SGE Policy	
Prepared by	**IMS Manager**
Approved by	**CEO**
Version	**1.0**
Date	**10/12/2025**
Classification	**Public**

1. IMS Policy

Techstar views the quality and security of information as essential factors for ensuring the effectiveness, efficiency, and reliability of the services it provides, as well as for protecting its own information assets and those of its customers. These aspects are of strategic importance and can readily be converted into a competitive advantage in the delivery of the services offered.

In line with this approach, Techstar has decided to implement an *Integrated Management System* (IMS) for quality and information security, designed in accordance with the rules and criteria set out in "best practices" and relevant international standards.

The aim of Techstar's *Integrated Management System* is to ensure the quality of the services provided and an appropriate level of information security within its data processing services. This is achieved by identifying, assessing, and addressing the risks to which the processes underpinning the services provided are exposed.

Furthermore, Techstar's *Integrated Management System* sets out, with a particular focus on information security, a set of organisational, technical, and procedural measures to ensure compliance with the basic security requirements listed below:

- *Confidentiality*, meaning the characteristic of information being known only to those who have the necessary privileges.
- *Integrity*, meaning the property of information to be modified only and exclusively by those who have the necessary privileges.
- *Availability*, meaning the characteristic of information being accessible and usable when required by the processes and users who have the necessary privileges.

Techstar will periodically review the effectiveness and efficiency of the *Integrated Management System*, ensuring appropriate support for the implementation of necessary improvements in order to enable the following:

- Define the *Integrated Management System for* assessing the suitability of the company's information system, ensuring that security and quality are integral parts of the process for delivering company services;
- Adopt criteria and methodologies for risk analysis and management;
- Establish organisational, procedural, and technological security measures to safeguard the quality, continuity, and reliability of the service, by implementing and maintaining the business continuity plan;
- Plan a specific, regular training programme covering topics related to the *Integrated Management System for* Techstar staff;
- Periodically review the exposure of the company's services to the main threats;
- Investigate security incidents and implement appropriate countermeasures;
- Promote a culture of information quality and security;
- Ensure that individual budgets allocated to achieving quality and safety objectives are appropriate, in line with the company's defined policies and strategic guidelines;
- Ensure the management of non-conformities and corrective actions, identifying their causes and promoting continuous improvement;
- Define the objectives and responsibilities of organisational roles;
- Measure and monitor customer satisfaction in order to continuously improve the services provided.

The safety guidelines, procedures, and operating instructions are set out in a dedicated set of documents and made available to staff according to their roles.

Regardless of their role, it is the responsibility of all Techstar staff to:

- To be familiar with the contents of this document and to contribute to the implementation of the guidelines and objectives set out within it.
- Apply the guidelines, procedures, and operating instructions for which they are responsible.
- Handle information correctly.
- Report any security incidents, anomalies, or potential threats.

Techstar permits the communication and dissemination of information externally only for the proper conduct of company activities, which must be carried out in compliance with applicable rules and regulations and in accordance with the specific formalised workflows that have been defined. This ensures the full and efficient management of the communication process.

Management

Luca Chiabrera