Information Security Policy – Summary

Pakelo Motor Oil S.p.A. (hereinafter also referred to as Pakelo or the Company) has developed and implemented an **Information Security Management System** (hereinafter also referred to as **ISMS**) with the primary aim of:

- Identifying, assessing, and addressing information security risks;
- Demonstrating commitment and compliance with global best practices;
- Showing customers, suppliers, and stakeholders that information security is a fundamental requirement;
- Protecting all critical, financial, sensitive, and confidential data, thereby minimizing the likelihood of unauthorized or illegal access.

All Company personnel (employees and non-employee collaborators), as well as third parties where agreed, are required to comply with the provisions of Pakelo's ISMS.

Information Security Policy

This Policy aims to provide managerial guidance and support for the proper management of information security and applies to all functions and operational units of Pakelo.

The Company considers the information it manages as an integral part of its assets. For this reason, it sets as a fundamental objective the safeguarding of its information assets from any intentional or accidental, internal or external threat, protecting the **confidentiality**, **integrity**, **availability**, and **authenticity** of the information produced, collected, or otherwise processed.

This Policy, which everyone must adhere to according to their role and responsibilities within the Company, outlines the principles that inspire Pakelo.

To define the Policy, the Company has first established its commitments and objectives regarding information security.

To achieve corporate goals, the information processed must meet the following requirements:

- **Confidentiality**: Information must be known only by those who have the right to access it, respecting the principle of least privilege ("need to know") based on the roles held ("need to operate");
- **Integrity**: Information must be accurate and complete, must reflect corporate values and expectations, and must be protected from unauthorized modifications and deletions. To meet this requirement, information must be correct, up-to-date, and readable;
- **Availability**: Information must be available when required by business processes, in an effective and efficient manner;
- **Effectiveness**: Information must be relevant and appropriate to the business process and, at the same time, must be promptly available, error-free, and provided in a way that allows users to utilize it;
- **Efficiency**: Information must be provided through optimal use of resources, both in terms of productivity and cost-effectiveness.

To achieve these objectives, the Company is committed to:

- Ensuring that personnel and collaborators possess adequate knowledge and awareness of the principles and risks related to information security, enabling them to understand their responsibilities and roles in handling such information;

- Ensuring that all external suppliers are aware of the risks related to information security and commit to complying with the security policy adopted by the Company;
- Establishing guidelines for the application of standards, procedures, and systems for the management and protection of information;
- Increasing awareness and sensitivity among users of corporate devices and tools by defining a clear set of rules and procedures aimed at proper information management;
- Ensuring that recipients are aware of the rules adopted regarding data protection and their implications, as well as the methods for applying the measures provided, as outlined in the operational security procedures;
- Ensuring that the risk management process adopted by the Company is properly monitored and periodically updated in light of the parameters set out in the regulations forming the ISMS;
- Ensuring that, for each operational function of the Company, specific criteria for identifying, assessing, and managing risk are defined and implemented, based on the type of activity performed.

The Company implements the Policy through the definition of specific performance objectives, for which plans, programs, and implementation procedures are formulated. The Company monitors and measures these performances and related results in relation to the defined objectives.

It is the responsibility of all personnel and anyone acting on behalf of the Company to respect their responsibilities and commit to achieving continuous improvement in information security performance, reporting any situation that does not align with the commitments and principles outlined above or that may pose risks to information security.

The **General Policy**, together with other related policies and procedures adopted, is approved by Management, communicated within the organization, and made available to other interested parties, where agreed.

Below is the contact email of the ISMS Manager of Pakelo Motor Oil S.p.A.: **sgsi@pakelo.it**