INFORMATION SECURITY POLICY

Rev.: 0

Date: 21/07/2025

Introduction

Indel B has established an Information Security Management System (ISMS) to ensure the protection of data and information, with a continuous risk management process. This translates into compliance with the following fundamental principles:

- Confidentiality, i.e., ensuring that sensitive information is available to authorised individuals and processes and is not disclosed to third parties;
- Integrity, i.e., ensuring that information is not altered or deleted due to errors, deliberate actions, or malfunctioning of storage systems;
- Availability, i.e., ensuring that users have access to the information for which they are responsible, after appropriate checks.

This Policy applies to all employees, customers, suppliers, and partners working with Indel B and covers all data and information stored in the company, including customer data and personal data.

This Policy is reviewed annually during the management review or at significant events, such as regulatory or organisational changes, to ensure its effectiveness and adequacy.

Contents

The general principles of the current Information Management System are:

- Security aspects are identified and analysed through a risk analysis approach;
- The company must be aware of the information it handles and its degree of criticality in order to assess the implementation of the most suitable levels of protection;
- Information is accessed through appropriate levels of security to prevent disclosure to unauthorised third parties;
- The key figures in the system are outlined and have defined responsibilities;
- Incidents involving information management systems must be detected as soon as possible and managed through appropriate response systems in order to minimise their impact;
- The relevant legal and third-party requirements are complied with, including in the area of personal data processing.

The company is therefore committed to raising awareness among its employees and collaborators about these issues so that they always act strictly in accordance with the instructions given. In addition, the effectiveness of IT systems, a clear definition of organisational roles and security responsibilities, and extensive awareness and training on the most critical issues are ensured.

General Manager and CEO

Luca Bora