TESISQUARE® business aim is to create collaborative solutions between business partner and suppliers by means of infrastructural technologies able to allow the partners themselves to achieve their business objectives efficiently and effectively.

Following the International and National regulations, TESISQUARE® has adopted an Information Security Management System (ISMS) for the following field of application:
Design and provision of solutions for: supplier relationship management, collaborative transportation management, customer collaboration, dematerialization and optimization of business processes, electronic invoicing, EDI services, compliant document storage.

The Information Security Management System (ISMS) aims at:

- **ensure the confidentiality, integrity and availability** of information to third parties;
- **minimize the impact** on business activities in case a security incident happens;
- **guarantee the continuity of services** as defined by current regulations and contractual SLAs;
- **continuously improve information security** by taking into account the technological evolution.

This policy is shared by the ISMS Top Management with interested parties. It is also shared with all the areas included in the perimeter of the certification
TESISQUARE® has defined the security objectives of its ISMS; these objectives are constantly uploaded during the Top Management meeting or if requested by the ISMS management.
According to the specific third parts requests TESISQUARE®, provides services ensuring adequate levels of security and minimizing the risks deriving from threats to information security
Moreover, TESISQUARE® is committed to a constant improvement of ISMS, considering the following points:

- **Business strategies** – Business strategies are defined considering market needs, current legislation, contracts and other regulation and guidelines;
- **Environmental impact and climate change** - In managing the Information Security System, measures are taken to mitigate the impact of climate change. The consequences of climate change, such as extreme weather events or prolonged interruptions to essential services, can significantly affect the operational capacity of organizations, exposing information systems to potential vulnerabilities in terms of data availability, integrity and confidentiality. For this reason, such risk scenarios are considered in the information security impact analysis.
- **Actual and future risk scenarios** – The risk scenarios are preventively subjected to the Top Management examination, in order to establish the consistency of the countermeasures in place with the evolution and needs of the market;
- **Defined roles and responsibilities** - Role, responsibilities and specific powers for ISMS human resources are specified and disclosed to collaborators by means of documents;
- **Training and Information Plan –** All the people working in the areas of the context subject to certification are trained through specific training sessions and / or organizational provisions;
- **Audit Planning** - The ISMS is subject to periodic audits to ensure its effectiveness and compliance.

The TESISQUARE® management undertakes to:

- periodically review this Information Security Policy;
- keep this Policy conformable to its company business model and to its organization;
- orienting its own strategies in order to obtain a continuous improvement;
- make adequate resources available to achieve the objectives of the ISMS.

ISMS Top Management

Guido Ferrero
Massimo Crivello
Gianluca Giaccardi

TESISQUARE S.p.A.
Registered office: Via Mendicità Istruita, 24 – 12042 Bra (CN) - Headquarters: Via Savigliano, 48 - 12062 Roreto di Cherasco (CN)
Phone +39 0172 476301 - Fax +39 0172 476399 - www.tesisquare.com - info@tesisquare.com
Tax Code and VAT no. IT02448510046 – Cuneo Chamber of Commerce - Economic and Administrative Register no. 177331 -
Share Capital € 750,000 fully vested