Information Security Policy (ISMS)

ISO 27001:2022

NORDLOGWAY, S.L. has decided to manage its **Information Security Management System (ISMS)** in accordance with international best practices, aligning with **ISO/IEC 27001 and Directive (EU) 2022/2555 (NIS2)**.

PURPOSE OF THE INFORMATION SECURITY POLICY

The Policy pursues a dual purpose:

- **Reference framework:** to establish the foundations that enable the protection of the security properties of the assets supporting NORDLOGWAY's processes. This framework is based on the results of risk analysis, on the business strategic requirements aligned with security, and on the legal and contractual obligations. In accordance with the above, the Policy sets out the essential principles that are developed in standards, procedures, technical instructions, records, and other documents that define the appropriate use of information, systems, and the assets that support them.

- **Security measures:** to define the organisational, physical, and logical measures necessary to preserve the security of such assets, based on the understanding that **security is an integral and cross-cutting process** (encompassing technical, human, material, and organisational components of information and communication systems) and that it must be considered an investment to prevent negative impacts on the business, not merely a cost.

SCOPE OF APPLICATION

This Policy applies to the Information Systems that support all NORDLOGWAY processes in the performance of its activities.
Any regulation, procedure, or internal document dealing with specific aspects of Information Security must respect and comply with this Policy.
The Policy applies to **all persons involved in business** activities and processes within the scope of the ISMS: employees, partners, collaborators, and third parties.

FUNDAMENTAL PRINCIPLES AND OBJECTIVES

1. Regulatory compliance: information systems shall comply with applicable legal, regulatory, and sectoral requirements concerning Information Security, with special attention to the protection of personal data and the security of systems, data, communications, and electronic services.

2. Risk management: risks shall be reduced to acceptable levels, seeking a balance between security controls and the nature of the information. Security objectives shall be established, periodically reviewed, and be consistent with the requirements of Information Security.

3. Awareness and training: training programmes, awareness actions, and campaigns on security shall be implemented for all users with access to information.

4. Confidentiality, integrity, availability, authenticity, and traceability:

- **Confidentiality:** only authorised persons may access the information.
- **Integrity:** information must be kept accurate and complete, ensuring the precision of its content and associated processes.
- **Availability:** information and services must be available when required, ensuring business continuity through contingency plans.
- **Authenticity:** the identity of entities (persons or processes) handling information must be guaranteed.
- **Traceability:** actions performed on information must be indisputably attributable to the entity that carried them out.

5. Proportionality: the implementation of security controls to mitigate risks shall maintain a balance between the measures applied, the nature of the information, and the existing risk.

6. Accountability: all members of NORDLOGWAY shall act responsibly in matters of Information Security and comply with the established rules and controls.

7. Continuous improvement: the Management assumes responsibility for promoting the continuous improvement of the Information Security Management System, ensuring that the implemented controls are regularly reviewed and reinforced to anticipate the evolution of risk and the technological environment.

This Policy constitutes the reference framework for establishing security objectives.

BUSINESS CONTINUITY

NORDLOGWAY has a Business Continuity Plan to guarantee the availability of critical systems and services. In particular, the following have been defined:

- **Business Continuity Plan.**
- **Business Impact Analysis (BIA).**
- **Disaster Recovery Plan (DRP).**

The Business Continuity Plan is designed to sustain the operation of NORDLOGWAY's key support activities, reduce damage and the impact of unforeseen incidents on services, and accelerate the recovery of activity.

THIRD PARTIES

Any third party accessing NORDLOGWAY information within the framework of a service provision must be aware of this Policy and its associated regulations and commit to complying with its obligations. They may develop their own operational procedures to meet these requirements. Specific procedures for incident reporting and resolution shall be established. It shall be required that personnel of such third parties are properly trained and aware of Information Security, at least to the same level required in this Policy.

CONTACT

For any additional information regarding this Policy or to submit suggestions, you may contact:
info@nordlogway.com

Víctor Gastón Puyo
Managing Director of Nordlogway
10 July 2025