Engineering progress
Enhancing lives

REHAU Group
Information Security Policy

Document Owner: REHAU Group CISO Document
Version: 2
Approved: 07/20/2023
Classification: PUBLIC

Preamble
The REHAU Group (hereinafter also referred to as "REHAU") understands that effective information security management is crucial for the sustainable success of our company. It helps us fulfil our legal requirements, comply with contractual obligations, and reduce business risks and potential damage to the company image.

We are committed to fulfilling our responsibilities in this area. We achieve this through the following:

- Compliance with legal regulations and company-wide guidelines.
- Expert resources for planning, implementing, monitoring, measuring, and checking operational effectiveness.
- A management structure with a clear definition of responsibilities in terms of information security.
- Internal communication and training that promotes appropriate conduct and actions.

The Group's Supervisory Board actively promotes information security and provides the resources required to implement a consistent information security policy.

Scope of application
The information security principles contained herein apply throughout the Group without exception. However, if more restrictive local legal regulations apply, they always take precedence.

Security goals
The responsible handling of information concerning business partners and employees, as well as the company's own information, is an integral part of our activities. We protect all information appropriately, taking into account its value based on the information security objectives of confidentiality, integrity, and availability

- REHAU receives and safeguards the know-how and intellectual property developed in an innovation and technology-driven environment against loss of confidentiality.
- REHAU observes regulatory, normative, and customer-specific requirements regarding information security and protects information accordingly.
- REHAU ensures the highest integrity of all information systems in the core and management processes in order to maintain our quality standards.
- REHAU protects the information systems that are required to maintain the value chain.
- REHAU takes timely precautions to deal with disruptions and restrictions in the IT process in order to resolve disruptions and emergencies within the defined maximum restart time.
- REHAU ensures that employees have a sense of responsibility. Negligence could harm the company. For this reason, REHAU provides training and awareness-raising measures to employees.

Basics of security process
To achieve its security goals, REHAU bases the group-wide regulations in the area of information security on international standards (e.g. ISO/IEC 27001) and defines responsibilities at both a global and local level. REHAU has guidelines on the systematic analysis and fulfillment of requirements, as well as the proactive reduction of risks arising in cyberspace. The divisions also implement the specified guidelines. This includes the following elements in particular:

Introduction and operation of an information security management system (ISMS)
The divisions use written processes to define, implement, execute, monitor, check, maintain, and continuously improve an ISMS.

The ISMS follows a risk-oriented approach. For this purpose, a method for identifying and evaluating information security risks, including the interface to the Group's strategic risk management, has been defined. The responsible bodies report identified risks via the defined reporting channels. They approve measures to reduce risk, document them in an action plan, and arrange for implementation within the defined time frame.

Monitoring/management review
The responsible bodies monitor the achievement of defined security goals, compliance with the ISMS processes, and the effectiveness of protective measures by means of a key figure system, among other tools. They initiate measures to eliminate identified deviations and, in the event of significant disruptions or delays, they escalate these incidents to the executive management of the respective division.

Continuous improvement
The REHAU Group continuously reviews and improves its processes and protective measures for information security and aligns them with international standards and best practices. Internal and external requirements are taken into account.

Security organization

The Director Group Information Security Management (Group CISO) is responsible for the implementation and ongoing development of the REHAU information security policy and the information security management framework at the group level.

The CISO Council supports the standardization and continuous improvement of information security management in the REHAU Group and prepares decision templates for the relevant committees.

The divisions appoint Chief Information Security Officers (CISO) to implement the information security management framework and to set up and operate the ISMS. The executive management of the respective division actively promotes the information security process and provides appropriate resources for the implementation of the information security policy.

REHAU expects all employees to be conscious of information security at all times in all of their daily activities and promotes this through written regulations and corresponding training measures. It is the responsibility of all managers to ensure that their employees comply with information security regulations and they must monitor this appropriately. Failure to comply with regulations may result in action being taken under labor law in accordance with local regulations.