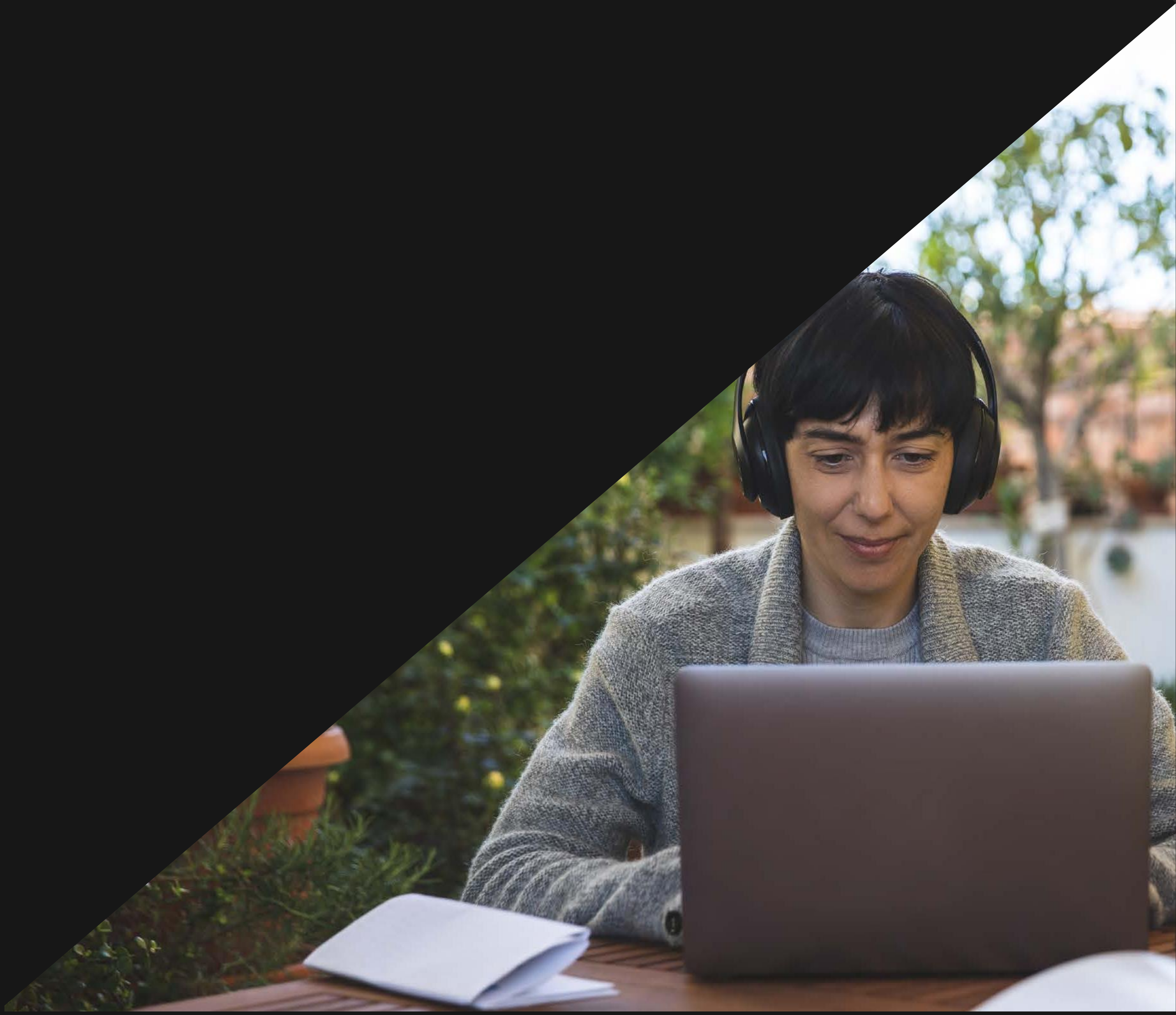
T: +34 937 880 333
E: info@flexxible.com

Security Policy



Index

1. Regulatory framework

No.	Legislation
1	Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27th 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).
2	Organic Law 3/2018, December 5th, on Personal Data Protection and guarantee of digital rights.
3	Law 34/2002, of July 11th, 2002, on information society services and electronic commerce.
4	Royal Decree 3/2010, of January 8th, 2010, regulates the National Security Scheme in Electronic Administration.
5	Royal Decree 1777/2004, of July 30th, 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 23rd, 1995, of the Penal Code.
8	Law 25/2007, of October 18th, 2007, on conserving electronic and public communications data.
9	Law 6/2020, of November 11th, 1920, regulates certain aspects of electronic trust services (Repeals Law 59/2003).
10	Royal Legislative Decree 1/1996, of April 12th, 1996, approved the revised Intellectual Property law's revised text, regularizing, clarifying, and harmonizing the legal provisions in force on the subject.

