



Information Security Policy

Date and version	22/10/2025 v.1
Classification	PUBLIC USE DOCUMENTATION
Realization by	Security Officer
Approved by	Security Committe

Index

Introduction and Purpose	3
Principles	3
Responsibilities	4
Objectives	4

Introduction and Purpose

The organization's Information Security Policy reflects the concepts, principles, responsibilities, and objectives regarding security, the results of which allow the company to guarantee the necessary freedom of action.

THINGER.IO is a technology company that offers a cloud-based platform specialized in Internet of Things (IoT) solutions, enabling its clients to connect, manage, store, monitor, and analyze data from devices distributed across multiple locations. Its services facilitate the rapid deployment of IoT solutions through Amazon Web Services (AWS) cloud servers provided by the organization.

The objective of the organization's Comprehensive Security is to protect the people working in the company, the confidentiality of their communications, and the integrity and availability of their information. It also safeguards other assets that comprise the company's patrimony, such as facilities and all types of content.

Comprehensive Security encompasses the traditional concepts of physical and logical (technological) security in order to maintain business continuity under any adverse circumstances.

Increasing the "security culture" among company personnel will provide clear benefits by enhancing the security of systems and procedures, and minimizing the risk of potential malicious acts.

It is essential that all information regarding security matters flows through the appropriate channels to the company's decision-making bodies.

Principles

- **Integration.** Global Security is an integrated process aligned with the business, in which the entire company participates.
- **Profitability.** Security is guided by business criteria, taking into account the relationship between expenditure and investment. These criteria are established centrally, leveraging any existing synergies. This management

allows for an overall reduction in expenses and improved return on investment for the effort applied to security.

- Continuity. Security must be present throughout its entire work cycle: protection, prevention, detection, response, and recovery.
- Adequacy. The means employed must be adapted to the business environment. Among other factors, those that stand out for their impact on the business and the organization's security levels include competition with other companies, social, political, and economic unrest, amateur or professional hacking, etc.

Responsibilities

The ultimate responsibility for security lies with the management team, which is directly responsible for managing its development and implementation.

The management team will analyze security risks and vulnerabilities that could affect the proper functioning of the business and will propose the appropriate rules, resources, and measures to minimize them.

All personnel within the organization must assume responsibility for maintaining the security of the assets under their charge, adhering to the security standards implemented by the management team.

Objectives

- To achieve and maintain the required level of security to adequately guarantee business continuity, even in adverse situations.
- To increase the integration and mutual support of the physical and logical aspects of security.
- To collaborate in the management of other security disciplines, including labor and environmental aspects, adhering to criteria that promote Corporate Social Responsibility.

- To establish the corporate security structure defined by the organization's decision-making bodies and create appropriate communication channels among all stakeholders.
- To comply with official security regulations and other requirements.
- To establish and implement Security Training and Awareness Plans to improve staff training.
- Explicit commitment to continuous improvement.
- To integrate the company's various departments into a security management system that, under common criteria, leverages synergies and achieves consistency in resources and actions. All personnel of the organization will know and apply the regulations that develop this Security Policy.