Annex D1.2-2
INFORMATION SECURITY POLICY

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

Ver.2	03/28/2025	Revision for extension to ISO/IEC 27017 and compliance with ISO/IEC 27002:2022/5.1	MG, MT	MT	CEO	Public
REVIEW	DATE	EDIT	REDACTED	VERIFIED	APPROVED	DISTRIBUTION

Camillo Ghelfi, CEO 40Factory

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 management of information security and the assets involved, or that may impact 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 offers a well-established product-consulting portfolio 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 processes through the intelligent and advanced exploitation of the "value" represented by machine and company data.

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

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

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 extension ISO/IEC 27017:2021 (adopted at European level as EN standards and at national Italian level as UNI/CEI standards).

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

- improving "*the ability to consistently provide products and services that meet customer requirements 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, evolution, and innovation;
- enhancing the capability to preserve "*the confidentiality, integrity, and availability of information through the application of a risk management process*"[2] to face emerging cybersecurity challenges in a context of growing technological interconnection and data-driven environments;
- ensuring "*compliance with the specified requirements of the quality management system*"[1] and with applicable legal and regulatory requirements concerning information management;
- building a solid foundation to realize 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 in an efficient and effective way, while pursuing continuous 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. Planning is based on a context analysis (considering internal and external factors as well as stakeholder needs) and applies a systematic, preventive risk-based approach that minimizes corrective actions and the occurrence of issues.

3. Information Security

3.1 The Importance of Information Security for the Company

The Company's Information Assets — which include data belonging to the company itself, its customers, and suppliers — represent the primary resource on which the company's business processes are based (ranging from market relations, the development and quality management of its products and services, the continuous innovation process, the management of all internal structures, to the products and services used by customers). Its security must be adequately ensured through a constant balance between two factors: on one hand, the accepted level of risk and the need to guarantee the efficiency, effectiveness, and continuity of processes; on the other hand, the degree of protection to be applied through a complex set of measures and controls, not solely 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 the cybersecurity risk landscape due to the growing digitalization and sharing of information through ICT infrastructures and cloud computing. This affects all stakeholders as well as the company's own organizational structure, alongside the rising threats to cybersecurity and privacy.

Given the nature of its activities, the Company's Management regards the security of the Information Assets managed by the company — in compliance with contractual obligations and new laws and regulations — as an essential factor for protecting its business. Today, this requires guarantees not only regarding the quality and innovation of the products and services provided but also the proper handling of information.

Therefore, the Company's Management considers investments in information security management to be strategic where required by the application context, as these are fundamental aspects to ensure, beyond 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 According to 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 Management System, certified by an internationally recognized body, and based on acknowledged standards and established methodologies.

The chosen certification and consulting body is Det Norske Veritas (DNV), and the regulatory framework is the ISO 27000 series, recognized internationally.

Specifically, considering 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", which is the subject of the integrated

certification with ISO 9001:2015, defines the requirements to establish and manage 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 represent the collection of best practices related to the 114 controls to be adopted based on information security risks, aimed at fully satisfying 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 guidelines **"**ISO 31000:2018 Risk management — Guidelines", general for *risk management*, which provide a common approach to risk management customizable according to the organization and context, applied by the Company to manage information security risks based on the identification of assets, threats, and vulnerabilities (*asset-based risk assessment* approach).

Within the company's ISMS, information security is achieved—starting from this General Policy and based on a structured analysis of the company's risk context—through the selection, applicability, and implementation of the comprehensive set of controls indicated by the standards and guidelines. This is accomplished via a structured and efficient system of *Policies, Responsibilities, Processes, Procedures, Organizational Structures, Hardware and Software Features, Reports, and Records for monitoring*, all specifically tailored to topics and security areas, as defined in the Integrated Management System Manual (IMSM) and its annexes [3].

In defining the ISMS, the company places particular emphasis on two key areas identified as "*focal points*" of its information security certification:

- the entire lifecycle of its products and services (design, development, release, maintenance), which represent a primary asset of the company;
- the development and management of its services that use SaaS cloud computing technologies, operating on critical customer application data and information.

