Index

Regulatory framework

Nº	Legislation
1	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
2	Organic Law 3/2018, December 5, on Personal Data Protection and guarantee of digital rights.
3	Law 34/2002, of July 11, 2002, on information society services and electronic commerce.
4	Royal Decree 3/2010, of January 8, 2010, regulates the National Security Scheme in Electronic Administration.
5	Royal Decree 1777/2004, of July 30, 2004, approving the Corporate Income Tax Regulations.
6	Royal Legislative Decree 2/2015 of October 23, 2015, approving the revised Workers' Statute Law text.
7	Organic Law 10/1995, of November 23, 1995, of the Penal Code.
8	Law 25/2007, of October 18, 2007, on the conservation of data relating to electronic communications and public communications networks.
9	Law 6/2020, of November 11, 1920, regulates certain aspects of electronic trust services (Repeals Law 59/2003)
10	Royal Legislative Decree 1/1996, of April 12, 1996, approved the revised Intellectual Property law's revised text, regularizing, clarifying, and harmonizing the legal provisions in force on the subject.

1. Responsibilities and organization of security

a. STIC Committee (ICT Security)

ICT activities are coordinated through the STIC committee. This committee is composed of technical personnel from different departments for decision-making.

The ICT security committee will be formed by:

POSITION	NAME
Manager	Sebastià Prat
Responsible for the information	Noelia Fernandez
Responsible for the service	Josep Prat
Security Manager	Leopold Pons

The Director chairs the STIC Committee and is primarily responsible for:

- Use the casting vote to agree on the appropriate decisions when there is no agreement within the team.
- Implement, maintain and improve the Information Security Management System (ISMS).
- Allocate the necessary resources and approve the
- Assign and communicate the roles, specifically of information security and quality risks' owners.
-

Other roles of great relevance within the information security system are:

POSITION	NAME	RESPONSIBILITIES
ICT Systems Administrator	Leopold Pons	Responsible for the implementation, configuration, and maintenance of ICT-related security services.
ICT systems operators	Flexibble IT, S.L.	Continuity team. They are responsible for the daily operation of ICT-related security services.

b. Roles and Responsibilities

STIC Committee

- Establish, review, and approve the ISMS's scope and the information security policy.
- Ensure that information security policies, processes, procedures, and laws and regulations reflect business requirements and are aligned with the requirements of internal and external stakeholders.
- Establishing, reviewing, and approving the ISMS objectives and checking whether they are effectively implemented and maintained.
- Monitor significant changes in information.
- Review information security incidents and agree on necessary actions, if appropriate.
- Approve the most critical initiatives to maintain information security and the established quality level.
- Conduct Management reviews at planned intervals.
- Ensure that personnel know the importance of complying with safety requirements, legal and regulatory requirements, contractual obligations, quality requirements, quality levels, and service level agreements.

Responsible for the information

- It can establish the security requirements for the information managed. If this information includes personal data, the requirements derived from the legislation must also be considered.
- Determines the levels of information security.

Responsible for the Service

- Has the power to establish the safety requirements for the services provided.
- Determines the security levels of the service.

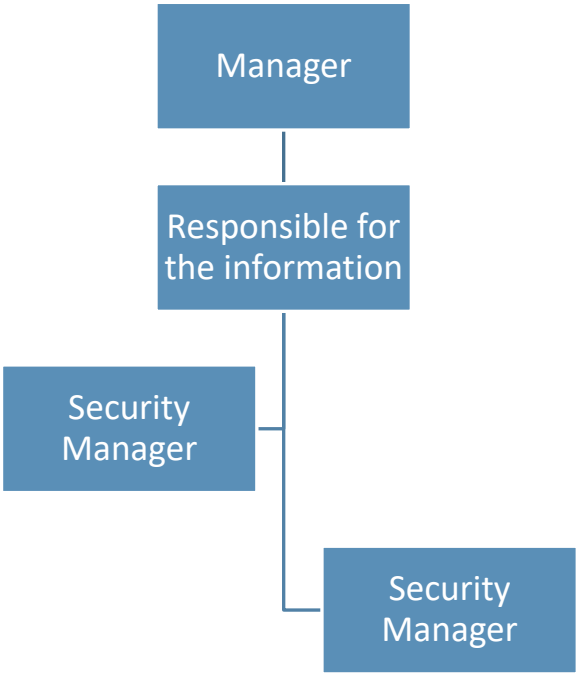
Security Manager

Responsible for defining, coordinating, and verifying compliance with the information security requirements defined according to the objectives.

