INFORMATION SECURITY POLICY

NORDLOGWAY

OBJECTIVE

To protect the information, systems and assets that support NORDLOGWAY's processes through an ISMS aligned with ISO/IEC 27001:2022 and Directive (EU) 2022/2555 (NIS2).

SCOPE AND COMMITMENT

Applies to all information systems and to everyone involved in the processes: employees, partners, collaborators and third parties. Security is managed as a comprehensive, cross-functional process focused on continuous improvement.

Víctor Gastón Puyo
General Manager, Nordlogway

28/09/2026 POL-SGSI-01 rev 02

NORD LOGWAY
LOGISTICS PROVIDER

01

REGULATORY COMPLIANCE
We comply with applicable legal, regulatory and industry requirements, with particular attention to data protection and the security of systems, data, communications and services.

02

RISK MANAGEMENT
We identify, analyse and reduce risks to acceptable levels, maintaining a balance between controls, the nature of the information and the existing risk.

03

SECURITY OBJECTIVES
We set and regularly review objectives consistent with information security requirements and the strategic needs of the business.

04

AWARENESS AND TRAINING
We promote training and awareness programmes for all users with access to information.

05

CONFIDENTIALITY
We ensure that only authorised persons can access information.

06

INTEGRITY AND AUTHENTICITY
We keep information accurate and complete, and we guarantee the identity of the people or processes that handle it.

07

AVAILABILITY
We ensure that information and services are available when needed, with measures aimed at business continuity.

08

TRACEABILITY
We ensure that actions on information can be unequivocally attributed to whoever performed them.

09

ACCOUNTABILITY AND PROPORTIONALITY
Everyone must comply with the rules and controls, applying measures proportionate to the information and the risks.

10

BUSINESS CONTINUITY
We have a Business Continuity Plan, a Business Impact Analysis (BIA) and a Disaster Recovery Plan (DRP).

11

THIRD PARTIES
Third parties with access to information must be aware of and comply with this policy, manage incidents and maintain an appropriate level of awareness.

12

CONTINUOUS IMPROVEMENT
We regularly review and strengthen the ISMS and its controls to anticipate changes in risks and in the technological environment.