Annex D1.2-2
INFORMATION SECURITY POLICY

(UNI CEI EN ISO/IEC 27001:2024 - UNI CEI EN ISO/IEC 27017:2021)

Ver.3	09/11/2026	MC	MT	CEO	PUBLIC
REVISION	DATE	DRAFTED	VERIFIED	APPROVED	CONFIDENTIALITY

Sommario

1 Purpose of the Document....3

2 The Company's Integrated Management System....3

3 Information Security....4

3.1 The Importance of Information Security for the Company....4

3.2 Why an Information Security Management System Based on Standards....4

3.3 Definition of Information Security....5

3.4 Information Security Objectives....6

3.5 Fundamental Principles of Information Security....6

3.6 Assignment of Responsibilities....10

3.7 Review of the Policy and of Topic-Specific Policies....11

4 Compliance with Directive (EU) No. 2022/2555 NIS2....11

5 Compliance with Personal Data Protection: Regulation (EU) 2016/679 GDPR and ISO/IEC 27001:2022....11

1 Purpose of the Document

This document, approved by Management, **defines the general guidelines according to which the entire Information Security Management System (ISMS)** of 40FACTORY has been established, implemented in an integrated manner with the Quality Management System (QMS). Every plan and procedure related to the handling of information security and of the assets that manage it, or that may have an impact on such security, must comply with the policy outlined in this document.

2 The Company's Integrated Management System

40FACTORY is an innovative SME operating in various industrial sectors as a provider of ready-to-use, highly configurable and scalable technological solutions, based on modern *Industrial Internet of Things (IIoT)* and *Artificial Intelligence (AI)* technologies. The Company has a well-established product-strategic consulting offering that enables **machine manufacturers** to adopt new business models and **end users** to enhance their internal digital culture and implement more efficient and sustainable production, through the intelligent and advanced exploitation of the "value" represented by machine and company data.

In its process of growth, review and continuous improvement, the Company has decided to establish an Integrated Management System (IMS) for quality and information security, which fully covers the Company's core activities.

The IMS covers all phases of the lifecycle of the application products, MAT and Wilson software, and related services: design, production, marketing, installation and support, as well as the provision of IT services such as the distribution of the applications in SaaS (Software-as-a-Service) mode.

The IMS adopted by the Company results from the integrated and certified adoption of two management systems, the Quality Management System (QMS) and the Information Security Management System (ISMS), compliant respectively with the standards ISO 9001:2015 and ISO/IEC 27001:2022 with the ISO/IEC 27017:2021 extension (adopted at European level as EN standards and at Italian national level as UNI/CEI standards).

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

- improving *"the ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements" [1]* and those of relevant interested parties, in an increasingly competitive economic and productive system;
- *"addressing risks and opportunities associated with its context and objectives" (1)* characterized by rapid changes, developments and innovations;
- improving the ability to preserve *"the confidentiality, integrity and availability of information by applying a risk management process" [2]* to face the emerging cybersecurity challenges in a context of growing technological interconnection, *data driven*;
- ensuring *"conformity to the specified requirements of the quality management system" (1)* and to the legal and regulatory requirements applicable to information management;
- building a solid foundation for achieving sustainable and resilient development strategies within its business objectives.

[1] ISO 9001:2015

[2] ISO/IEC 27001:2022

To achieve these IMS objectives of quality and information security efficiently and effectively, while pursuing the continual improvement of the system itself, the 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 **a context analysis** (internal and external factors and stakeholder needs) and applying a **systematic, preventive, risk-based approach** that minimizes corrective actions and the occurrence of problems.

3 Information Security

3.1 The Importance of Information Security for the Company

The Company's Information Assets - which include its own data and those of its customers and suppliers - represent the primary resource on which the Company's business processes are based (from market relations, to the development and quality management of its products and services, the continuous innovation process, the management of all internal structures, and the products and services used by customers), and **their security must be adequately ensured** through a constant balance between two factors: on the one hand, the accepted level of risk and the need to ensure the efficiency, effectiveness and continuity of processes; on the other, the degree of protection to be applied through a complex set of measures and controls, not only of a technological nature but also managerial and related to personal responsibility.

This protection is increasingly necessary today, considering the profound and rapid changes in cybersecurity risk scenarios, due to the growing digitalization and sharing of information through ICT and cloud computing infrastructures, which concerns all stakeholders as well as the Company's own organizational structure, and to the growth of threats to cybersecurity and privacy.