The duties of the Information Security Officer are:

- Coordinate and control information security and data protection measures.
- Supervise the implementation, maintain, control, and verify compliance with:
    - The information security strategy defined by the Security Committee.
    - The rules and procedures contained in the Information Security Policy.
    - Monitor security incidents.
    - Disseminate the rules and procedures contained in the information security management system among the company's personnel and the functions and obligations of information security.
    - To supervise and collaborate in the internal or external audits necessary to verify the degree of compliance with the Security Policy, development regulations, and applicable laws regarding personal data protection and information security.
- Advise on information security matters to the different operational areas of the company.
- Updating of documentation related to ENS.

Role dependencies



2. Designation and renewal of security roles

Management is ultimately responsible for designating the different security roles. This designation will be made formally with the approval of this policy. The security manager will file the original signed by Management.
The established organization chart will reflect these designations.

The designation shall be renewed in the following cases:

- Medium or long-term leave of the designated personnel.
- Personnel leave the company indefinitely
- Lack of skills
- Management criterion based on HR management and strategic reasons.

3. Risk management

Assets subject to this security policy shall be subjected to a risk analysis, assessing possible threats and the risks to which they may be exposed. This analysis shall be repeated regularly, at least once a year, or when serious vulnerabilities are reported.

4. Resources

For the effective application of the Information Security Policy in the company, the Management will provide the necessary resources for its proper development, both in

the activities of implementation and operation and improvement of said policy and the information security controls established at any given time.

The protection of the company's and its customers' information assets is vital for the correct alignment with business objectives. To this end, an Information Security Management System (ISMS) has been established that implements all the processes and controls necessary to establish how information assets are protected.

The Information Security Management System is continuously updated and improved to meet the needs of the business, customers, and stakeholders; new objectives are set periodically, and business processes are regularly evaluated.

5. Approval and review

The Information Security Management System is reviewed annually or when there is a significant change in the business.
The Information Security Management System implemented, operated and improved, based on the National Security Scheme (NSC) in the organization, ensures:

- Establishing and maintaining the context, determining stakeholder needs and expectations
- That roles, responsibilities, and authorities are assigned
- The objectives established for the Information Security Management System are aligned with the strategic objectives.
- That indicators are established to measure the performance of the controls and are periodically analyzed and evaluated.
- That a risk criterion is established for the identification, analysis, evaluation, and treatment of risks.
- All personnel should receive training and awareness on information security and information security policies (physical and logical access control, physical security, malicious code, backup copies, information classification, information processing, continuity, etc.) implemented in the company.
- That the Management System is operated on the basis of approved documented information, policies, processes, procedures,...
- That compliance is verified through external audits, monitoring of objectives and indicators, and management reviews.
- That non-conformities and complaints are corrected through the implementation of corrective actions and the evaluation of the result of the same.
- That continuous improvement of the Information Security Management System is carried out.

The principles of the Information Security Policy are assumed and promoted by the Management, which provides the necessary means and provides employees with sufficient resources for its compliance, expressing them and making them public through a strategic Security Policy.

6. Development of the information security policy

This information security policy complements the company's security policies on different security matters available on the intranet.

This policy will be developed by means of security policies that address specific aspects. The security policy will be available to all members of the organization who need to know it, in particular to those who use, operate, or manage information and communication systems.

The company processes personal data. Access to certain security documents is restricted to authorized persons and those responsible. All the company's information systems shall comply with the security levels required by the regulations for the nature and purpose of the personal data included in the aforementioned security document.

The security regulations will be available on the intranet.

7. Level requirement

The required security level is **MEDIUM**, within the framework established in Article 43 and the general criteria prescribed in Annex I of the ENS. Some of the criteria that determine this level is that the process is fully defined. The process catalog is kept up to date and ensures consistency of actions among the different parts of the organization.

In addition, there are established rules and procedures to be able to react to any security incident and they are updated and maintained on a regular basis. Likewise, there is a high level of coordination between departments and the projects carried out.

The STIC committee considers the possibility of modifying the required security level.

The Management assumes and promotes the principles of the Information Security Policy, provides the necessary means, and provides employees with sufficient resources for its compliance, expressing them and making them public through this Security Policy.

8. Political approval

June 2nd, 2022
Management: *Josep Prat*