SECURITY POLICY

RINA considers the security of people and company's assets as a priority.

According to the Ethical Code and the internationally recognized duty of care principle, RINA Group is committed to give to its people a prospect of stability and security. Security activities are aimed at ensuring the protection of the people present in company premises and of company's assets from threats deriving from adverse behaviors that could cause direct or indirect damages to RINA people, assets and reputation.

RINA adopts a security model suitable to guarantee appropriate risk mitigation and effective crisis management. This through solutions that can minimize the impact and probability of negative events that might occur.

In line with the above-mentioned principles, the objective to protect the Group's personnel, assets, information and reputation from potential security threats is realized through the following activities:

i. The assessment of security risks related to assets, projects and activities, on the basis of recognized risk assessment methodologies, in order to adopt suitable mitigation measures;

ii. The management of the security of people and company's assets, in compliance with applicable international and national regulations, with particular reference to the Universal Declaration of Human Rights and the Voluntary Principles on Security and Human Rights;

iii. The adoption of a business travel risk management program, including the assessment of related security risks and criteria for the adoption of security protocols able to minimize them;

iv. Crisis Management, to ensure consistent and coherent response in case of possible security emergencies and crisis, and guarantee business continuity;

v. Information Security, to avoid the improper use of all information, both physical and digital, relating to personnel, to third parties and to company activities as specified in the Information Security Addendum;

vi. Business intelligence, to perform - in compliance with the Ethical Code and in the cases provided for by RINA internal procedures - information checks assessing the reliability of natural and legal persons.

This Policy will be annually reviewed, in order to ensure that security risk management is efficiently implemented within the organization of RINA.

Genova, 9th September 2019

Chairman & CEO

(Ugo Salerno)

SECURITY POLICY

Information Security Addendum

Information is a critical asset for RINA and its stakeholders, in consideration of Company business activities in the TIC (testing, inspection and certification) and consulting engineering services. Breaches to the confidentiality, integrity or availability of RINA information, deriving from either endogenous or exogenous sources, may lead to relevant impact for RINA itself and its stakeholders, including financial and reputational losses.

RINA is committed to ensure that interested parties manage sensitive and confidential company information to avoid its improper use and to guarantee an appropriate confidentiality, integrity and availability of data.

For the purpose of this Policy, Company Information means all the information directly and/or indirectly relevant to the nature and activity of the Company, which are generally property of the Company itself. Information means any group of data, paper, public statements used in performing the company activity (such as document, videos, etc.). Information can be loaded in any media suitable to gather and store groups of data, such as paper or data storage.

In order to implement the above, RINA adopts an information security management system according to best international standards and in compliance with ISO 27001, consisting of a comprehensive set of organizational, procedural and security measures.

RINA adopted an organizational structure to manage the information security risk, enforce relevant procedures, and implement control measures. RINA managers in all operational units are responsible to oversee information security within their respective areas of responsibility. All RINA personnel have to comply with internal regulations and procedures and must ensure, to the extent of their responsibility, that company information is managed accordingly.

RINA is committed to ensure that all personnel receive security training relevant to the activity and scope of information managed and to ensure that at all time is maintained an appropriate level of awareness on information security risks as well as on internal policies and procedures.

RINA periodically reviews the performance indicators of the Information Security Management System and is committed to continuous improvement. The objectives are to ensure that the risk exposure is aligned with company strategies and objectives and that corrective actions are implemented, as needed.

All Information Security activities are conducted in full compliance with any applicable legislation and best international standards.

This Addendum will be periodically reviewed, in order to ensure that it is aligned with RINA strategy and organization.

Genova, 9th September 2019