2025

RNE INFORMATION SECURITY STRATEGY STATEMENT

RailNetEurope (RNE) is dedicated to protecting its activities supporting rail transportation through a robust Information Security Strategy aligned with its mission to harmonize processes, support international rail traffic competitiveness, and promote cooperation. The Information Security Strategy is based on four main pillars: ISO 27001 conformity, risk orientation, economical sustainability and cyber resilience, which ensure consistency with the Association's founding objectives.

At the core of RNE's Information Security Strategy is the implementation and operation of an information security management system (ISMS) in accordance with both the international standard ISO 27001 and the legislative environment (EU and national) with the primary objective of protecting the confidentiality, integrity, availability and authenticity of information, data and IT systems through technical and organizational measures.

The Information Security Strategy and all policies, rules, and work instructions integrally associated with it as part of the ISMS form the basis for creating a common awareness of information and cyber security for all RNE employees, members and partners and ensure a minimum standard for risk-appropriate and economically reasonable measures. They therefore create a basis for targeted business activities, continuous improvement and further development of the ISMS as well as cyber resilience.

The RNE General Assembly considers that it is a key task to foster awareness of responsibility, information security and risk among RNE employees, members and partners and to regulate the responsibilities and processes for all relevant activities. The Association's processes follow a risk-oriented approach; they are continuously reviewed for appropriateness and risk characteristics and managed through measures.

The RNE General Assembly considers that it its duty to ensure compliance with applicable laws and the protection of internal and confidential information, personal data and the contractual terms agreed with its members and customers.

In this context, the performance and responsibilities of suppliers, partners and (sub)contractors are also regularly reviewed and all necessary obligations to authorities are fulfilled in an appropriate manner.

Therefore, the RNE Joint Office Board (JOB) shall define both clear information security objectives and the requirements for effective risk management within the ISMS' framework of corporate guidelines - in form of an Information Security Policy and subordinate work instructions - and

Austria Campus 3
Jakov-Lind-Straße 5
AT-1020 Vienna

Phone: +43 1 907 62 72 00
E-Mail: mailbox@rne.eu

www.rne.eu

periodically assesses these for their appropriateness and effectiveness as part of an annual management review of the ISMS.

RNE JOB must demonstrate its leadership responsibility and commitment to establishing, maintaining, testing the effectiveness of, and continuously improving the ISMS and provides the necessary resources.

In this context, the following factors are ensured for the effective implementation of information security management and for the operation and control of security processes, which are continuously steered and supervised by the CIO in cooperation with RNE Joint Office Board and periodically reported to the Management Board:

- Resources (people, infrastructure, knowledge, etc.)
- Competence (education, training, experience, etc.)
- Awareness (publications, sensitization, risk culture, etc.)
- Communication (internal and external communication guidelines, etc.)
- Documented information (information security processes and rule's structure)

RNE's Information Security Strategy ensures a resilient and secure environment for RNE activities for its activities through robust governance, continuous improvement, and alignment with ISO 27001 standard and legislative requirements. By fostering a culture of responsibility and risk awareness among employees, partners, and suppliers, RNE aims to safeguard critical information assets. This strategy underscores RNE's commitment to harmonized processes, cyber resilience, and the protection of data integrity, enabling the Association to meet its mission and operational objectives effectively.