

# Managementhandbuch

## Chapter 1.7 Information security policy

---

We see it as the basis of our business activities to protect our company and business secrets. The protection of information provided by customers and partners is just as important to us in this regard as is the protection of our own know-how.

This policy applies to the entire company. The scope of the management system covers research and development, safety assessment and project sponsorship in the fields of industrial plant and nuclear safety, waste management, disposal, decommissioning and environmental protection.

The objective of this information security policy and the guidelines derived therefrom is to protect information from internal and external threats, to ensure the continuation of business operations, and to minimise possible damage caused by security incidents as far as possible. Information can exist in many different forms. It can include electronically stored or transmitted data as well as information on paper.

We consider the maintenance of confidentiality, integrity and availability of our company data and IT systems as well as of the information provided to us by our business partners to be the most important security objectives of GRS.

The basis for the choice of technical and organizational measures is compliance with legal, regulatory and contractual obligations as well as with the requirements of ISO/IEC 27001:2013. In addition, the standards of the German Federal Office for Information Security (BSI) serve as orientation. GRS endeavours to continually improve the suitability, adequacy and effectiveness of its measures for information security.

The IT security officer and the compliance officer draw up the guidelines in the area of information security in cooperation with the organisational units concerned, submit them to the management for approval, ensure communication with the groups of persons concerned, and monitor their implementation. The IT security officer and the compliance officer are directly subordinated to the company management and report to them.

The heads of division and heads of department are responsible within their organisational units for the introduction, compliance with and monitoring of the information security policy and the guidelines derived therefrom. Each employee is responsible for complying with the regulations of the information security policy and the guidelines derived therefrom that affect them.

### General Management of Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

Cologne / Garching, 20 January 2020

Hans J. Steinhauer  
Managing Director

Uwe Stoll  
Managing Director