



Version Nr.	Author	Writing date	Approved by	Approval date
0	Melissa Conte	02/10/2023	DIREZIONE	02/10/2023

CORPORATE POLICY

The management of MODO Network S.r.l. has defined this Corporate Policy and is committed to:

- Keeping it active by periodically reviewing and updating it;
- Providing the necessary resources for the effective protection of information;
- Defining objectives related to information security;
- Disseminating it to all levels of the organization;

The application of the management system requires the full participation, commitment, and interaction of all human and technological resources.

All individuals operating within the company to achieve corporate objectives are required, without exception, to comply with this policy in the handling of data and in the management of business activities in order to ensure the security and quality of processes, customer satisfaction, of the general market and compliance with current regulations.

The purpose is to:

1. Ensure the protection and defense against all threats, whether internal or external, intentional or accidental, of information within the scope of their activities, in accordance with ISO/IEC 27001 standards and ISO/IEC 27002 guidelines.
2. Ensure the protection and defense of data in accordance with the provisions of the European General Data Protection Regulation (GDPR 679/16).
3. Ensure continuous improvement of processes and the Corporate Management System through periodic assessment of business risks, allowing control and adaptation to changes in management, environmental, business, and legal contexts that the company may face.
4. Ensure the satisfaction of market and stakeholder needs.
5. Ensure compliance with all applicable legal requirements.
6. Ensure the training of personnel through participation in training programs aimed at developing and improving skills.
7. Ensure the maintenance and improvement of relationships with business partners, including suppliers of products and services, to provide the highest level of quality to customers.

It is therefore necessary to ensure:

1. Confidentiality of data, meaning that data should only be accessible to authorized individuals.
2. Data integrity, meaning ensuring the accuracy and completeness of data and the methods for their processing.



3. Data availability, meaning that only authorized users can effectively access data when needed. Communication and dissemination of data to external parties should only occur for the proper conduct of business activities, in compliance with rules and legal requirements.
4. Compliance with legal requirements and principles related to data security in contracts with third parties.
5. Compliance with legal provisions, statutes, regulations, and contractual obligations, as well as any requirements related to data security.
6. Security aspects must be included in all stages of system design, development, operation, maintenance, support, and decommissioning.
7. Every access to systems must undergo an identification and authentication procedure to prevent unauthorized access to company premises and individual locations where data is managed, and equipment security must be ensured.
8. Access permissions to data must be differentiated based on individuals' roles and responsibilities so that each user can access only the data they need, and permissions must be periodically reviewed.
9. Any security-related incidents must be promptly managed, meaning that everyone must report any security-related issues.
10. Company procedures must be followed.
11. Necessary tests must be conducted to ensure the correct functioning, adequacy, and security of service processes.

MODO NETWORK SRL
Board of Management