with the requirements of the IMS and Fundació Esade's strategy;
- → Define a methodology to assess and address these risks;
- → Establish criteria to be able to measure the IMS' degree of fulfillment;
- → Revise the IMS' degree of fulfillment;
- → Correct any non-fulfillment by implementing corrective measures;
- → Duly train its personnel and make them aware of information security and privacy issues;
- → Inform all personnel about their obligation to comply with the Information Security and the Protection of Processed Personal Data Policy.
- → Allocate the necessary resources to manage the IMS;
- → Identify and comply with all legal, regulatory and contractual requirements;
- → Identify and analyze the implications of information security and personal data privacy with respect to business requirements;
- → Keep track of metrics regarding the information security and privacy management system's degree of maturity; and
- → Continuously improve the IMS.

Fundació Esade's has created a framework to achieve its information and security objectives. It will accomplish the abovementioned goals by means of a series of organizational measures and concrete, clearly-defined norms.
The basic principles that have to be respected in terms of security and privacy are as follows:

- → Confidentiality: Only personnel duly authorized to access information processed by Fundació Esade may do so after duly identifying themselves at that specific time and by the means established for this.
- → Integrity: This guarantees the validity, accuracy and completeness of the information processed by Fundació Esade. The content of said information will be that duly provided by the corresponding individuals. Only authorized personnel will be permitted to modify said information.
- → Availability: The information will be accessible and usable in the agreed-on time intervals. The information managed by Fundació Esade is accessible and usable by duly authorized and identified clients and users, ensuring its permanence for any foreseen circumstance.
- → Privacy: This refers to protecting the privacy of students', faculty's and administrative staff's personal data processed by Fundació Esade as well as personal data of any external collaborators, ensuring that all applicable laws and regulations are complied with at all times.
- → Legality: Complying with current legislation.

Fundació Esade Management commits to allocate all the necessary resources to successfully achieve these objectives as well as periodically revise and monitor their fulfillment.

5.2 Scope

The scope of the Information Security and the Protection of Processed Personal data Policy coincides with the scope of the IMS:

"Information and privacy systems related to IT services which support Fundació Esade's educational, research and social debate processes in keeping with the latest scope o applicability".

The latter was approved by the Director General's Office and duly communicated to the entire organization. It is also available on the organization's intranet for consultation.

5.3 Roles and responsibilities

Fundació Esade has defined the roles and responsibilities of the people involved in managing the security and privacy of personal information and data at the university, from senior management positions to support personnel:

→ The Fundació Esade Director General's Office is responsible for approving this Policy.
→ The Chief Security Officer (CSO) is responsible for maintaining this Policy.

5.4 Risk management

Fundació Esade's holistic Information and Privacy Security Management System (IMS) includes a general process to assess and mitigate risks which could potentially affect the security and privacy of the information related to the services rendered. This process consists of the following:

→ Identify the threats that could potentially take advantage of the IT systems that support the services or on which the information's security and privacy depend.
→ Analyze the risks based on the consequences of said risks should they arise and the probability of those risks occurring.
→ Assess the risks according to previously established levels of risk: acceptable, tolerable or unacceptable.
→ Address unacceptable risks by means of the appropriate control mechanisms or safeguards.

This process is cyclical in nature and has to be carried out periodically, once a year at a minimum. An "owner" will be assigned to each identified risk, and a single person or committee may be responsible for several.

5.5 Training and awareness

With a view to supporting interested parties and helping them in their personal growth and improving information security and privacy, Fundació Esade has created a training program in this area as well as dedicated learning pills to raise greater awareness.

5.6 Audits

The Fundació Esade Director General's Office will carry out internal and external audits to guarantee and verify the degree of fulfillment of this Policy and determine if its guiding principles have been correctly implemented and put into practice. It also assumes responsibility for ensuring that the corrective measures defined to maintain the system's ongoing improvement are complied with.

5.7 Disciplinary measures

Failing to comply with this Information Security and the Protection of Processed Personal Data Policy and the other norms and procedures it encompasses will result in the application of disciplinary measures depending on the magnitude and type of non-compliance, all in keeping with current legislation.

5.8 Validity and modifications

This Policy will be considered valid the moment it is published and will be revised at least once a year.

The aim of these periodical revisions is to adapt the Policy to changes in the organization's context, both external and internal, analyzing the information security and privacy issues which may have arisen and any deficits identified within the IMS. These will also be compared and updated according to the results of the different risk assessment processes.

When revising this Policy, attention will also be paid to all the related norms and documents included, reviewing them periodically to update the Policy depending on the relevant changes which might occur at the organizational level due to any new services or infrastructures.

Fundació Esade has classified the information and will protect the latter depending on its importance and sensitivity. The Security and Privacy Committee has to guarantee that all personnel working with the IMS are aware of this Policy, its objectives and processes, informing them about all the above, creating training programs and organizing campaigns to raise greater awareness.

It also has to guarantee that the corresponding documents that are relevant for each specific level are duly distributed and made available in keeping with the different roles defined in the company.

5.9 Approval

Xavier Mendoza Mayordomo, in due representation of Fundació Esade, fully accepts the content of this Policy and commits to duly implement it.

Do Good.
Do Better.

esade

www.esade.edu