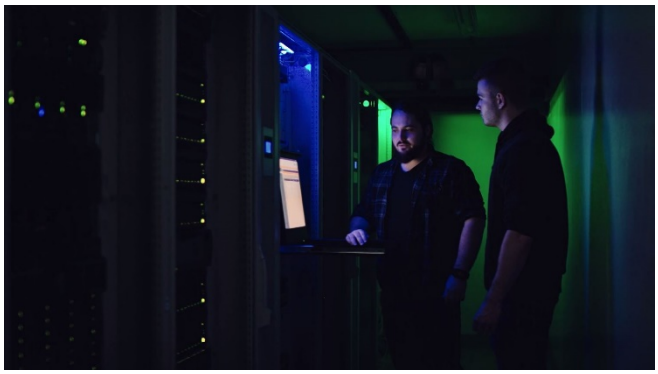
Rosenberger

Information Security Guideline

Rosenberger Hochfrequenztechnik GmbH & Co. KG – a medium-sized, family-owned industrial company founded in 1958 – is today one of the world's leading manufacturers of standardized and customer-specific connection solutions in high-frequency, high-voltage and fiber optics technology.

The product portfolio includes RF coaxial connectors, components and accessories, RF measurement technology products and assembled cables. Well-known high-tech companies in mobile and telecommunications, industrial measurement technology, automotive electronics, data technology, medical and industrial electronics or aerospace rely on the precision and quality of our products. In the industries division, Rosenberger designs innovative system solutions for M2M applications, e.g. for telematics projects. In the area of precision manufacturing, the company produces customer-specific components for drive systems and the commercial vehicle and mechanical engineering industries.

1. Scope and document management



The information technology systems of Rosenberger Hochfrequenztechnik GmbH & Co. KG, their security and availability play a key role at the company. Both the management of Rosenberger Hochfrequenztechnik GmbH & Co. KG and all employees must make sure to maintain the business processes that depend on information technology systems.

This information security guideline focuses on this requirement with regard to the security of information processing within Rosenberger Hochfrequenztechnik GmbH & Co. KG at the Fridolfing location.

The information security strategy of Rosenberger Hochfrequenztechnik GmbH & Co. KG is the framework according to which the information security guidelines of Rosenberger Hochfrequenztechnik GmbH & Co. KG are created. The information security strategy relates to information of all forms and has the particular objective of protecting the following information properties.

- Confidentiality
- Availability
- Integrity

With this information security strategy, the management and the Rosenberger Management Board underline the relevance and critical importance of information security and data protection within the company.

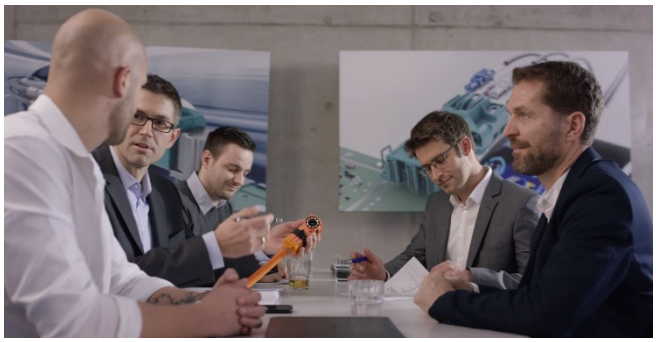
2. Requirements, risks and objectives

The trust of our customers and ultimately our business success are based on the fact that we, in particular

- comply with legal requirements and, in particular, data protection laws (compliance)
- protect our trade secrets
- maintain the confidentiality of our customers' data
- meet the relevant legal, regulatory and contractual requirements
- implement projects and services within planned and confirmed time periods

Meanwhile, the following principles are followed:

- Our approach to our approach to information security is business-oriented, risk-oriented and is in line with best practices
- All forms of information resources, whether digital or not, must be sufficiently protected over their entire life cycle
- All employees are responsible for internalizing the information security strategy and the relevant documents, guidelines and work instructions, and for acting in accordance with the guidelines contained therein
- The processing of personal data takes place in compliance with the legal principles for data protection
- The continuous improvement of information security and the associated protective measures and controls is an ongoing process and is the goal of the organization



Against this background the business success of our company depends on us recognizing existing risks for the stated objectives, avoiding or mitigating them with suitable measures, and treating any remaining risks appropriately. The risks include incomplete or incorrect compliance with legal requirements, the disclosure of trade secrets to unauthorized parties or unintentional disclosure thereof, the violation of our customers' requirements due to system failure, data loss and unauthorized disclosure of information.

3. The importance of security

Based on the external and internal requirements, but above all, in line with the security requirements of our customers, information security must be an integral part of our corporate culture. Every employee must be aware of the need for information security and be familiar with the fundamental impact of risks on business success.

4. Fundamental regulations

The management has set up an Information Security Department to implement the security objectives. The task of this department is to create uniform specifications for the security process, ensure sufficient sensitising all employees, and appropriately check or arrange for the checking of compliance with all security guidelines.

Information security at Rosenberger Hochfrequenztechnik GmbH & Co KG is based on TISAX (Trusted Information Security Assessment Exchange) which is related to essential aspects of the international standard ISO/IEC 27001.

These include the implementation of regular internal and external audits, appropriate document control, management evaluation and the application of the Continuous Improvement Model (PDCA).

Every employee is obliged to observe and comply with the general safety guidelines as well as those applicable to the respective workplace.

Violations of the information security guidelines may result in labour, civil or criminal liability.

5. Contact information

If you have any questions or comments regarding this document, please contact the Information Security Manager at Rosenberger Hochfrequenztechnik GmbH & Co. KG:

InformationSecurity@rosenberger.com

If personal data are affected, the company data protection officer must also be contacted:

Datenschutz@rosenberger.com