As part of the implementation of its information security management system, compliant with **UNI CEI ISO/IEC 27001** standard and in consideration of the strategic importance that it has for the Company's business, as RIMSA Management, we have adopted an appropriate security policy.

We are aware that information security management is a complex cultural process that involves the human resources assigned to all organizational units within the certification perimeter.

We believe that information security is the result of a set of scientific, technological, organizational, procedural, relational and communication elements, in which a decisive role is played by human variables that interact strongly in production processes and which translates into a constant commitment to the centrality of users and the improvement of their services.

The principles on which we base our Information Security system are:

- **INFORMATION SECURITY BY DESIGN**
  Understood as a way of operating by default within our Organization. The principles of Information Security by Design are applied to all types of information, and can be summarized in:
  - Proactivity not reactivity (prevent not correct): anticipate and prevent events that may cause damage to information before they occur.
  - Information Security incorporated into the design: an essential component for the realization of the functional core of our data processing and protection system.
  - Maximum functionality: Reconciling all legitimate interests and common goals with “win-win” positive value modes.
  - Security: Extending the system throughout the entire lifecycle of information to ensure that information is carefully stored and then securely destroyed at the end of the process.
  - Visibility and transparency: established information and objectives, subject to independent verification.
  - Respect for customer information: Prioritize customer interests by offering effective default information security interventions that are appropriate, confidential, intact, and available.
  - Use, if necessary, certified Cloud services that guarantee our organization and our customers/clients not only the security of information, but also the protection of the data contained therein.

- **INFORMATION SECURITY BY DEFAULT**
  Information Security by default: achieving the highest level of information protection by ensuring that Confidentiality, Integrity and Availability are automatically guaranteed in any system.
  RIMSA, puts in place mechanisms to ensure that:
  - information is not made accessible to an indefinite number of persons, with the exception of information of a public nature.
  - the media (software, hardware, digital and non-digital) that contain information, including any Cloud services, are mapped.
  - information redundancy policies are implemented to ensure its availability at all times.
  - the resources that can access the information are identified, as per the provisions on the protection of personal data in accordance with current legislation.
  - Geographically, the data will be stored in compliance with the GDPR, on the Italian territory or in the European Union.

- **INFORMATION SECURITY**
  Understood as the protection of information from:
  - "destructive" forces,
  - unwanted actions of unauthorized users,
  - accidental or fraudulent modifications.

And it is precisely through the constant application of these principles that we want to pursue our objectives and therefore it is essential for us:

- To guarantee the satisfaction and peace of mind of our members and customers because they are aware that for us the respect and security of their information and data is an indispensable element regardless of market logic;
- Ensure adequate protection of information in terms of confidentiality, integrity and availability;
- Protect the interest of customers, employees and third parties;
- Ensure compliance with applicable laws and regulations on the processing and protection of information and personal data in accordance with current legislation;
- Guarantee staff and collaborators adequate knowledge and degree of awareness of the problems related to information security, in order to acquire sufficient awareness of their responsibilities regarding its processing;
- Ensure that all external providers are aware of information security issues and comply with the security policy adopted, including cloud service providers who must ensure the security, integrity and availability of information and personal data stored on their servers;
- Establish precise rules for the application of standards, procedures and systems to implement the Information Security Management System (ISMS) and therefore be ready to respond to the constant new challenges and threats that the cyber world offers us;
- adopt the ISO 27002 standard – "Information Technology -- Security Techniques -- Code of Practice for Information Security Controls", as the standard for the implementation of the information security management system and pursue compliance;
- ensure that all personnel are aware of the technical and organisational rules in the use of company information systems described in the management system procedures;
- ensure that all staff are informed of their responsibility in handling information;
- Use adequate resources and technologies, which guarantee the result of the services;
- To guarantee security conditions in any type of activity or phase of processing of personal and sensitive data:
  - **Confidentiality:** Information should only be accessible to those who are authorized to access it.
  - **Integrity:** Information must be accurate and complete, and changes to information must be authorized and traceable.
  - **Availability:** Information should be available to authorized users when needed.

To achieve these objectives and intentions, **RIMSA** undertakes:

- to develop, maintain, control and constantly improve the Information Security Management System (hereinafter referred to as ISMS), in accordance with the ISO/IEC 27001 standard capable of meeting the declared requirements and continuously improving the effectiveness, reliability and availability of the IT services provided and of the primary and ancillary processes.
- the drafting, updating and control of development plans so that IT infrastructures and services support business activities, adopting appropriate security policies.
- the secure storage of the information managed, including the information of our customers / principals.
- the adequate definition of the technical content of the services provided (service specifications) which is reflected in a series of specialized regulatory references including IT protocols and technical-scientific documentation.

- the qualification and competence of the personnel in charge.
- the correct execution of investigation, analysis (including experimental), design and assistance activities, essential prerequisites for the validity of the services provided, ensured by the competence and reliability of the staff, according to validated and recognized protocols and, in the alternative, the compliance of the system with the ISO/IEC 27001 standard.
- to provide a structural framework for establishing and reviewing information security objectives.
- to disseminate the principles and values declared in the company policy by the organization and to make communication to and from the various interested parties active and effective so that it is understood and participated.
- compliance with rules and laws governing the services and the processing of related data and keeping the security of all records and information managed under control.
- to periodically review its policy and objectives whenever necessary, following the implementation of changes that affect it, to ascertain their continued suitability and to implement its commitment to continuous improvement.
- to disseminate the principles and values declared in the company policy by the organization and to make communication to and from the various interested parties active and effective so that it is understood and participated.

to carry out training in the field of information security and privacy for all staff

The Management
RIMSA P. LONGONI SRL