Information Security Policy

History:

Edition	Date	Reason for revision / comments
01	March 03 2026	First Issue

Approval:

	Function
Drafted by:	QHSE & Sustainability Function
	Security & Compliance Function
Verified by:	QHSE & Sustainability Director
	Corporate Chief Information & Digital Officer
Approved by:	Board of Directors

INDEX

1. INTRODUCTION

The Polifin Group (hereinafter, “the Group” or “Polifin”) operates in compliance with the principles of work ethics, technical competence, and continuous improvement, promoting a culture oriented toward innovation and operational excellence. These values constitute the foundation of the Group’s positioning within its reference sectors.

Based on sustainability principles, corporate values, as well as the size of the Group and its organizational context, this Information Security Policy has been defined.

The purpose of the Policy is to establish the fundamental principles and provide employees with guidelines aimed at ensuring the protection of Polifin Group’s information systems, corporate data, and information.

This Information Security Policy defines the core principles and guidelines through which the Polifin Group intends to ensure the **confidentiality, integrity, and availability** of information, protecting the organization from ever-evolving cyber threats.

The objective of the Policy is to provide a framework for defining information security goals and to support continuous improvement, in line with the Group’s operational needs and risk context.

The Policy applies to all companies within the Polifin Group and concerns employees, external collaborators, suppliers, and any party that accesses or handles corporate information. All recipients of this Policy are required to operate in compliance with the principles and provisions it contains. The Policy is made available to stakeholders, is properly communicated within the organization, and is made available externally.

This document is approved by the Board of Directors of the Polifin Group. The Board of Directors also ensures its periodic review, in order to assess its adequacy and identify potential improvement actions.

In this context, all Group companies adopt the contents of the Policy through their organizational structures, committing to:

• ensure compliance with applicable regulations;

• provide employees with a clear reference and guidance framework;

• contribute to the identification and pursuit of the Group’s goals and objectives.

2. INFORMATION SECURITY APPROACH

The Polifin Group addresses information security by adopting a **systematic and risk-based approach**. This methodology requires that security measures be balanced according to the criticality of the information assets to be protected, thereby ensuring an adequate and proportionate level of protection in relation to the identified risks.

To ensure an effective and consistent management of information security, the Group is committed to adhering to the following fundamental principles:

- **Protection of confidentiality, integrity, and availability of the information processed:** including that of customers, employees, and business partners;
- **Business continuity and resilience**: measures are implemented to ensure that business processes can continue even in the presence of adverse events, minimizing the impact of potential disruptions and enabling a prompt restoration of operations;
- **Prevention of unauthorized access, improper alterations, and unavailability of information**, by minimizing risks through effective change management and IT process governance;
- **Timely management of security incidents**: Polifin Group aims to promptly detect, manage, and resolve any information security incidents, limiting potential damage and preventing the recurrence of similar events;
- **Protection of corporate reputation**: safeguarding information is essential to preserve the credibility and image of the Group with customers, partners, and the reference market;
- **Maintaining trust with customers and stakeholders**: the actions undertaken aim to meet the expectations and needs of all interested parties, strengthening their confidence in the organization;
- **Regulatory and contractual compliance**: all applicable information security regulations are observed, as well as any specific requirements established in contracts with customers and suppliers;
- **Promotion of a cybersecurity culture**: Polifin Group fosters awareness and accountability regarding information security throughout the organization, encouraging a widespread security-oriented culture at all organizational levels.

3. OVERVIEW OF MEASURES FOR COMPANIES WITHIN THE SCOPE OF THE NIS2 DIRECTIVE

The following sections apply exclusively to the Polifin Group companies covered by the scope of the European Network and Information Security Directive 2 (also referred to as NIS2) (2022/2555).

These companies are required to adopt specific measures for information security and cybersecurity in order to ensure a high and consistent level of protection. This Policy outlines the key areas and the measures necessary to comply with the NIS2 Directive.

At Group level, the Security & Compliance function is responsible for coordinating security activities, maintaining an adequate level of information security, and ensuring consistency in the application of this Policy across the various companies.

The commitments and responsibilities undertaken by top management with regard to information security are implemented through the following actions:

- promoting the importance of effectiveness in cybersecurity-related activities, in compliance with requirements and with the objective of achieving the established goals;
- establishing and disseminating the information security policy, including its principles and objectives;
- facilitating the integration of information security into business processes;
- ensuring the availability of adequate resources according to needs;
- overseeing security incidents and risk management.