Given the nature of its activities, the Company's Management considers the security of the information assets managed by the Company, in compliance with contractual obligations and new laws and regulations, **an essential factor for the protection of its business**, which today requires providing guarantees not only on the quality and innovation of the products and services delivered but also on the correct handling of information.

The Company's Management therefore considers **investments in information security management strategic, where required by the application context**, as they are fundamental to ensure, in addition to business sustainability and legal compliance, the maintenance of a reputation as a reliable enterprise towards all stakeholders.

3.2 Why an Information Security Management System Based on Standards

To achieve this goal, the approach adopted is the implementation and maintenance within the Company of an Information Security Management System (ISMS) integrated with the Quality System, **certified by an internationally qualified body** and based on recognized standards and established methodologies. The choice fell on the certification and consulting body Det Norske Veritas (DNV) and on the internationally recognized ISO 27000 framework.

Specifically, given the Company's characteristics and business, **the following standards and guidelines have been identified:**

- The standard **"ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems – Requirements"**, subject of the integrated certification with ISO 9001:2015, which defines the requirements for establishing and managing the ISMS and covers all three dimensions of information security: logical, physical and organizational.

- The guidelines "**ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls**", which constitute the collection of "best practices" for the 114 controls to be adopted according to information security risks, in order to best meet the requirements of the ISO/IEC 27001:2022 standard
- The guidelines "**ISO/IEC 27017:2015 - Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services**" which extend the applicability of the ISO/IEC 27001:2022 information security certification specifically to cloud service management activities, both as a customer and as a service provider, fully integrated within the Company's ISMS.
- The general *risk management* guidelines **"ISO 31000:2018 Risk management - Guidelines"**, which provide a common approach to risk management that can be tailored to the organization and its context, applied by the Company to the management of information security risks, based on the identification of assets, threats and vulnerabilities (*asset-based risk assessment* approach).

In the Company's ISMS, information security is achieved, starting from this general Policy and on the basis of a structured analysis of the risks of the Company's context, **through the selection by applicability and the implementation of the comprehensive set of controls indicated by the standards and guidelines,** by means of a structured and efficient set of *Policies, Responsibilities, Processes, Procedures, Organizational structures, Hardware and software functions, Reports and Records* for monitoring, which are specific to topics and security areas, as defined in the Integrated Management System Manual (IMSM) and its annexes ([3]).

In defining the ISMS, the Company pays particular attention to **two topics** considered ***"focal points"*** of its information security certification:

- **the entire lifecycle of its products and services** (design, development, release, maintenance), which are a primary asset of the Company;
- **the development and management of its services that use SaaS cloud computing technologies** operating on the data and critical information of customers' applications.

In addition, **specific attention is paid to new organizational and operational methods**: the structural internal adoption of smart working and the implementation of an integrated ecosystem involving the Company, its customers and suppliers, based on cloud services.

3.3 Definition of Information Security

The primary objective of the ISMS is to ensure information security, which means guaranteeing the basic "CIA+A" requirements for information classified as critical:

- Confidentiality: information must be accessible only to authorized persons;
- Integrity: information must be modifiable only and exclusively by those who have the right to do so, in order to prevent improper or fraudulent changes, also with controls that make it possible to detect or prevent accidental changes;
- Availability: information must be accessible and usable when required by processes and by users with the relevant privileges, within timeframes consistent with their operational needs.
- Authenticity: information must be authentic and not altered, falsified or counterfeited.

In specific contexts, Non-repudiation is added: actions on data by users and processes must be tracked in a non-repudiable way.

[3] Integrated Management System Manual – Quality and Information Security – 40FACTORY

3.4 Information Security Objectives

With this information security policy, in accordance with what has already been implemented within the quality management system, **Management defines the following corporate objectives:**

- Protect its own and its customers' information assets as effectively as possible;
- Fully comply with the requirements of applicable laws and regulations;
- improve the transparency of its services, including in the use of new cloud technologies, to facilitate the definition and management of solid and secure contracts, in compliance with applicable legal obligations.
- Optimize the lifecycle management processes of its products and services.
- Best preserve the Company's image as a reliable and competent technology partner, also in the field of information security;
- Increase secure digital integration with stakeholders
- Increase the Company's resilience to cybersecurity threats in its context
- Increase the level of awareness, competence and responsibility of its personnel on security matters.

