BUSINESS INFORMATION & DIGITAL SERVICES AREA

INFORMATION SECURITY POLICY

IESE Business School
University of Navarra

Table of Contents

Versions Control

VERSION	DATE	SUMMARY	EDITED / APROBED	CONFIDENTIALITY LEVEL
0	01/12/2023	Creation of se Information Security Policy	IESE	PUBLIC
0	12/12/2023	Approval	Cybersecurity and Privacy Committee	PUBLIC

1. INTRODUCTION

The UNIVERSIDAD DE NAVARRA, in addition to its purely educational work, also undertakes significant healthcare and postgraduate student training activities. In this regard, THE UNIVERSIDAD DE NAVARRA has established its own General Information Security Policy, covering both the University itself and its associated entities.

IESE Business School (IESE), as an entity belonging to the University of Navarra, through this document and following the guidelines set by The University of Navarra, establishes its own Information Security Policy. This policy is aligned with the University of Navarra's policy but adapted to its distinct activities, considering specific risks and threats in information security.

2. OBJECTIVE

This policy aims to demonstrate the commitment of the IESE Management, represented by its Cybersecurity and Privacy Committee, to information security and the protection of information assets necessary for the performance of the functions described in the scope.

This commitment is realized through the implementation and maintenance of an Information Security Management System (ISMS) in accordance with the international standard ISO/IEC 27001.

The Information Security Policy primarily aims to ensure information security and the continuous provision of services by acting preventively, monitoring activities, and responding promptly to incidents.

This policy should establish the foundations for the access, use, custody, and safeguarding of information assets used by IESE to carry out its functions with security guarantees in various dimensions:

- Availability: The property or characteristic of assets allowing authorized entities or processes to access them when needed.
- Integrity: The property or characteristic ensuring that information assets are not altered without authorization.
- Confidentiality: The property or characteristic ensuring that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- Authenticity: The property or characteristic ensuring that an entity is who it claims to be or guarantees the source of the data.
- Traceability: The property or characteristic ensuring that the actions of an entity can be attributed exclusively to that entity.

Based on these principles, the specific objectives of Information Security at IESE include:

- Ensuring information security in the various dimensions described above.
- Formally managing security based on risk analysis processes.
- Developing, maintaining, and testing availability and business continuity plans for various services offered by the organization.
- Effectively managing incidents affecting information security.
- Keeping all personnel informed about security requirements and promoting best practices for secure information handling.
- Providing agreed-upon security levels when sharing or transferring information assets to third parties.
- Complying with current regulations and standards.

3. SCOPE

This Information Security Policy applies to all areas and departments within IESE, its systems, and information assets:

- All departments, including their managers and employees.
- All campuses of the institution.
- Partners (clients and suppliers), as well as any other organization with access to the institution's information or systems.
- Databases, electronic files, and paper-based support, processes, equipment, media, programs, and systems.
- Information generated, processed, and stored, regardless of its medium and format, used in operational or administrative tasks.

4. DISTRIBUTION

Approved by the IESE Management, this policy must be accessible to all affected individuals and organizations through publication on public website and on the corporate intranet. Similarly, the policy will be available to any interested party or competent authority upon formal request.

All IESE personnel, as well as external collaborators, are responsible for complying with this Information Security Policy.

5. REGULATORY FRAMEWORK

The control of regulations and applicable laws related to this information security policy is included within the Information Security Management System of IESE, available in the "Information Security Regulations."

6. MANAGEMENT COMMITMENT

The IESE Management commits to providing the necessary resources for the establishment, implementation, maintenance, and improvement of the institution's ISMS. The Management also demonstrates leadership and commitment to the ISMS through the establishment of the Cybersecurity and Privacy Committee. This committee is responsible for:

- Ensuring the establishment of this policy and information security objectives, aligning them with IESE's strategy.
- Ensuring the integration and compliance with applicable ISMS requirements in the institution's processes.
- Ensuring that the necessary resources for the ISMS are available.
- Facilitating communication about the importance of effective security management and compliance with ISMS requirements.
- Ensuring that the ISMS achieves the intended results.
- Supporting individuals to contribute to the effectiveness of the ISMS.
- Promoting evolution and continuous improvement in information security.
- Supporting other relevant roles of the Management, leading their areas of responsibility in information security.
- Monitoring indicators to assess results/compliance.
- Ensuring the adoption of measures necessary to comply with recommendations and instructions from supervisory authorities and monitoring regulations related to Security and Privacy.
- Ensuring the development of awareness measures and training plans for personnel related to information security and personal data processing.

