fives

INFORMATION SECURITY POLICY

The information security policy aims to protect information from any possible threat, internal or external, intentional or accidental, and describes the objectives, strategies, processes, roles and responsibilities implemented by Fives Intralogistics S.p.A. to ensure the aspects of confidentiality, integrity and availability to all stakeholders (customers, suppliers, partners, employees and collaborators), in compliance with the law and contractual requirements.

The information security policy is inspired by ISO 27001 standards and EU Regulation 2016/679 (GDPR). In particular, ISO 27002 is used as a reference for operating practices, a collection of "best practices" that can be adopted to meet the requirements of the ISO 27001 standard in order to protect information resources.

The data, information and, consequently, the applications and systems that process them, especially those that are of strategic importance for the company's business, are protected by security systems commensurate with their value and the risks to which they are exposed. In this context, "assets" are defined as tangible and intangible company resources that need protection for their business value.

The information security policy is based on basic principles and protection requirements that are guaranteed through a set of procedures for the processing of assets and information within company business processes (logical security) and an appropriate context where these processes take place (physical security).

The principles underlying the information security policy are:

- Asset security (systems, applications, network equipment and data) is a prerequisite for every business process carried out by the company and must involve customers, suppliers, partners, employees and collaborators;
- Information security is considered in project management, regardless of the type of project considered;
- Protection is adequate when the confidentiality, integrity and availability of assets are guaranteed and the risk of violations is avoided or can be reduced in an acceptable manner;
- All employees are responsible for implementing the information security system and must therefore be informed and regularly updated on the procedures to be followed;
- Each company asset has a formal manager who identifies and classifies the asset and defines the protection requirements in relation to the risk to which it is exposed;
- All users are identified and authorized before having access to the assets and the information must be protected from unauthorized access;

- Access rights to assets are established by the manager on the basis of the principles of "need to know" (access to information strictly necessary for the performance of the assigned task), "least privilege" (limited access to information with the minimum privilege necessary for the assigned task), "separation of duties" (authorization and execution must be the responsibility of different persons);
- Access rights are limited in scope based on the profile assigned to each user;
- Access rights are immediately modified or removed according to changes in the user's role and the end of the collaboration relationship;
- Accesses and activities are tracked in order to detect the user who performed the operation and when it occurred, the collection of this information is in compliance with the Regulations and laws in force;
- The laws, regulations and contracts relating to information security are complied with;
- Physical, logical and environmental security is guaranteed;
- Any violation, ascertained or presumed, of the information security system shall be promptly reported, investigated and documented;
- All breaches of the information security policy shall be punished.

Lonate Pozzolo, September 2021

Lorenzo Moroni
Chief Executive Officer