3.5 Fundamental Principles of Information Security

Since the Company's general objective is to ensure the correct management of all information generated or processed in all processes, whether owned internally or externally, the organization has engaged all corporate functions and levels, starting from top management, in implementing, within its certified *Information Security Management System*, **the measures and controls of the ISO 27000 standards relating to the fundamental principles of information security:**

1- TRAINING AND AWARENESS - All employees, from the time of selection and for the entire duration of their employment, and relevant third parties must be periodically instructed and made aware of the value of information and of the threats to its security, and trained, through specific training based on roles and responsibilities, on the information security policy and specific procedures established by the organization.

2- PERSONNEL MANAGEMENT - Procedures must be defined, in compliance with laws, regulations and ethical conduct, for the screening of all employees and third-party personnel who regularly access the organization's premises, in proportion to the security risks of the information managed. Furthermore, all employees and third-party personnel must sign non-disclosure agreements before having any interaction with the organization's information, and their contracts must require compliance with the organization's policies.

3- SUPPLIER MANAGEMENT - All suppliers, and any subcontractors, with whom the Company's critical information is exchanged must be contractually bound to be aware of and comply with the applicable corporate information security policies, allowing audits to be carried out. Compliance with corporate security clauses and information security service levels must be constantly monitored through formal procedures.

4- EXTERNAL CONTACTS AND COMMUNICATIONS - The organization must systematically carry out monitoring activities with sufficient contacts, both with the competent authorities, in order to react quickly and effectively to widespread threats in a coordinated manner at national level, and with specialist interest groups, forums or associations, in order to obtain information on current information security threats and the best practices to adopt to avoid or counter them.

5- LEGAL AND CONTRACTUAL REQUIREMENTS – All applicable information security requirements arising from national, international or sector-specific regulations must be kept under constant control, as well as those arising from contracts with third parties, with particular attention to the protection of personal and confidential data and to those relating to the cloud services used or provided.

6- PROTECTION OF INTELLECTUAL PROPERTY – Adequate procedures must be defined and implemented to ensure compliance with legislative, regulatory and contractual requirements on the use of material covered by intellectual property rights and on the use of proprietary software products.

7- PHYSICAL AND ENVIRONMENTAL SECURITY - Unauthorized access to the organization's premises and individual rooms and to its systems where information is managed must be prevented, through access points kept to a minimum and equipped with physical barriers protected by access control systems. Furthermore, such premises and systems must be provided with physical protection against damage caused by natural causes or any other type of natural or man-made disaster (such as fire, humidity and earthquakes).

8- ASSET MANAGEMENT - A centralized, constantly updated inventory of the Company's assets must be established and maintained, with their characteristics, the information managed, traceability throughout their lifecycle and operating procedures for secure use, with ownership and responsibilities clearly identified, documented, accepted and implemented (management of all assets assigned to employees or third parties).

9- INFORMATION CLASSIFICATION, LABELLING AND HANDLING - Information must be classified, labelled and handled with regard to its confidentiality, availability and integrity, according to its value to the organization and current legislation (and therefore its criticality), by all information owners of the organization.

10- NETWORK SECURITY - ICT networks, including virtual cloud networks, must be implemented and verified (where necessary with Vulnerability Assessment and Penetration Testing) so as to limit the possibility of interception or alteration of traffic, also by limiting authorized communications to what is necessary and blocking all other unauthorized ones. Services, users and IT systems should be appropriately segmented and segregated within the different network areas with homogeneous security requirements, to define watertight compartments with different security levels capable of isolating and confining any threats, using firewalls and specific hardware and software systems.

11- CLOUD COMPUTING – The organization, as both a cloud service customer and a cloud provider, defines that: the released applications may be provided in a cloud environment; information stored in the cloud computing environment may be subject to access and management by the cloud service provider; processes may be executed on a multi-tenant and virtualized cloud service; the cloud service customer's cloud service administrators may have privileged access; the geographical areas of the cloud resources are defined. Furthermore, the organization defines the basic information security requirements applicable to the design and implementation of the cloud service, the risks from authorized insiders, access to cloud service customer resources by the cloud service provider's personnel, access control procedures such as strong authentication for administrative access to cloud services, virtualization security requirements, the methods for accessing and protecting cloud service customers' data, and the lifecycle management of cloud service customer accounts.

12- ASSET SECURITY - All assets, including virtual cloud assets, that carry data or support information services must be located so as to be protected from accidental and environmental threats and always connected to adequate supporting utilities both inside and outside the organization's premises. All equipment must be maintained within the context of the organization's information security plan. Access to information systems for maintenance must be defined and controlled. Unattended equipment must always be left with adequate protection against both unauthorized physical access and theft and unauthorized IT access: all sessions must be locked when leaving any equipment, or equipment must be able to disconnect automatically after a defined and configured period of inactivity. No storage media must be left unattended in a workplace.

