Annex D1.2-2

INFORMATION SECURITY POLICY

(UNI CEI EN ISO/IEC 27001:2024)

Ver.1	05/09/2024	1st Release	MG	Management Team	CEO	Audience
REVIEW	DATA	EDIT	REDACTED	VERIFIED	APPROVED	DISTRIBUTION

Camillo Ghelfi, CEO 40Factory

INFORMATION SECURITY POLICY

The Company's Integrated Management System

In its process of growth, revision, and continuous improvement, 40-FACTORY has decided to establish an Integrated Management System (IMS) for quality and information security, covering the entirety of the Company's characteristic activities.

The GIS encompasses all phases of the life cycle of MAT and Wilson software application products and related services: design, production, marketing, installation and support, and delivery of IT services such as SaaS (Software as a Service) distribution of applications.

The GIS with which 40FACTORY has been equipped is the result of the integrated adoption of the two management systems of Quality Management System (QMS) and Information Security System (ISMS), which comply with the standards respectively:

- UNI EN ISO 9001:2015 - Quality management systems - Requirements.
- UNI CEI EN ISO/IEC 27001:2024 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements *(recalling ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements).*

Management is convinced that the adoption, in the implementation of an IMS, of the concepts and principles underlying these standards brings important I benefits to the Company:

- improve "the ability to consistently provide products and services that meet customer and applicable mandatory requirements" (1) and relevant stakeholders in an increasingly competitive productive economic system,
- "address risks and opportunities associated with its context and goals" (1) characterized by rapid change and evolution and innovation
- improve the ability to preserve "the confidentiality, integrity and availability from information through the application of a risk management process" (2) to meet emerging cybersecurity challenges in an environment of increasing technological, data-driven interconnectedness;
- Ensure "compliance with the specified requirements of the quality management system" (1) and legal and regulatory requirements applicable to information management;
- build a solid foundation for implementing within their business goals, sustainable and resilient development strategies.

To achieve these IMS objectives of quality and information security efficiently and effectively and pursuing continuous improvement of the system itself, IMS activities have been defined and structured within a set of interrelated processes, managed using the "Plan-Do-Check-Act" (PDCA) cycle with planning based on an analysis of the context (internal factors, external factors and stakeholder needs) and applying a systematic preventive approach based on risk analysis" that minimizes corrective actions and the occurrence of problems.

Information Security

Since the overall objective of the Company is to ensure the proper management, in all processes, of all internally and externally generated or processed proprietary information, the organization with its IMS is committed to promoting, with all relevant functions and levels of the Company, the general principles of information security management, encompassing the following aspects, considered the most significant:

1. A **constantly updated catalog of Company assets** with their characteristics and responsibilities and **a classification of the information itself** with its level of criticality must be maintained so that it is managed with consistent and appropriate levels of confidentiality, availability and integrity.

2. **All access to systems must undergo an appropriate identification and authentication procedure (**periodically reviewed), which allows access to only relevant information and functions, differentiated by role and task.

3. **Procedures** must be established **for the secure use of Company assets, particularly computer assets, and information** and their management systems.

4. With specific activities, **full awareness of information security issues** must be **promoted and encouraged in all personnel** (employees and contractors) from the time of selection and throughout the duration of the employment relationship.

5. In order to handle incidents in a timely manner, everyone must **report any information security issues.** Each incident must be handled as outlined in the procedures.

6. **Unauthorized access to locations and individual Company premises where** information **is managed must be prevented**, and **the security of the equipment that handles it must** be ensured.

7. Implemented processes must **ensure** *confidentiality, integrity, availability* **of critical impact information**. In addition, **the characteristic of** *non-repudiation of data* must be **implemented**, (achieved through the management of electronic or digital signatures that must be documented where required by specific norms and standards.

8. **Compliance with legal requirements and principles related to information security must** be ensured **in contracts with third parties.**

9. A **continuity plan** (***business continuity***) must be in place to enable the Company to deal effectively with an unforeseen event, ensuring the restoration of critical services in a timeframe and in a manner that minimizes the negative consequences on the security of information to the actors in its environment (customers collaborators suppliers, institutions, etc.) and on the Company's mission.

10. **Security aspects must be included in all phases of design, development, operation, maintenance, support and decommissioning of IT systems and services.**

11. **Compliance with legal provisions, statutes, regulations or contractual obligations, and any requirements inherent in information security must be ensured**, minimizing the risk of legal or administrative sanctions, significant loss or reputational damage.

In this engagement and promotion, the Company has a specific focus on the new organizational and operational modes adopted: outsourcing of SaaS services, internal structural adoption of smart working, implementation of an integrated ecosystem of products and services involving customers and suppliers.

40-Factory's management considers investments in information security management (where required by the application context, as strategic, as key aspects to ensure, in addition to business sustainability and legal compliance, the maintenance of a trustworthy business reputation, towards all stakeholders.

Management is also aware that the proper management of information security affects all aspects of corporate life and requires the active participation of all stakeholders and is therefore actively committed to pursuing the competent and responsible involvement of all Company employees and, as far as possible, Third Party Stakeholders.

Protection of personal data

Regarding the policy for the protection of personal data, the Company provides its employees, collaborators, suppliers or consultants with organizational and technical instructions that enable compliance with legal obligations relating to the protection of personal data. For these obligations it outlines the security framework adopted for the information system and defines all measures to ensure the reliability of hardware and software components for the purpose of protecting processed personal data. It also informs users of products and services of the measures put in place to protect and store personal data through the appropriate notices.