Furthermore, specific attention is given to new organizational and operational methods: the structured internal adoption of smart working and the implementation of an integrated ecosystem involving the company, customers, and suppliers, based on cloud services.

3.3 Definition of Information Security

The primary objective of the ISMS is to ensure information security, meaning the protection of the fundamental "CIA+A" requirements for information classified as critical:

- Confidentiality: Information must be accessible only to authorized individuals;
- Integrity: Information must be modifiable only and exclusively by those with the appropriate rights, in order to prevent unauthorized or fraudulent modifications, including controls that enable the detection or prevention of accidental changes;
- Availability: information must be accessible and usable when required by processes and by users with the appropriate privileges, within timeframes consistent with their operational needs.
- Authenticity: Information must be authentic and not altered, falsified, or counterfeited.

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

Additionally, in specific contexts, Non-repudiation is required: actions performed on data by users and processes must be tracked in a way that prevents denial of their execution.

3.4 Objective of Information Security

With this Information Security Policy, in accordance with the measures already implemented within the Quality Management System, Management defines the following corporate objectives:

- To effectively protect the company's own information assets and those of its clients;
- To fully comply with the provisions of applicable laws and regulations;
- To improve the transparency of its services, including through the use of new cloud technologies, to facilitate the definition and management of solid and secure contracts, in compliance with applicable legal obligations;
- To optimize the processes related to the lifecycle management of its products and services;
- To safeguard the company's reputation as a reliable and competent technological partner, also in the field of information security;
- To enhance secure digital integration with stakeholders;
- To increase the company's resilience against cybersecurity threats in its operating context;
- To raise awareness, competence, and responsibility on security-related matters among its personnel.

3.5 Fundamental Principles of Information Security

Since the Company's overarching goal is to ensure the proper management of all information generated or processed throughout its processes—whether owned internally or externally—the organization has engaged all functions and corporate levels, starting from top management, in the implementation of its certified Information *Security Management System* (ISMS). This includes the adoption of the measures and controls defined by ISO 27000 standards concerning the fundamental principles of information security:

1. TRAINING AND AWARENESS - All employees, starting from the hiring phase and throughout the duration of their employment, as well as relevant third parties, must be periodically informed and made aware of the value of information and the threats to its security. They must also receive specific training, based on their roles and responsibilities, regarding the organization's information security policies and procedures.
2. PERSONNEL MANAGEMENT - Procedures must be established, in compliance with laws, regulations, and ethical conduct, for screening all employees and third-party personnel who regularly access the organization's premises, proportionate to the security risks related to the information managed. Furthermore, all employees and third-party personnel must sign non-disclosure agreements (NDAs) before engaging with the organization's information, and their contracts must require compliance with the organization's policies.
3. SUPPLIER MANAGEMENT - All suppliers, including any subcontractors, who process or exchange the Company's critical information must be contractually bound to acknowledge and comply with the applicable corporate information security policies, allowing for the execution of audits. Compliance with corporate security clauses and agreed information security service levels must be constantly monitored through formal procedures.
4. EXTERNAL CONTACTS AND COMMUNICATIONS - The organization must systematically develop monitoring activities by establishing adequate contacts both with the competent authorities—so

as to react promptly and effectively to widespread threats in a coordinated manner at national level—and with specialist interest groups, forums, or associations in order to obtain up-to-date information on current information security threats and the best practices to prevent or mitigate them.

