The “Security Policy” is aimed at:

1. Establishing general principles of action to ensure an adequate level of security and protection of people and assets (“physical security”), data and information (“information security”) from threats deriving from endogenous and exogenous adverse situations and behaviors;
2. Confirming the commitment to protect constantly people and corporate assets (property, data and information) according to current legislation;
3. Outlining a Security model to guarantee negative events risk reduction, minimizing probability and impact, and an efficient crisis management, should they occur.

To this purpose, RINA conducts the following Security activities:

a) The assessment of Security risks related to corporate assets and people, on the basis of recognized risk assessment methodologies, in order to adopt suitable mitigation measures;

b) The management of physical security in compliance with applicable international and national regulations and reference standards, including the Universal Declaration of Human Rights and the Voluntary Principles on Security and Human Rights;

c) The adoption of a business travel risk management program, including the assessment of security risks for travelers in risk areas and criteria for the adoption of Security protocols to minimize them;

d) The management of information security to minimize breaches of data confidentiality, integrity and availability due to endogenous and exogenous adverse actions;

e) Business intelligence and Third Party Due Diligence, to perform - in compliance with the Ethical Code and in the cases referred to RINA internal procedures – information checks assessing the reliability of natural and legal persons;

f) A protection program for the CEO and RINA top management to ensure continuity in the management and strategic guidance of the company;

g) The promotion of Security awareness through internal communication tools and specific training courses.

Regarding information security, RINA adopts a certified management system according to ISO27001 pursuing the following specific goals:

i. To protect corporate assets by ensuring the confidentiality, integrity and availability of information and the systems used to manage it;

ii. To ensure compliance with applicable national and international regulations and the highest reference standards;

iii. To assess inherent risks related to information security and manage residual risks following mitigation and control measures taken to reduce risks to an “As Low As Reasonably Practicable” (ALARP) level;

iv. To ensure business continuity through initiatives to improve resilience and effective incident management;

v. To pursue continuous improvement of the Information Security Management System by periodically reviewing its adequacy and effectiveness through internal control activities and audits conducted by accredited external bodies.

This document applies to all RINA SpA subsidiary companies, according to law.

This Policy is subject to review at least every three years and whenever deemed necessary, in order to ensure that the management of Security risks is efficiently implemented within the organization.

Ugo Salerno
Chief Executive Officer and Managing Director