	INFORMATION SECURITY POLICY	Use: Internal
Department: DIREZIONE - IT	ITMD-02-01	R00 – 26/07/2024

INFORMATION SECURITY POLICY

The Information Security Policy aims to provide management guidelines and support for the proper management of information security, being applied within all offices and operational units of Italcarrrelli S.p.A. The Company considers the information managed as an integral part of its assets. In this regard, it sets the essential goal of safeguarding the security of its information assets from any intentional or accidental threat, internal or external, protecting the confidentiality, integrity, availability, and authenticity of the information produced, collected, or otherwise processed.

The Policy, which everyone must adhere to in relation to their role and responsibilities within the company, outlines the principles that the Company is inspired by.

For the definition of the Policy, the Company has first defined its commitments and objectives regarding information security.

To pursue corporate objectives, the information processed must meet the requirements of:


- Confidentiality: information must be known only by those who have the right to it, respecting the principle of least privilege (“need to know”) based on the roles performed (“need to operate”);
- Integrity: information must be accurate and complete, must respect corporate values and expectations, and must be protected from unauthorized modifications and deletions. To meet this requirement, information must be exact, up-to-date, and readable;
- Availability: information must be available when required by business processes, in an effective and efficient manner.
- Personal data must be processed:
- In compliance with confidentiality criteria;
- Lawfully and fairly;
- For a period not exceeding that necessary for the purposes for which they were collected or subsequently processed;
- In full compliance with minimum security measures, storing and controlling the data being processed to avoid risks, even accidental, of destruction or loss, unauthorized access, or processing not allowed or not in line with the purposes of the collection.

To achieve the set objectives, the Company commits to:

- Ensuring that personnel and collaborators have adequate knowledge and awareness of the principles and risks related to information security, to enable them to acquire sufficient awareness of their responsibility and role in processing information;
- Ensuring that all external suppliers are aware of the risks related to information security and commit to respecting the security policy adopted by the Company;
- Establishing guidelines for the application of standards, procedures, and systems for managing and protecting information;
- Increasing awareness and sensitivity of users of corporate devices and tools, defining a precise scheme of rules and procedures aimed at the correct management of information;
- Ensuring that recipients are aware of the adopted data protection rules and their implications, as well as the methods of applying the measures provided, as referred to in the operational security procedures;
- Ensuring that the risk management process adopted by the company is adequately monitored and periodically updated in light of the parameters contemplated within the ISMS regulations;
- Ensuring that, for each operational function of the company, specific criteria for identifying, evaluating, and managing risk are defined and implemented, based on the type of activity performed.

The Information Security Policy concerns the management and use of the information system in all its aspects. The Policy is disseminated to partners, contractors, and suppliers of goods and services, and they are actively involved in its application and in pursuing their improvement objectives, also ensuring and monitoring compliance with internal regulations and information security legislation.

The Company implements the Policy through the definition of specific performance objectives, for which plans, programs, and implementation procedures are formulated. The Company monitors and measures these performances and the related results, in relation to the defined objectives. It is the responsibility of the personnel and all those acting on behalf of the Company to respect the

	INFORMATION SECURITY POLICY	Use: Internal
Department: DIREZIONE - IT	ITMD-02-01	R00 – 26/07/2024

responsibilities and commit to achieving the continuous improvement objectives of performance in information security, reporting any situation not in line with the commitments and principles mentioned above or that may pose risks to information security. The Information Security Policy is approved by the Management and communicated within the organization (via the HRPeople portal) and made available to other interested parties, where appropriate.

In our commitment to excellence in information security management, we are dedicated to the continuous improvement of our Information Security Management System (ISMS). Through a constant process of monitoring, evaluation, and review, we ensure that our practices, procedures, and controls are always updated and improved to address new threats and challenges. Our goal is to ensure the protection of corporate data and information, fully complying with legal and regulatory requirements, and promoting a culture of security within the organization.

Chiampo, 26/07/2024

Italcarrelli SpA
Ivan Lambertucci