7. FUNCTIONS AND RESPONSABILITIES

IESE has established an organizational structure for the implementation of this policy with the following functions and responsibilities:

Cybersecurity and Privacy Committee (the "Committee"): This committee provides the necessary resources for the operation and improvement of the ISMS, assigns responsibilities for information security, approves the Information Security Policy in terms of ISO 27001, and promotes and supports the implementation of necessary technical and organizational measures, including audits, to minimize potential risks to information and their potential consequences.

Security Commission: This commission serves as a support body to the Cybersecurity and Privacy Committee, overseeing the day-to-day implementation of the Information Security Management System. Its role includes reviewing and approving all regulatory documents emanating from this Information Security Policy.

CIO (Chief Information Officer) and Information Asset Managers (detailed in the ISMS Risk Analysis): They define security requirements, identify, and prioritize the importance of different assets so that the most important and/or sensitive processes receive greater protection. They also approve residual risk levels obtained through the risk assessment process and approve risk treatment plans necessary to reduce risks to an acceptable level.

CISO (Chief Information Security Officer): This role proposes measures and implements selected measures to mitigate risks, supervises the security of information assets and applied measures.

IT Compliance Manager: As the person responsible for the ISMS, they ensure that this Information Security Policy and policies, procedures, and technical notes derived from it are kept updated and under permanent review. They communicate them to stakeholders, supervise compliance, ensure compliance with applicable regulations and legislation, document actions and incidents adequately, suggest improvements to processes and procedures related to regulatory compliance in the IT field.

Data Protection Officer (DPO): This person ensures that personal data is processed and protected in accordance with the General Data Protection Regulation (GDPR), the Organic Law on Personal Data Protection and Digital Rights Guarantee (LOPDGDD), and recommendations from competent control authorities.

All IESE personnel, as well as external collaborators, are responsible for complying with this Information Security Policy.

7.1. SECURITY OBJECTIVES

Information security objectives will be established, seeking continuous improvement based on:

- Applicable information security requirements and the results of risk appreciation and treatment to ensure the confidentiality, integrity, availability, traceability, and authenticity of information.
- Internal factors, such as the application of organizational techniques that improve incident tracking and resolution.
- External factors, such as technological advances whose application improves the effectiveness of risk treatment.
- Improved effectiveness of training and awareness of personnel working in the institution, affecting their performance in information security.
- Changes in guidelines by the University of Navarra.
- Changes in the needs of stakeholders leading to an improvement in the scope of the system.

Additionally, planning for the achievement of established information security objectives will consider the following elements:

- What will be done.
- Why it will be done.
- Necessary resources.
- The responsible.
- Achievement period.
- Indicators to evaluate the result/compliance.

7.2. IMPLEMENTATION AND IMPROVEMENT OF THE ISMS

The deployment of IESE's ISMS will commence following the Risk Analysis, which will determine the level of information security risk in which the institution finds itself and identify the necessary security controls for risk treatment to bring it to an acceptable level, as well as improvement opportunities, considering internal and external factors and the aforementioned requirements of stakeholders.

Security controls must be implemented, maintained, and continuously improved, and should be available as documented information through procedures, regulations, technical instructions, manuals, etc., reviewed and approved by the Security Committee, under the supervision of the Data Protection Officer.

This Information Security Policy is developed by applying the following minimum requirements, which must be included in the documentation supporting the ISMS:

- Organization and implementation of the security process.
- Analysis and management of risks.
- Personnel management.
- Authorization and access control.
- Protection of facilities.
- Product acquisition.
- Security by default.
- System integrity and updates.
- Protection of stored and in-transit information.
- Prevention against other interconnected information systems.
- Activity logging.
- Security incidents.
- Business continuity.
- Continuous improvement of the security process.

Documented information on security controls must be communicated to the institution's personnel (employees/staff and suppliers), who are obligated to apply it in

the performance of their work, thereby committing to compliance with ISMS requirements.

Audits based on ISO/IEC 27001 will be conducted to review and verify ISMS compliance. If necessary, personnel within the scope must cooperate in these audits and in the implementation of corrective actions for continuous improvement.

