



INFORMATION SECURITY POLICY

VERSION CONTROL

Revision	Author	Description	Date
00	Security Officer	Initial version adapted for MEINS CONSULTING SLU	22-04-2026
01	ISMS	Review and update of the Policy	28-07-2026

☐

Controlled Copy

Responsible: Security Officer (CISO)

☐

Uncontrolled Copy

☐

Obsolete Document

Date:

Security Officer	ISMS Manager	General Management
Name: Marcos Turrión	Name: Victor Macías	Name: Julián Herrero
Signature: 	Signature: 	Signature: 

ÍNDICE

1. MANAGEMENT COMMITMENT3

2. MISSION AND SCOPE3

3. SECURITY OBJECTIVES3

4. SECURITY PRINCIPLES.....3

5. REGULATORY FRAMEWORK.....4

6. SECURITY ORGANIZATION4

7. CONTINUOUS IMPROVEMENT4

1. MANAGEMENT COMMITMENT

The Management of MEINS CONSULTING SLU (hereinafter, "MEINS") is committed to protecting the Company's own information and that of its clients, ensuring its confidentiality, integrity, availability, authenticity and traceability. To this end, MEINS maintains an Information Security Management System (ISMS) aligned with the Spanish National Security Framework (Royal Decree 311/2022) and the UNE-ISO/IEC 27001:2022 standard, and provides the resources necessary for its implementation, maintenance and continuous improvement.

2. MISSION AND SCOPE

MEINS is a Spanish electrical engineering company serving the renewable energy and industrial sectors. This Policy applies to the information systems that support the organization's services, as well as to all internal and external personnel with access to such systems or to the information processed. The system has been assigned the Medium Level category under the National Security Framework.

3. SECURITY OBJECTIVES

MEINS Management establishes the following information security objectives:

- Ensure the confidentiality, integrity, availability, authenticity and traceability of the information processed.
- Protect information systems against internal and external threats and ensure the continuity of services.
- Comply with the requirements of the National Security Framework, the UNE-ISO/IEC 27001:2022 standard and applicable legislation.
- Manage security risks systematically and in proportion to the system's category.
- Foster a security culture throughout the organization through ongoing training and awareness.
- Securely manage relationships with suppliers and collaborators.

4. SECURITY PRINCIPLES

MEINS applies the basic principles and minimum requirements established by the National Security Framework, including:

- Comprehensive security and risk management as ongoing processes.
- Least privilege and need-to-know principles governing access to information.
- Security by default and the capacity for incident prevention, detection and response.
- Periodic reassessment and continuous improvement of security measures.
- Segregation of duties within the security organization.:

5. REGULATORY FRAMEWORK

The applicable legal and regulatory framework includes, among others:

- Royal Decree 311/2022, of 3 May, regulating the National Security Framework.
- UNE-ISO/IEC 27001:2022 — Information Security Management Systems.
- Regulation (EU) 2016/679 (GDPR) and Organic Law 3/2018 on the Protection of Personal Data.
- Directive (EU) 2022/2555 (NIS2) and its transposition into Spanish law.
- Law 34/2002 on Information Society Services and Electronic Commerce.
- Royal Legislative Decree 1/1996, Intellectual Property Law.
- Applicable ENS Security Technical Instructions and CCN-STIC Guides..

6. SECURITY ORGANIZATION

Responsibility for information security rests with General Management, which is supported by a Security Committee acting as the decision-making body, together with the roles defined by the National Security Framework. The nominal assignment of these roles is managed internally in accordance with the ISMS documentation..

ENS Role	Key Responsibilities
Information Officer (RINFO)	Determines the security requirements of the information processed. Owner of the information assets.
Services Officer (RSER)	Determines the security levels of the services. Verifies that services are delivered with adequate security.
Security Officer (RSEG / CISO)	Makes decisions to satisfy security requirements. Oversees the implementation of security measures. Reports to the Security Committee.
System Officer (RSIS)	Develops, operates and maintains the information system. Defines the system's topology and management.

7. CONTINUOUS IMPROVEMENT

MEINS continuously reviews and improves its ISMS through internal audits, periodic management review, and the monitoring of nonconformities and corrective actions, thereby ensuring its ongoing compliance with the requirements of the National Security Framework and the UNE-ISO/IEC 27001:2022 stand