13- ACCESS CONTROL AND LIFECYCLE MANAGEMENT - Every access to the organization's systems and networks must undergo an appropriate identification, authorization and authentication procedure, periodically reviewed, which allows access only to the relevant information and functions, differentiated by role and duty (principle of least privilege). Users of systems and services must be uniquely identified through a formal registration and deregistration procedure for granting and revoking access privileges, which are periodically verified. Authentication credentials and the systems that verify them must be sufficiently robust to minimize access by unauthorized personnel (through the management of electronic signatures with two-factor authentication or digital signatures where required by specific regulations and standards). The controls necessary to define the access of the personnel managing the cloud infrastructure and the lifecycle for granting, modifying and deleting access are included.

14- MANAGEMENT OF STORAGE MEDIA - Specific restrictions must be defined and implemented for the management of all removable and portable media. Furthermore, IT system media containing information must be protected against unauthorized access, misuse or destruction when transferred outside the organization's premises. Strict procedures must be defined for the reassignment or secure disposal of media, in order to make previously stored data unrecoverable.

15- MALWARE PROTECTION - Adequate cybersecurity hardware and software systems for malware protection must be installed and kept constantly updated on all IT resources that may be infected.

16- INFORMATION TRANSFER - In the transfer and management of information, compliance with legal provisions, statutes, regulations or contractual obligations and with information security requirements and principles must be ensured, minimizing the risk of legal or administrative sanctions, significant losses or reputational damage. Information transferred via electronic messaging and IT platforms must be selected and configured to ensure confidentiality and detect attacks on these channels. The transfer of information on removable media must be minimized through security controls.

17- CRYPTOGRAPHY – Where necessary, cryptographic controls with "robust" algorithms must be developed, documented, implemented, maintained and reviewed to ensure the confidentiality of critical information both in transit and at rest. Cryptographic keys must be used, protected and stored according to strict and documented procedures throughout their entire lifecycle. This principle applies to the services offered by the organization and to the organization's suppliers.

18- SECURE CONFIGURATION AND MANAGEMENT OF IT ASSETS AND ENDPOINTS - Procedures must be defined for the secure use of IT assets, including endpoint devices, with defined configuration procedures.

19- MOBILE DEVICES AND REMOTE WORKING - Mobile devices used for work purposes must be securely configured and strictly controlled. Remote working tools must be developed with additional security protections to prevent information leaks, misuse and malware. The remote access used for this purpose must be hardened against unauthorized access.

20- BACKUP, REDUNDANCY, BUSINESS CONTINUITY - Procedures must be defined and implemented for the adequate creation and testing of backup copies of software and information. Information processing facilities must be designed and implemented to guarantee sufficient redundancy to meet availability requirements even in failure situations. A continuity plan (*business continuity*) must be in place that enables the Company to deal effectively with an unforeseen event, ensuring, through backup and redundancy systems, the restoration of critical services in times and ways that minimize the negative consequences on information security and on the processes, objectives and interests of the Company and its stakeholders (customers, collaborators, suppliers, institutions, etc.).

21- INCIDENT MANAGEMENT - Procedures must be defined and applied for the control, recording, prompt management and communication of information security incidents and their *escalation*, based on specific responsibilities approved and established by management and with interactions with the national authorities designated by regulations, where necessary. The handling methods and, where necessary, the procedures must be adapted based on the knowledge gained from the analysis and resolution of incidents (*incident lessons learned*) and from the analysis of any security weaknesses reported by users, observed or suspected. The organization has defined a breach communication process and guidelines for information sharing to support investigations and forensic analyses towards external bodies; this process complies with applicable laws and the standards applied by the organization.

22- EVENT MONITORING AND LOGGING - The events most relevant to information security must be monitored and securely stored, protected from modification and subject to regular review. All activities of system administrators and operators must be logged, as well as their successful and attempted logins/logouts.

23- SECURE DEVELOPMENT - Security aspects must be included by design in all phases of the lifecycle of IT systems and services: design, development, operation, maintenance, support and decommissioning. All the organization's projects should include information security considerations. Application service security - The information systems used to develop products and provide services must be protected from attacks through secure configurations hardened with additional security controls, and constantly monitored and protected by dedicated security devices, in proportion to their exposure to risk. Protection of the application and IT service development lifecycle - Organizations must integrate information security criteria into the development lifecycle of their applications, in order to minimize security vulnerabilities. These criteria include: the separation of development and test environments; the security criteria to be implemented in development and acceptance testing for new IT systems, their updates and maintenance; the application of the patches for software vulnerabilities made available by suppliers.

