Rail Cargo Hungaria
Member of ÖBB

Rail Cargo Hungaria Zrt.'s Information Security Policy

As a member of the Rail Cargo Group, Rail Cargo Hungaria Zrt is part of of Europe's leading rail freight group. Aiming for a strategic partnership, we meet the expectations of our stakeholders in a reliable, safe, cost-effective and environmentally friendly way.

Managing information security, including IT security has a key role in the company's business processes.

Rail Cargo Hungaria Zrt ensures that the protection and security of the information held by the company is locked, comprehensive, and implemented on an ongoing basis and proportionate to the risks, in accordance with the following principles:

- **confidentiality:** data and information stored in an electronic information system may be accessed, used or disposed of only by those authorised to do so and only according to the level of authorisation;
- **integrity:** the content and properties of the stored data are as expected, including the certainty that it originates from the expected source (authenticity), that the origin can be verified and established (non-repudiation), and the property of the elements of the electronic information system that the elements of the electronic information system can be used as intended;
- **availability:** electronic information systems are accessible to the authorised person and the data processed therein can be used at a specified place and time.

In order to achieve our aims:

- we operate in compliance with applicable laws, official regulations, standards and other obligations,
- our company is run by **managers and staff committed to the continuous improvement** of our information security management system,
- we maintain ongoing communication with our employees, customers, and all stakeholders to ensure that they understand our integrated governance policy, our goals and programs, and that we take into account **our stakeholders' information security requirements**,
- we continuously assess and improve our processes, with a particular focus on information security,
- we identify our information security **risks** and **opportunities** and then continuously assess and manage them to achieve the expected results and prevent unintended consequences,
- we implement and maintain **appropriate control and protection mechanisms** to maintain information security,
- we provide our staff with the appropriate level of **regular training** to ensure that their activities are carried out to a high standard and in compliance with information security rules.

Our company has implemented, operates responsibly and continuously improves a system that meets the requirements of the ISO standard 27001:2013 Information Technology. Security Engineering. Information Security Management Systems.

Budapest, 31. May 2022.

Norbert Körös
Member of Board of Directors, CEO