Policy on

Information security

GARRIGUES

4th edition, June 2025

Contents

1. Introduction

The Garrigues Group has taken the decision to manage its information systems (ISMS) using international best practices, in line with ISO/IEC standard 27001 and the Spanish National Security System (ENS).

With this in mind, this Information Security Policy has been prepared in compliance with the legal requirements envisaged in the following regulations:

- Royal Decree 311/2022, of May 3, 2022, regulating the National Security System.
- The ISO27001 standard.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), and Organic Law 3/2018, of December 5, 2018, on data protection and the safeguard of digital rights (LOPD-gdd).

The processing of information must be based on the principles of confidentiality, integrity, availability, traceability and authenticity.

2. Purpose

The purpose of this document is to define the Information Security Policy of the Garrigues Group. This policy specifies the commitments undertaken by Management in relation to the Information Security Management System applied to information systems that support legal and tax advisory services, advice on transactions and on administrative and/or judicial proceedings, and consulting services provided by Garrigues Group companies to their clients, defining the organizational and executive framework to ensure the confidentiality, integrity and availability of the information system.

The approval of the policy forms part of the process to implement the Garrigues Information Security Management System, which seeks to ensure that our information systems are managed with the required levels of security, following international best practices in line with ISO/IEC standard 27001 and the National Security System.

The objective of the Information Security Policy is twofold:

- Firstly, to define the **reference framework** to enable us to safeguard the security features of the assets that support Garrigues Group processes. The framework is based on the results of the risk analysis performed, on the alignment of strategic business requirements and security requirements, and on legal and contractual requirements. As specified in the above-mentioned framework, this Information Security Policy serves to establish the fundamental security principles of the information systems set out in the regulations, procedures, technical instructions, records or other documents necessary in order to specify the use of the information, of the systems and of the assets that support them.

- Secondly, the Garrigues Information Security Policy seeks to establish adequate organizational, physical and technical **security measures** to safeguard the security features of the above-mentioned assets, based on the premise that security must be conceived as an integral and cross-cutting process (that includes all technical, human, material and organizational elements related to information and communications systems) and should not be considered a management expense but rather an investment to prevent negative impacts on the business.

3. Legal and regulatory framework

The applicable legal and regulatory framework is regulated in the "Legal and contractual compliance management procedure", included in the ISMS as document "PRG 18.1", which sets out the applicable legislation, the data protection implications and the assigned obligations and responsibilities.

A detailed record of the applicable legislation is also kept in the "Record of applicable legislation and contractual obligations", included in the ISMS as document "RG 18.01".

4. Scope

This policy is applicable to the information systems related to client processes performed by the Garrigues Group in the pursuit of its activities. Any internal regulations, procedures or documents that deal with a specific security aspect of the information systems must respect and comply with this policy.

The policy established in this document applies to all employees, partners and other members of Garrigues Group companies integrated into Garrigues' systems, as well as collaborators and third parties involved in the business activities and processes defined in the scope of the ISMS, which support the client-related processes of the Garrigues Group (the "users of the information" or, simply, the "users").

5. Fundamental principles of the Information Security Policy

Given the importance of the information systems, Garrigues Management has established the following Fundamental Information Security Principles:

(a) **Regulatory compliance principle**: all information systems will be brought into line with the applicable legislation, regulations and industry rules on information security, particularly those relating to personal data protection, and the security of systems, data, communications and electronic services.

(b) **Risk management principle**: risks should be minimized to acceptable levels and a balance should be sought between security controls and the nature of the information. Security objectives should be established, reviewed and consistent with information security aspects.

All systems affected by this Information Security Policy are subject to a risk analysis to evaluate the threats and risks to which they are exposed. This analysis will be repeated:

- At least once a year.
- Where there is a significant change in the information and/or services managed.
- When there is a serious incident or serious vulnerabilities are detected.

The criteria for determining system security levels will be defined when categorizing the systems.

(c) **Awareness and training principle**: information security training programs and awareness campaigns will be drawn up for all users with access to information and tailored to each professional profile.

