INFORMATION SECURITY MANAGEMENT SYSTEM POLICY

FOMA S.p.A. has set itself the goal of making its brand, which we proudly imprint on every piece we deliver, a symbol of pride and satisfaction for our customers.

To achieve and maintain its goals, the company adopts a Quality Management System based on ISO 9001 and IATF 16949 standards. We have named this organised, methodical, ingenious and collectively intelligent production system 'Foma Quality Production System'.

In this context, the digitalisation of our processes plays an increasingly important role. We have long been living in the digital age, where technological innovation goes hand in hand with IT innovation. It is, therefore, essential to work to ensure to our stakeholders, particularly our customers, an adequate management of information security and the continuity of the supporting IT (Information Technology) and OT (Operational Technology) processes.

GUIDELINES AND OBJECTIVES

- Adopt and maintain an effective Information Security Management System (ISMS) that complies with the international standard UNI CEI EN ISO/IEC 27001:2024+A1:2024, in compliance with the legal requirements of the applicable regulations and in compliance with other requirements that the Company decides to voluntarily subscribe to.
- Maintain the third-party certification of the ISMS in accordance with the international standard UNI CEI EN ISO/IEC 27001:2024+A1:2024 in the IT (Information Technology) area and proceed with the evaluation of the opportunity and possibility of extending the certification also in the OT (Operational Technology) area, in the next three years.
- Define, in the context of the information security, the responsibilities assigned to all corporate functions, in particular in the person of the Information Security Officer and the ISMS, verifying that they are understood and applied.
- Ensuring the availability of the resources, information and knowledge necessary for the operation and control of IT processes and the ISMS, through periodic training activities aimed at informing employees of the relevance and importance of their activities and how they contribute to improving the performance of the ISMS and thus to information security.
- Motivate and involve all personnel so that they become increasingly aware of the importance of their role and their contribution to the effectiveness of the ISMS; promote shared values and correct models of behaviour to reduce the risks related to the activities performed.
- Comprehend and strengthen the relationship with Customers and all Stakeholders, by understanding their information security needs and improving their degree of trust in the Company.
- Commit to minimising the environmental impacts of operations through a continuous process of improving the company's environmental policies, programmes and behaviour, considering advances in technology, scientific knowledge and community expectations.
- Define improvement goals in the context of the information security and periodically monitor the achieved results.
- Identify the causes of non-compliance and ensure rapid and effective responses.
- Define and disseminate clear documented information to ensure the effective and efficient operation of IT processes and information security governance through the ISMS.
- Carry out audits to measure the implementation and effectiveness of the ISMS and its compliance with this Policy, ensuring that appropriate corrective actions are taken to remove any causes of inadequacy.
- Select and qualify suppliers of products and services that have an impact on the final quality of processes and information security, involving them, to the extent of their competence, in the achievement of corporate objectives.
- Identify digital innovation needs to ensure a high level of service combined with an adequate level of information security.

Managers must implement and disseminate the commitments and directives listed above, and develop activities aimed at achieving the company's objectives and continuously improving the effectiveness of the ISMS.

Publication date	06/11/2024
Class information	Public
Expiry date	03/11/2027
Document category	D101_030

Editorial staff		Approval	
Chiarini Matteo	04/11/2024	Bertilotti Andrea	04/11/2024

REVISION HISTORY

REVIEW	DATE	DESCRIPTION
0	26/10/2021	New issue
1	05/04/2023	Company logo change
2	12/10/2023	Adaptation to the OT (Operational Technology) security environment.
3	06/11/2024	New revision