2. Responsibilities and security organization

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
Service Manager	Josep Prat
Security Manager	Leopold Pons
PII Treatment Organization Point of Contact and Privacy Officer	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 budget.
- Assign and communicate the roles 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	Flexxible Information Technology, 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.
- In addition to establishing, reviewing, and approving the ISMS objectives and checking if they are effectively implemented and maintained.
- Monitor significant changes in information security.
- 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 Information

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

Responsible for the Service

- It can 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 determined 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 among the company's personnel the rules and procedures in the Information Security management system and the functions and obligations regarding information security.
    - Supervise and collaborate in the internal or external audits necessary to verify compliance with the Security Policy, development regulations, and applicable personal data protection and information security laws.
- Advise on information security matters to the different operational areas of the company.
- Updating of documentation related to ENS.

PII Treatment Organization Point of Contact and Privacy Officer

The Company has designated a specific point of contact for our customers regarding processing Personally Identifiable Information (PII).

The designated point of contact will be available for:

- Answering inquiries,
- Assist and
- Facilitate communication between our customers and the team responsible for treating PII in our organization.

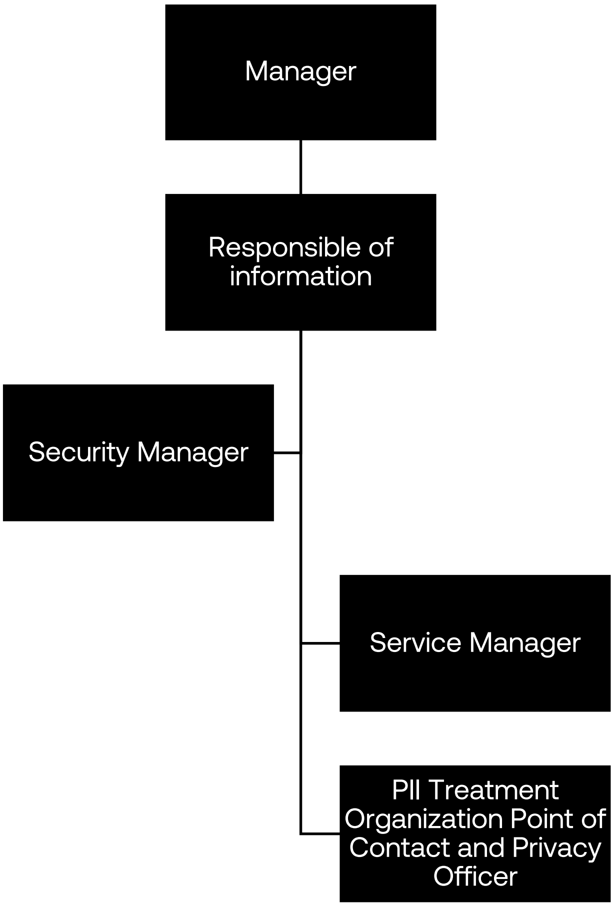
In addition, we have designated the person responsible for developing, implementing, maintaining, and monitoring our organization-wide privacy and governance program to ensure compliance with all applicable laws and regulations regarding the treatment of PII.

You will perform the following responsibilities:

- Be independent and report directly to the appropriate management level of the organization to ensure effective privacy risk management.

- Participate in the management of all issues related to the treatment of PII.
- Be an expert in data protection legislation, regulation, and practice.
- Act as a point of contact for the supervisory authorities.
- Inform senior management and employees of the organization of their obligations concerning treating PII.
- Provide advice concerning privacy impact assessments conducted by the organization.

Role dependencies


Manager
Responsible of information
Security Manager
Service Manager
PII Treatment Organization Point of Contact and Privacy Officer

3. 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 designated personnel.
- Staff leaves the company indefinitely.
- Lack of competencies
- Management criteria based on HR management and strategic reasons.

4. Risk management

Assets subject to this security policy shall undergo 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.

5. Resources

For the practical application of the company's Information Security Policy, Management will provide the necessary resources for its proper development, both in the implementation, operation, and improvement of said policy and the information security controls established at any given time.

Protecting the company's and its customers' information assets is vital for correctly aligning 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 established periodically, and business processes are regularly evaluated.

6. 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 (CCN) in the organization guarantees:

- Establishing and maintaining the context, determining stakeholder needs and expectations.
- Those roles, responsibilities, and authorities are assigned.
- Those objectives are established for the Information Security Management System and aligned with the strategic goals.
- Those indicators are established to measure the performance of the controls and are periodically analyzed and evaluated.
- That a risk criterion is established for identifying, analyzing, evaluating, and treating risks.
- All personnel receive training and awareness regarding Information Security and Information Security policies (physical and logical access control, physical security, malicious code, backups, information classification, information processing, continuity, etc.) implemented in the company.
- That the Management System is operated based on approved documented information, policies, processes, and procedures, ...
- Compliance is verified through external audits, monitoring of objectives and indicators, and management reviews.
- That nonconformities and complaints are corrected by implementing corrective actions and evaluating the results of these actions.
- That continuous improvement of the Information Security Management System is carried out.