24- SEGREGATION OF CUSTOMER INFORMATION IN CLOUD ENVIRONMENTS – The organization has processes that guarantee and monitor the segregation of customer data in cloud environments, a fundamental requirement for the services offered by the Company.

25- CHANGE MANAGEMENT - All changes to the organization, processes or business and information systems that affect information security must be recorded, duly approved and tested. Changes to systems and software must be allowed only to authorized personnel. The information and communication processes towards customers for updates and changes to cloud solutions are managed.

26- AUDIT AND ASSESSMENT - Information security systems must be periodically reviewed by independent auditors. Managers must ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards. IT systems should be periodically reviewed to ensure ongoing compliance with security implementation standards.

3.6 Assignment of Responsibilities

Management is also aware that the correct management of information security concerns all aspects of the Company's life and requires the active participation of all the parties involved, and is therefore actively committed to pursuing the **competent and responsible involvement** of all the Company's collaborators involved in information management.

To achieve this objective of responsible involvement, Management undertakes to ensure that this policy is distributed, understood, accepted and implemented, through the framework of specific policies and procedures defined by the ISMS, by **all personnel, internal and external, who in any capacity collaborate with the Company and are in any way involved** with the information falling within the scope of the ISMS: *internal staff, interns, external collaborators, consultants, contracted suppliers.*

In particular, **all personnel** are required to:

- protect the confidentiality, integrity and availability of the information and intellectual resources of the Company or entrusted to the Company by third parties, also through the formal signing of *a confidentiality agreement*;
- protect all information, activities, physical assets, IT systems and resources of the Company under their responsibility or entrusted to the Company by third parties;
- formally confirm that they have received, understood and accepted this policy, where applicable:
- report to the Information Security Supervisor or to the Management Team any anomalies, weaknesses and actual or suspected security breaches they become aware of, even if not formally codified, in order to prevent and manage any incidents promptly.
- report to the Information Security Supervisor or to the Management Team any change they consider necessary to the security requirements, standards, the policy and the specific policies and procedures.

Specific responsibilities are assigned, as defined by the IMSM[4], the job descriptions[5], the organizational chart[6] and the regulations[7], to the different roles: **Management (CEO), Management Team (MT), Information Security Supervisor (ISS), Personnel.**

[4] Integrated Management System Manual – Quality and Information Security – 40FACTORY
[5] D1.2-5 – Company Job Descriptions
[6] D1.2-3 - Company Organizational Chart
[7] D1.2-8 - Regulation and Policy for IT Security

In the spirit of responsible involvement, the assignment of the development, review and approval of policies/procedures on specific information security topics to collaborators is promoted, in a manner appropriate to their role, level of authority and technical competence, while Management retains the role of final approver.

Violations of the principles and behaviours protecting information security will be pursued by the Company, in proportion to the seriousness of the infringements committed and in line with the provisions of the company **regulations**[8]**.**

3.7 Review of the Policy and of Topic-Specific Policies

The periodic ISMS review activities - internal audits, management review and annual surveillance by the accredited body for the maintenance of the certification - allow **the control of the system, its review and its continual improvement**, in response to significant changes in the Company's context: corporate strategy; factors internal to the organization; national and international standards, regulations, statutes and contracts; information security risks due to internal and external factors; lessons learned from information security events and incidents.

4 Compliance with Directive (EU) No. 2022/2555 NIS2

Following the notification carried out by the Company, it was recognized by the competent authority for Italy, ACN, as a subject *"not within the scope of NIS2"*. Nevertheless, the Organization has defined corporate objectives to meet the requirements of the NIS2 regulation in order to support its customers that fall within the scope of NIS2 as important or essential entities.

5 Compliance with Personal Data Protection: Regulation (EU) 2016/679 GDPR and ISO/IEC 27001:2022

Regarding the personal data protection policy, the Company provides its employees, collaborators, suppliers or consultants with organizational and technical instructions that ensure 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 the measures to ensure the reliability of hardware and software components for the protection of the personal data processed. Furthermore, it informs the users of products and services of the measures implemented to protect and preserve personal data through the appropriate privacy notices.

[8] D1.2-7 - Company Regulation and Policy