(d) **Principles of confidentiality, integrity, availability, traceability and authenticity**:

- The **confidentiality** of the information must be guaranteed, such that it can only be accessed by authorized persons.
- The **integrity** of the information worked with must be guaranteed, so that it is concise and precise, with an emphasis on accuracy, both of the content of the information and the processes involved.
- The **availability** of the information must be guaranteed, ensuring the continuity of the business supported by the information services through contingency plans.
- The **traceability** of the information must be guaranteed, to ensure that the actions of an entity (person or process) can be unequivocally traced to that entity.
- The **authenticity** of the information must be guaranteed, to ensure the identity of the entity (person or process) processing such information.

(e) **Proportionality principle**: controls to mitigate asset security risks should be implemented, seeking a balance at all times between the security measures, the nature of the information and the risk.

(f) **Responsibility principle**: All members of the Garrigues Group should be responsible for their conduct as regards information security, complying with the rules and controls established.

(g) **Continuous improvement principle**: the degree of effectiveness of the security controls implemented at the firm will be reviewed on a continuous basis in order to increase the ability to adapt to the constantly changing nature of risks and of the technological environment. The reviews carried out will take into account, on an annual basis, the review of services and information and their categorization, rules, procedures and the conduct of internal or external audits, and the performance of an annual risk analysis.

6. Responsibilities

Although each user is responsible for the information to which they have access and/or handle as a result of the performance of their functions, there are individuals and/or bodies with specific functions within the Garrigues ISMS, which have the following specific responsibilities in relation to this policy:

6.1 Management

Management is directly responsible for ensuring compliance with security regulations. This means that it must demonstrate leadership and commitment with respect to the information security management system, ensuring that the security policy and objectives are established and that they are compatible with strategic management.

As a result, its functions include approving this Information Security Policy, appointing the Information Systems Security Officer and other roles required by the National Security System, approving the formation and composition of the Security and Privacy Committee and authorizing the creation of the Information Security Department.

In addition, Management must provide information and training to users of the information systems regarding the existence and contents of this policy, which must be known to all members of the organization since it forms the basis for the other guidelines on the application of security measures to ensure an adequate level of protection.

6.2 Security and Privacy Committee

The Security and Privacy Committee must verify, at least once a year, that the Information Security Policy continues to be fit for the organization’s purposes, provides a coordination and reference framework for the establishment of information security objectives, includes a commitment to continuous improvement, is available to all interested parties and has been communicated internally. The Security Committee must also ensure that the policy has been approved by Management.

In short, the Security and Privacy Committee must verify each year, and whenever any significant changes occur, that the Information Security Policy is suitable, adequate and effective, proposing improvements where necessary. The Security and Privacy Committee is also the established body for the resolution of potential conflicts.

The composition of the Security and Privacy Committee is defined in the document “Regulations defining roles and responsibilities”, included in the ISMS as document “NOR02”, under section 5.2 Security and Privacy Committee.

Appointments will be reviewed each year or whenever a position becomes vacant.

6.3 Information Security Department

The Information Security Department is responsible for ensuring that all operational projects pursued at Garrigues follow and respect the fundamental principles established in this Information Security Policy.

6.4 Roles and responsibilities - National Security System

The following roles and responsibilities are defined in compliance with the National Security System:

- **Information Officer**, responsible for determining the security requirements of the processed information.

- **Service Officer**, responsible for determining the security requirements of the services provided.

- **Security Officer**, person responsible for making decisions regarding security requirements and supervising the implementation of the necessary measures to ensure such requirements are met.

- **System Officer**, person responsible for establishing the specific way of implementing system security and supervising the daily operation of the system.

Information Officer: Security and Privacy Committee

Service Officer: Security and Privacy Committee

Security Officer: CISO

System Officer: CIO

National Security System roles will be appointed and reviewed by Management each year or whenever any of the positions becomes vacant.

7. Users

All users must comply with the fundamental principles of the Information Security Policy and of the other internal policies included in Garrigues' Internal Regulations.

In the event of any user breach of the information security policy, rules and procedures in force, the corresponding disciplinary process will be followed.