Management assumes and promotes the principles of the information security policy, which provides the necessary means and employees with sufficient resources for compliance, expressing them and making them public through a strategic security policy.

7. Development of the information security policy

7.1 General considerations:

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

This policy will be developed using security policies that address specific aspects. It shall be available to all members of the organization who need to know it, particularly to those who use, operate, or manage information and communication systems.

The company processes personal data. Access to certain security documents will only be granted 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 security above document.

The safety regulations will be available on the intranet.

7.2. Considerations in the Definition of the Information Security Policy for Cloud Computing:

We recognize the complexity and challenges associated with information security in the cloud computing environment. In defining our information security policy for cloud computing, we have taken into account the following considerations:

- We recognize that information stored in the cloud computing environment may be subject to access and management by the cloud service provider. Therefore, we are committed to implementing appropriate security measures to protect our confidential information in this environment.

- We know that our assets, such as applications and programs, may reside in the cloud computing environment. We are committed to implementing appropriate security controls to protect these assets against internal and external threats.

- We understand that processes can run on a multi-tenant virtualized cloud service. We are committed to implementing security measures to ensure proper data and resource segregation between tenants in the cloud environment.

- We consider the different users of the cloud service and the context in which they use the service. We are committed to implementing robust access and authentication controls to protect our information from unauthorized access.

- We recognize that the provider's cloud service administrators may have access privileges to our data. We are committed to establishing procedures and monitoring controls to manage these privileges and prevent potential abuse properly.

- We consider the geographic locations of the cloud service provider's organization and the countries where the provider may store our data, including temporarily. We are committed to assessing and addressing the risks associated with storing data in specific geographic locations in compliance with applicable data protection regulations.

This statement of considerations in defining the information security policy for cloud computing will be communicated to all employees and relevant stakeholders within our organization.

7.3. Considerations in the Definition of the Information Security Policy for Compliance with PII Protection Legislation and Contractual Terms in the Public Cloud:

We recognize the critical importance of complying with personally identifiable information (PII) protection legislation and the contractual terms agreed upon with our cloud services customers. We are committed to ensuring the appropriate security and protection of sensitive information.

In line with this commitment, we affirm that our information security policies are complemented by an official statement expressing our support and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed with our cloud services customers.

We understand the importance of clearly allocating responsibilities among ourselves as public cloud PII processors, subcontractors, and cloud service customers. We recognize that the allocation of responsibilities may vary depending on the type of cloud service provided.

We are, therefore, committed to including explicit liability provisions in all our contractual agreements with our cloud service customers. These provisions will be specific to the type of cloud service in question, ensuring that security controls corresponding to each layer of the cloud architecture are adequately addressed.

We recognize that the type of cloud service may influence the allocation of responsibilities, especially concerning application layer controls. We are committed to adapting our policies and contractual agreements to reflect these differences and ensure clarity and transparency regarding all parties' responsibilities.

This statement of considerations in defining the information security policy for cloud computing will be communicated to all employees and relevant stakeholders within our organization.

7.4. Statement of Commitment and Support for Compliance with PII Protection Legislation and Contractual Terms:

We recognize the importance and seriousness of complying with applicable legislation and regulations protecting personally identifiable information (PII) in all our operations and activities. We are committed to ensuring the integrity, confidentiality, and security of the PII we handle.

As part of our commitment, we produce and maintain an official statement expressing our support and commitment to achieving compliance with applicable PII protection legislation and regulations. This statement will be regularly reviewed and updated to reflect any changes in legislation or our contractual obligations to partners, subcontractors, and relevant third parties such as customers and suppliers.

We understand allocating responsibilities between our organization and all parties treating PII is essential. We are, therefore, committed to including explicit provisions on responsibilities in all contractual agreements with our partners, subcontractors, and relevant third parties. These provisions will ensure a clear understanding of each party's responsibilities and obligations regarding PII's proper protection and management.

We recognize that, as an organization dealing with PII, whether as a data controller or processor, it is critical to consider applicable PII protection legislation and regulations while developing and maintaining our information security policies. We are committed to integrating these into our information security-related policies and procedures.

This statement of commitment and support will be communicated to all employees and relevant stakeholders within our organization.

8. Requirement level

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 guarantees the consistency of actions between the different parts of the organization.

In addition, established rules and procedures are updated and maintained regularly to react to any security incident. Likewise, there is a high level of coordination between departments and projects.

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

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

9. Policy approval

March 11th, 2024
Management: Josep Prat