POL Information Security Policy

Company Name	Intuisco LTD
Effective Date	31/03/2025

Version History

Version	Date	Description	Author	Approved by
1	31/03/2025	-- N / D --	Raimondo Fanale	Raimondo Fanale

Purpose

The purpose of this policy is to declare and communicate Top Management's commitment to protecting the organisation's information assets. This document defines the framework for establishing, implementing, maintaining, and continually improving the Information Security Management System (ISMS), in order to protect the confidentiality, integrity, and availability of information and to support the organisation's strategic objectives.

Scope

This policy applies to all activities, processes, information assets, technological systems, and premises of the organisation. It involves all contracted collaborators and third parties who have access to company information or systems, regardless of their geographical location.

Regulatory references

- **ISO 27001:2022** – Requirements for information security management systems.
- **ISO 27002:2022** – Guidelines for information security controls.
- **Regulation (EU) 2016/679 (GDPR)** – Protection of natural persons with regard to the processing of personal data.

Terms and Definitions

- Information Security: The protection of the confidentiality, integrity, and availability of information.
- Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- Integrity: The property of safeguarding the accuracy and completeness of information and processing methods.
- Availability: The property of being accessible and usable upon request by an authorized entity.
- ISMS (Information Security Management System): The organisation's systematic approach to managing sensitive information so that it remains secure.

Roles and Responsibilities

ISMS Manager:

- Oversee overall compliance with the policy.

Employees / Third Parties:

- Understand and apply this policy, along with its principles and guidelines.
- Immediately report any anomaly or violation of this policy.

Information Security Objectives

The organisation's commitment to information security is not an end in itself, but a strategic pillar that translates into a set of clear and measurable objectives guiding every related decision. The primary and fundamental objective is to ensure solid regulatory compliance, in full respect of laws, regulations, and contractual obligations, ensuring that security practices are always aligned with the most recent legal requirements.

Beyond compliance, the organisation's primary goal is the proactive protection of its information assets. Efforts are made to actively safeguard the information entrusted to the organisation by its clients, as well as its own intellectual property, protecting them with determination from any threat, whether internal or external. This commitment extends to the objective of ensuring operational resilience; not only preventing incidents but also preparing to respond effectively. The organisation aims to maintain the continuity of critical operations and to restore services quickly and efficiently, minimising the impact on business and clients.

The organisation recognises that technology alone is not enough. Therefore, a crucial objective is the promotion of a pervasive security culture, in which every staff member is not only aware of the policies but also deeply understands the value of their role in protecting information. Finally, all organisational initiatives are guided by a mature approach to risk management, enabling the intelligent and prioritised identification, assessment, and treatment of threats, ensuring that resources are always invested where they can generate the greatest value for information security.

Fundamental Principles of Information Security

The organisation's information security strategy is not based on a single control, but on a set of interconnected principles that form the foundation of the adopted Management System.

The pillar supporting the entire structure is the principle of **shared responsibility**. Information security is not a task confined to a single department, but a duty belonging to every individual within the organisation. Therefore, a culture is promoted in which each employee is aware of their role and feels responsible for promptly reporting any known or suspected security incident, weakness, or anomaly.

This widespread responsibility is guided by a **proactive, risk-based approach**. Decisions on information security are not arbitrary but are the result of a formal analysis of threats and vulnerabilities, enabling the implementation of proportionate and effective controls. One of the main outcomes of this approach is the **access control principle**, whereby access to information and systems is granted according to the "least privilege" and "need-to-know" principles, ensuring that each user has only the permissions strictly necessary to perform their duties.

Controls, in turn, are not isolated elements. The security-by-design principle ensures that security is an inherent component and not an afterthought, being considered from the design phase of new processes, systems, or services. Finally, the organisation applies a defence-in-depth strategy, implementing multiple layers of security controls (technological, physical, and procedural). In this way, if one barrier fails, others are ready to intervene, creating a layered

and resilient protection for our most valuable assets.

Storage and Update

This policy is a controlled document and will be reviewed annually, or following significant changes in the organisation, technology, or threat landscape, under the supervision of the ISMS Manager.

Reference Documents

- POL Information Security Roles and Responsibilities Policy
- POL Management System Policy
- POL Information Classification and Labelling Policy
- POL Operational Security Policy