

Information Security Policy

Information and the media supporting it shall remain available, accurate, and confidential for all authorized personnel. Information shall be created, processed, and managed in accordance with the security levels defined by TÜNKERS to ensure protection against loss, unauthorized modification, or unauthorized disclosure. These security levels are based on the controls defined in ISO/IEC 27002, the objectives established in ISO/IEC 27001:2022, and applicable TISAX information security best practices.

Within the TÜNKERS Information Security Management System (ISMS), the following principles constitute the main information security objectives:

- **Confidentiality:** Ensuring that information is accessible only to authorized individuals, systems, and processes.
- **Integrity:** Preserving the accuracy and completeness of information and processing methods.
- **Availability:** Ensuring that authorized users have access to information, systems, and supported processes when required.

To achieve these objectives, management commits to:

- Develop and maintain controls and control objectives to identify, assess, and manage risks related to information assets.
- Comply with all applicable business, legal, regulatory, and contractual information security requirements.
- Provide the necessary resources and assign responsibilities to implement, operate, and continuously improve the Information Security Management System.

All employees and third parties using TÜNKERS resources are required to acknowledge and support the achievement of these objectives. They are responsible for preserving the confidentiality, integrity, and availability of information assets in compliance with this policy and the organization's information security objectives.

Ratingen (Germany), January the 31st, 2026

CEOs