3.1 CYBER RISK MANAGEMENT

Risk management is a fundamental process for protecting the information of the Polifin Group companies. The Security & Compliance function is committed to identifying, assessing, and treating cyber risks in a structured manner, associating them with vulnerabilities and threats affecting the assets.

Critical assets are mapped, and through residual risk analysis it is possible to define intervention priorities and the most appropriate countermeasures, which are properly recorded, monitored, and reported.

3.2 ASSET PROTECTION AND CONFIGURATION

Every IT asset, whether hardware or software, is identified and managed through an inventory that each company is responsible for populating, maintaining, and updating. With regard to corporate data, it is classified based on its criticality, and specific security measures are applied to each category.

As for device configurations, these are managed centrally, with particular attention to updates, secure configuration practices, and endpoint protection.

3.3 SUPPLY CHAIN SECURITY

Supply chain security represents a strategic element for the Group. Suppliers identified as critical are subject to a preliminary risk assessment, and relationships with them are managed through specific information security clauses and monitored over time.

3.4 PHYSICAL AND LOGICAL SECURITY

The protection of the physical and logical environments that host data and systems is an integral part of the security strategy. Access to data centers and restricted areas is regulated by strict procedures and based on the identified risk, physical measures such as access control and video surveillance may be implemented. Simultaneously, IT systems are protected through effective logical security measures, including, for example, network segmentation, antivirus solutions, and secure backups.

3.5 INFORMATION SECURITY INCIDENT MANAGEMENT

Each Polifin Group company within the scope of NIS2 adopts a clear strategy for managing information security incidents, in line with this Policy. At Group level, the **Computer Security Incident Response Team** (CSIRT) has been established, tasked with detecting, classifying, and responding promptly to events. Every incident is documented and analyzed to identify root causes and to define corrective and preventive measures.

In the event of an incident, the competent authorities are notified in accordance with applicable regulations.
Communication with stakeholders is managed in coordination with the functions involved, in order to reduce reputational impact.

3.6 IT BUSINESS CONTINUITY AND DISASTER RECOVERY

Ensuring the continuity of business processes in the event of disruptions caused by cyber incidents or natural disasters is essential and is supported through specific IT business continuity and disaster recovery plans. These plans and related scenarios are tested regularly to verify their effectiveness and are updated according to technological developments and evolving risks. Moreover, clear escalation procedures and responsibilities are defined for crisis situations.

The objectives of IT business continuity management are to:

- ensure the continuity of IT operations according to the identified priorities;
- minimize the time and cost required to restore disrupted IT activities;
- operate in accordance with IT risk assessment results;

- define roles, responsibilities, and operational procedures for internal and external human resources (including external suppliers) involved.

The Security & Compliance function ensures that continuity plans comply with regulatory requirements and with the identified risk levels, in coherence with the provisions set out in this Policy.

3.7 INFORMATION SECURITY IN THE EMPLOYMENT RELATIONSHIP

The Group safeguards the security of corporate information by adopting appropriate controls and measures throughout the entire lifecycle of the employment relationship, ensuring that at every stage – from onboarding to offboarding – the protection of information is managed securely and in alignment with corporate policies. To this end, the organization also applies strict segregation-of-duties criteria, ensuring that critical activities are not concentrated under a single individual.

3.8 COMPETENCE AND AWARENESS

Awareness and an adequate level of knowledge among employees and top management regarding cybersecurity topics are crucial for the effective protection of the Group's assets.
Every employee receives appropriate training on the policies, procedures, and processes with respect to their role. Particular attention is given to the most exposed roles and to critical functions.

3.9 MONITORING

The effectiveness of security measures is subject to periodic controls through internal and/or external audits. Continuous monitoring of the systems makes it possible to identify anomalous behaviors and violations, enabling prompt corrective action. Reports monitoring results are shared with management and with the Boards of Directors of the companies within the scope of NIS2, in order to ensure appropriate oversight.

POLIFIN

POLIFIN S.p.A.
Viale Vittorio Emanuele II, 10/M - 24121 - Bergamo BG - Italy
Tel. e Fax +39 035 235 236
C.F./P.IVA 03440020166