POL Information Security Policy

Company name	Innovatech Holdings LTD
Effective Date	29/01/2025

Storia della versione

Version	Date	Description	Author	Approved by
1	29/01/2025	-- N / D --	Michele Fasolino	Michele Fasolino

Purpose

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

Scope

This policy applies to all activities, processes, information assets, technological systems, and locations of the organization. It involves all contracted collaborators and third parties who have access to information or corporate 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.
- **Regolamento (UE) 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 ensures 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 organization's systematic approach to managing sensitive information to ensure it remains secure.

Roles and Responsibilities

ISMS Manager:

- Supervise overall compliance with the policy.

Collaborators:

- Understand and apply this policy along with the principles and guidelines it contains.
- Immediately report any anomaly or violation of this policy.

Information Security Objectives

The organization’s dedication to information security is not an end in itself, but a strategic pillar translated into a set of clear and measurable objectives that guide every decision in this area. The first and fundamental objective is to ensure strong regulatory compliance, fully respecting laws, regulations, and contractual obligations, making sure that security practices are always aligned with the latest legal requirements.

Beyond compliance, the primary goal of the organization is the proactive protection of its information assets. The organization constantly works to actively safeguard the information entrusted by its clients and its own intellectual property, protecting them with determination against any threat, whether internal or external. This commitment extends to the objective of ensuring operational resilience; the organization not only aims to prevent incidents but also to be prepared to respond effectively. The goal is to maintain continuity of critical operations and to restore services quickly and effectively, minimizing the impact on the business and on clients.

The organization recognizes that technology alone is not sufficient. Therefore, a crucial objective is to promote a pervasive culture of security, where each staff member is not only aware of the policies but also deeply understands the value of their role in protecting information. Finally, all the organization’s initiatives are driven by a mature risk management approach, which enables the identification, assessment, and intelligent prioritization of threats, ensuring that resources are always invested where they can generate the greatest value for information security.

Fundamental Principles of Information Security

The organization’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.

Decisions made by the organization regarding information security are not arbitrary but are the result of a formal analysis of threats and vulnerabilities, allowing for the implementation of proportionate and effective controls. One of the main outcomes of this approach is the principle of access control, according to which access to information and systems is granted based on the principles of "least privilege" and "need-to-know."

Controls themselves are not isolated elements. The principle of integrated security (security-by-design) 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 organization adopts a defense-in-depth strategy by implementing multiple layers of security controls (technological, physical, and procedural). This way, if one barrier fails, others are ready to intervene, creating layered and resilient protection for the organization's most valuable assets.

Archiving and Updating

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

Reference Documents

- *POL Policy on Roles and Responsibilities in Information Security*
- *POL Management System Policy*
- *POL Information Classification and Labeling Policy*
- *POL Operational Security Policy*