7.3. CONFLICT RESOLUTION

In case of conflicts among different responsibilities within the organizational structure of the Information Security Policy, these will be resolved by IESE's Management, and the higher requirements derived from personal data protection will prevail.

7.4. CLASSIFICATION OF INFORMATION

Documented information will be classified as: public, internal, and confidential. It will be used appropriately according to this classification and as per the criteria established in the information classification, labelling, and protection procedure.

7.5. INFORMATION SECURITY POLICY REVIEW

This Information Security Policy will be reviewed during system reviews by Management, through the Security Committee proposing its continuity or changes to the Cybersecurity and Privacy Committee, whenever significant changes occur and at least once a year.

- Systematic periodic reviews: These should be performed when incidents or changes in the legal framework may question the validity of this Policy.
- Unplanned reviews: These reviews should be carried out in response to any security event or incident that could significantly increase the current risk level or has impacted the information security of IESE.

The review should ensure that the Information Security Policy aligns with IESE's information security strategy, mission, and vision, and ensures the fulfilment of established control objectives.

7.6. RISK MANAGEMENT

All systems subject to this Policy must undergo risk analysis and management, assessing the assets, threats, and vulnerabilities they are exposed to and proposing appropriate countermeasures to mitigate risks. Although continuous control of changes made to the systems is required, this analysis will be repeated:

- At least once a year (through formal review and approval)
- When the handled information changes
- When the provided services change

- In the event of a serious security incident
- When serious vulnerabilities are reported

To harmonize risk analyses, a reference assessment will be established for different types of information and services handled.

7.7. DEVELOPMENT INSTRUMENTS

A regulatory framework on information security is established at different levels so that the objectives set by this document have a specific development.
The information security policy will structure its regulatory framework at the following levels:

- The Information Security Policy, which sets out global protection requirements and criteria.
- Security standards that define what needs to be protected and the desired security requirements. The set of all security standards must cover the protection of all organization information system environments. They establish a set of expectations and requirements that must be met to satisfy and fulfil each of the security objectives established in the policy.
- They are proposed by the ISMS manager and approved by the CISO. The Security Committee is responsible for ensuring correct implementation.
- Security procedures that describe specifically how to protect what is defined in the standards and the people or groups responsible for implementing, maintaining, and monitoring their compliance level. These documents specify how to carry out routine tasks, who should perform each task, and how to identify and report anomalous behaviours.
- Their approval will depend on their scope of application, which may be in a specific area or in a specific information system.

Additionally, guidelines with recommendations and best practices may be established.

As best as possible, all documentation will be managed as per the current IESE document and record control procedure, which aims to establish criteria for the control of documentation and records used in the Information Security Management System.

7.8. PERSONAL OBLIGATIONS

All personnel with responsibilities in the use, operation, or administration of information and communication systems are obligated to be familiar with and comply with this Information Security Policy and the derived security regulations, regardless of the type of legal relationship that binds them to IESE. The Information Security Policy will be accessible to all personnel providing services in the organs and entities referred to in the 'Scope' section.

To promote the 'Security Culture,' the Committee will promote a continuous awareness program to educate all personnel.

Non-compliance with the Information Security Policy and its development regulations will lead to the establishment of preventive and corrective measures aimed at safeguarding and protecting networks and information systems, without prejudice to the corresponding disciplinary responsibility.

7.9. RELATIONS WITH THIRD PARTIES

When IESE provides services or shares information with third parties, they will be made aware of this Information Security Policy and the derived rules and instructions.

Likewise, when IESE uses services from third parties or shares information with third parties, they will also be made aware of this Information Security Policy and the security rules and instructions related to such services or information. All partners (internal and external) will be subject to the obligations and security measures established in these regulations and instructions, and they may develop their own operating procedures to meet them. Specific incident detection and resolution procedures will be established. It will be ensured that third-party personnel are adequately aware of information security, at least at the same level as established in this Information Security Policy.

Specifically, third parties must ensure compliance with information security policies based on auditable standards that allow verification of compliance with these policies. Likewise, it will be ensured through audit or a certificate of destruction/erasure that the partner cancels and eliminates data belonging to IESE at the end of the contract.

When any aspect of the Information Security Policy cannot be satisfied by a third party, a report from the CISO specifying the risks incurred and how to address them will be required.

8. APPROVAL OF THE POLICY

This Information Security Policy is approved by the Cybersecurity and Privacy Committee meeting minutes dated 12th December 2023.