5. LEGAL AND CONTRACTUAL REQUIREMENTS – All applicable information security requirements arising from national, international, or sector-specific regulations must be constantly monitored, as well as those deriving from contracts with third parties, with particular attention to the protection of personal and confidential data and to requirements relating to 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 regarding the use of intellectual property and proprietary software products.
7. PHYSICAL AND ENVIRONMENTAL SECURITY - Unauthorized access to the organization's premises and individual areas, as well as to its systems where information is managed, must be prevented by minimizing entry points and equipping them with physical barriers protected by access control systems. Furthermore, such premises and systems must be provided with physical protections against damage caused by natural events or any other type of disaster, whether natural or man-made (such as fire, humidity, or earthquakes).
8. ASSET MANAGEMENT - A centralized, constantly updated inventory of the Company's assets must be established and maintained, including their characteristics, the information they handle, traceability throughout their entire lifecycle, and secure usage procedures. Ownership and responsibilities must be clearly identified, documented, accepted, and enforced (including the management of all assets assigned to employees or third parties).
9. INFORMATION CLASSIFICATION, LABELLING, AND HANDLING - Information must be classified, labelled, and handled according to its confidentiality, availability, and integrity requirements, based on its value to the organization and current legislation (and thus its criticality), by all information owners within the organization.
10. NETWORK SECURITY - ICT networks, including virtual cloud networks, must be implemented and periodically tested (where necessary using Vulnerability Assessment and Penetration Testing) in order to minimize the risk of interception or tampering of network traffic. Authorized communications should be limited to what is strictly necessary, while unauthorized traffic must be blocked. Services, users, and IT systems should be appropriately segmented and segregated into different network areas with homogeneous security requirements, thereby creating isolated compartments with distinct security levels capable of containing and confining potential threats through the use of firewalls and dedicated hardware and software systems.
11. CLOUD COMPUTING – The organization, in its role as both a cloud services customer and a cloud provider, defines that: the released applications may be provided in a cloud environment; information stored within 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; cloud service customer administrators may have privileged access; the geographical areas of the cloud resources are defined. Furthermore, the organization establishes the basic information security requirements applicable to the design and implementation of the cloud service, including risks posed by 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, methods for accessing and protecting cloud service customers' data, and the management of the lifecycle of cloud service customer accounts.

12. ASSET SECURITY - All assets, including virtual cloud assets, carrying data or supporting information services must be located to be protected against accidental and environmental threats and always connected with 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 adequately protected both against unauthorized physical access and theft as well as unauthorized IT access: all sessions must be locked when leaving any equipment or be able to automatically disconnect after a defined and configured inactivity period. 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 appropriate identification, authorization, and authentication procedures, periodically reviewed, which allow access only to relevant information and functions, differentiated by role and duty (principle of least privilege). System and service users must be uniquely identified through a formal registration and deregistration procedure for granting and revoking access privileges, periodically verified. Authentication credentials and the systems verifying them must be sufficiently robust to minimize unauthorized personnel access (including management of electronic signatures with two-factor authentication or digital signatures where required by specific laws and standards). Necessary controls are included to define access for personnel managing the cloud infrastructure and the lifecycle of access issuance, modification, and revocation.
14. MANAGEMENT OF STORAGE MEDIA - Specific restrictions must be defined and implemented for managing all removable and portable media. Furthermore, IT system media containing information must be protected against unauthorized access, misuse, or destruction in case of transfer outside the organization's premises. Strict procedures must be established for secure reassignment or disposal of media to make previously stored data irrecoverable.
15. MALWARE PROTECTION - Adequate hardware and software cybersecurity systems to protect against malware 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 laws, statutes, regulations, contractual obligations, and the requirements and principles of information security must be guaranteed, 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 via removable media must be minimized through security controls.
17. CRYPTOGRAPHY – When 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 foundation applies both to 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 clearly 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. Remote access used for these purposes must be reinforced against unauthorized access.

20. BACKUP, REDUNDANCY, BUSINESS CONTINUITY - Procedures must be defined and implemented to ensure proper creation and testing of backup copies of software and information. Information processing infrastructures must be designed and implemented to guarantee sufficient redundancy to meet availability requirements even in failure situations. A *business continuity* plan must be established to enable the company to effectively handle unforeseen events, ensuring through backup and redundancy systems the restoration of critical services in a timely manner and in ways that minimize negative impacts on information security, 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, logging, prompt management, and communication of information security incidents and their *escalation*, based on specific responsibilities approved and established by management, including interactions with national authorities mandated and indicated by regulations, when necessary. Incident handling methods and, if necessary, procedures must be adapted based on knowledge gained from incident analysis and resolution ("*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 assist investigations and forensic analyses by external entities; this process complies with applicable laws and organizational standards.
22. EVENT MONITORING AND LOGGING - The most relevant events for information security must be monitored and securely stored, protected against modification, and subject to regular review. All activities of system administrators and operators must be logged, including 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 organizational projects should include information security considerations. *Application service security* – Information systems used to develop products and provide services must be protected from attacks through secure configurations reinforced with additional security controls and continuously monitored and protected by dedicated security devices, proportionate to their exposure to risk.

