

CLASSIFICATION: PUBLIC USE




Information Security Policy


CONTROL OF REVISIONS CARRIED OUT

Revision	Date	Description
1	13/03/2024	Preparation of the document

ELABORATE	REVISED	APPROVED
System Managers	Security Manager	Senior Management

	ISMS		ISMS	
	POLICY 1. INFORMATION SECURITY POLICY		Revision: 01 Date:13/03/2024	Page 2 of 7
CLASSIFICATION: INTERNAL USE				

This Document is the exclusive property of KNOWLEDGE CENTRIC SOLUTIONS, S.L., and its reproduction is prohibited without the express consent of the person responsible for the System. This document is considered, after printing, an UNCONTROLLED COPY, so once printed the validity of this document is not guaranteed.

	ISMS	ISMS	
	POLICY 1. INFORMATION SECURITY POLICY	Revision: 01 Date:13/03/2024	Page 3 of 7
CLASSIFICATION: INTERNAL USE			

Information Security Policy


KNOWLEDGE CENTRIC SOLUTIONS, S.L., as a company that provides services for the design, development, implementation and marketing of software products to customers in all sectors, as well as private and public sectors, assumes its commitment to information security and protection of personal data, committing itself to the proper management of the same. in order to offer all its stakeholders the greatest guarantees of confidentiality regarding the information used and the data processed.

For all of the above, the Management undertakes to strictly comply with the following **information security objectives**:


- Provide an operational framework to increase resilience and resilience for an effective response.
- Ensure the rapid and efficient recovery of services, in the face of any physical disaster or contingency that may occur and that could put the continuity of operations at risk.
- To prevent information security incidents to the extent technically and economically feasible, as well as to mitigate information security risks generated by our activities.
- Guarantee the confidentiality, integrity, availability, authenticity and traceability of the information.

In order to achieve these objectives, at KNOWLEDGE CENTRIC SOLUTION we work every day on:

- **Continuously improve** our Information Security Management System (ISMS).
- Comply with the **applicable legal requirements in force** and with any other requirements that we subscribe, in addition to the commitments acquired with customers, as well as the continuous updating of the same.

	ISMS		ISMS	
	POLICY 1. INFORMATION SECURITY POLICY		Revision: 01 Date:13/03/2024	Page 4 of 7
CLASSIFICATION: INTERNAL USE				

- Identify **potential threats**, as well as the **impact** on business operations that such threats, if they materialize, may cause.
- Preserve the **interests, expectations and needs of our main stakeholders** (customers, users, shareholders, employees, suppliers, etc.), **reputation, brand and value creation activities**.
- Work together with our suppliers and subcontractors in order to improve the provision of services, the continuity of the same and the security of information / confidentiality / protection of personal data, which have an impact on the **greater efficiency of our activity towards customers**.
- Evaluate and guarantee the technical competence of the staff, as well as ensure their adequate motivation for their participation in the continuous improvement of our processes, providing training **and adequate internal communication** so that they develop good practices defined in the system.
- Guarantee the **correct condition of the facilities and the appropriate equipment**, so that they are in accordance with the activity, objectives and goals of the company.
- Guarantee a **continuous analysis of all relevant processes**, establishing the relevant improvements in each case, based on the results obtained and the established objectives.

	ISMS	ISMS	
	POLICY 1. INFORMATION SECURITY POLICY	Revision: 01 Date:13/03/2024	Page 5 of 7
CLASSIFICATION: INTERNAL USE			

- Structure our **ISMS** in a way that is easy to understand. Our management system has the following structure:




All the elements of our ISMS are nourished by the respective records and evidence that guarantee their compliance.

The management of our system is entrusted to the **Security Committee** and the system will be available in our information system in a repository, which can be accessed according to the access profiles granted according to our current access management procedure.

For its part, the Management has the necessary means and provides its employees with sufficient resources to comply with them, which are reflected and made public through this Policy.


The defined security roles or functions are:

	ISMS	ISMS	
	POLICY 1. INFORMATION SECURITY POLICY	Revision: 01 Date:13/03/2024	Page 6 of 7
CLASSIFICATION: INTERNAL USE			

Function	Duties and responsibilities
Responsible for information and service	<ul style="list-style-type: none"> - Make decisions regarding the information processed - Coordinate the implementation of the system - Continuously improve the system
Data Protection Officer	<ul style="list-style-type: none"> - Ensure compliance with personal data protection regulations
Security Officer	<ul style="list-style-type: none"> - Determining the adequacy of technical measures - Providing the best technology for service
System Manager	<ul style="list-style-type: none"> - Coordinate the implementation of the system - Continuously improve the system
Senior Management	<ul style="list-style-type: none"> - Provide the necessary resources for the system - Leading the system

This definition is completed in the job profiles and in the system documents. The procedure for their appointment and renewal will be ratification by the Security Committee.

The Safety Committee is the body with the greatest responsibility within the **ISMS**, so that all the most important decisions related to safety are agreed by this Committee, drawing

	ISMS	ISMS	
	POLICY 1. INFORMATION SECURITY POLICY	Revision: 01 Date:13/03/2024	Page 7 of 7
CLASSIFICATION: INTERNAL USE			

up minutes and acting and deciding by majorities. The members of the Information Security Committee are:

- Information and Service Manager:
- Security Manager:
- System Managers:
- Data Protection Officer:

These members are appointed by the governing body of the Organization, which alone can appoint, renew and dismiss them.

The Security Committee is an autonomous, executive body with autonomy for decision-making and that does not have to subordinate its activity to any other element of our entity.

This policy is complemented by the rest of the policies, procedures, annexes and documents in force to develop our ISMS.