8. Prevention

To ensure compliance with the Information Security Policy, the organization will take the following prevention measures:

- System authorization prior to launch to ensure systems meet security requirements.

- Periodic security assessments, including evaluation of routine configuration changes.
- Periodic requests for review by third parties to obtain an independent assessment.

9. Detection

Detection, analysis and reporting mechanisms will be established to provide information to officers periodically and when there is a significant deviation from pre-established normal parameters.

10. Response

Garrigues performs a series of response actions:

- It establishes mechanisms to effectively respond to security incidents.
- It designates a contact point for reporting incidents detected in any area of the organization.
- It establishes protocols for the exchange of information related to the incident. This includes two-way communication with the client.

11. Recovery

Garrigues has a business continuity plan to guarantee the availability of critical services and systems. Specifically, Garrigues has established the following:

- Business continuity plan.
- Business impact analysis.
- Disaster recovery plan.

Garrigues' Continuity Plan is designed to support continued operation of key support activities at Garrigues, reduce the damage and impact of unexpected service incidents and improve the ability to quickly recover the business.

12. Notification of incidents

In accordance with the provisions of article 33 of Royal Decree 311/2022, of May 3, 2022, Garrigues will notify clients of any incidents that have a significant impact on the security of the information handled and of the services provided in relation to the National Security System categorization. This procedure is referred to in the information security incident management protocol, included in the ISMS as document “A.16”.

13. Third parties

The principles of this Information Security Policy are published on the Garrigues website and can be consulted by clients, suppliers and interested third parties.

Any third party that accesses Garrigues information, in the context of providing services to Garrigues, must have knowledge of this Information Security Policy and of the associated regulations and must undertake to duly comply with the obligations deriving from same, and may define their own operating procedures to fulfill such obligations. Specific procedures will be established for the reporting and resolution of incidents. The personnel of such third parties must be sufficiently security-aware, at least to the same level as established in this Information Security Policy.

When any aspect of this Information Security Policy cannot be met by a third party in the manner required in the preceding paragraphs, a report must be issued by the Security Officer specifying the risks incurred and how they should be handled. The report must be approved by those responsible for the information and affected services before proceeding.

14. Approval and dissemination of the Information Security Policy

This policy has been approved by Management, which has verified that:

- It is fit for the organization’s purposes;
- It includes a reference framework for the establishment of information security objectives;
- It includes the commitment to comply with the applicable security requirements and to continuous improvement.

As indicated in section 6.1. above, Management must inform users of the existence and contents of this policy, which must be known to all members of the organization.

Consequently, this Information Security Policy will be published on the Garrigues intranet, together with the other internal policies that form part of the firm’s internal regulations, and permanently available for consultation by users of the information who are members of Garrigues.

Once it has been published on the intranet, Management will inform all members of the organization by email, so that they are aware of the existence of this policy and where it can be consulted.

In addition, section 5 of this policy, which contains the Fundamental Principles of the Information Security Policy, will be published on the Garrigues website.

15. Review of the Information Security Policy

The Information Security Policy will be reviewed on an ordinary basis once a year and extraordinarily whenever any significant changes occur.

The Security and Privacy Committee must notify Management of the changes made to the Information Security Policy, in order to ensure that it remains suitable, adequate and effective and for such changes to be duly entered in the "Document Control" record.

16. References

The following references have been taken into account in drafting this Information Security Policy:

- ISO/IEC standard 27001
- Royal Decree 311/2022, of May 3, 2022, regulating the National Security System.
- Applicable European and local data protection legislation.
- The document entitled "Management Review of the Information Security Management System", which forms part of the Garrigues ISMS.

17. Record of versions

Version	Date	Summary of changes made
1st edition	July 2017	Initial version
2nd edition	April 2018	Modification to the scope and purpose of the policy to include Garrigues' commitments as regards implementation of the Information Security Management System and to define the organizational and executive framework that ensures the confidentiality, integrity and availability of the information system.
3rd edition	October 2018	Update to the reference to applicable data protection legislation
4th edition	June 2025	Adaptation of the policy to the Spanish National Security System (ENS) standard.