    Protection of the application and IT service development lifecycle – Organizations must integrate information security criteria into the lifecycle of their application development to minimize security vulnerabilities. These criteria include separation of development and testing environments; security criteria to be implemented in development and acceptance testing of new IT systems, updates, and maintenance; application of patches for software vulnerabilities provided by vendors.
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 IT systems that affect information security must be recorded, duly approved, and tested. System and software changes must only be allowed by authorized personnel. Processes for informing and communicating with customers regarding updates and changes to cloud solutions are managed.
26. AUDIT E ASSESSMENT - Information security systems must be periodically reviewed by independent auditors. Managers must ensure that all security procedures within their area of responsibility are correctly performed 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 proper management of information security concerns all aspects of the Company's operations and requires the active participation of all involved parties. Therefore, Management is fully committed to ensuring the competent and responsible involvement of all Company personnel engaged in information management.

To achieve this goal of responsible engagement, Management commits to ensuring that this policy is distributed, understood, accepted, and implemented by all internal and external personnel who, in any capacity, collaborate with the Company and are involved in any way with information falling within the scope of the Information Security Management System (ISMS). This includes *internal staff, interns, external collaborators, consultants, and contracted suppliers.*
Specifically, all personnel are required to:

- Protect the confidentiality, integrity, and availability of the Company's information and intellectual property, as well as those entrusted to the Company by third parties, including through the formal signing of a *confidentiality agreement*;
- Safeguard 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 Officer or Management Team any anomalies, weaknesses, or actual or suspected security breaches they become aware of, even if not formally documented, to enable timely prevention and management of incidents;
- Notify the Information Security Officer or Management Team of any necessary changes they believe should be made to security requirements, standards, policies, and specific procedures.

Specific responsibilities are assigned, as defined by the ISMS Manual[4], the job descriptions[5], the organizational chart[6] and the regulations[7] to the various roles: Management (CEO), Management Team (MT), Information Security Officer (ISO), and Personnel.

In the spirit of responsible engagement, the assignment of development, review, and approval of policies and procedures related to specific information security topics is promoted among collaborators, in a manner appropriate to their role, level of authority, and technical expertise, while the Management retains the final approval authority.

Violations of the principles and behaviors safeguarding information security will be addressed by the Company proportionally to the severity of the infractions committed and in accordance with the provisions established in the company regulations[8].

3.7 Review of the Policy and Specific Policies by Topic

The periodic review activities of the ISMS—including internal audits, management reviews, and annual surveillance by the accredited body for certification maintenance—enable the monitoring, revision, and continuous improvement of the system. This process responds to significant changes in the Company's context such as: the corporate strategy; internal organizational factors; national and international standards, regulations, statutes, and contracts; information security risks arising from internal and

[4] Integrated Management System Manual for Quality and Information Security – 40FACTORY
[5] D1.2-5 – Company Job Descriptions
[6] D1.2-4 - Named Organizational Chart
[7] S4.2-6 - Regulation and Policy for IT Security
[8] D1.2-7 - Company Regulation and Policy

external factors; and lessons learned from information security events and incidents.

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

Following the notification activity carried out by the Company, it was recognized by the relevant European 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 clients who fall under the NIS2 scope 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 related to personal data protection. For these obligations, it outlines the security framework adopted for the information system and defines all measures necessary to guarantee the reliability of hardware and software components to safeguard the personal data processed. Furthermore, it informs users of products and services about the measures implemented to protect and preserve personal data through appropriate privacy notices.