IT security policy (status 04 | 2025)

The main influence on the security policy based on ISO 27001 (International Organization for Standardization) and the BSI standard (German Federal Office for Information Security) is the careful consideration of, and adaptation to, the specific requirements of Klüh's stakeholders. The IT security policy is therefore regularly compared with the requirements of Klüh's opportunity and risk matrix. In addition, regular reviews and updates are carried out as part of the PDCA cycle (Plan-Do-Check-Act) to ensure that the security policy remains effective. To this end, the entire IT is now audited annually by the central QM department and not, as previously, on a random basis.

The pillars of Klüh's IT security policy are as follows:

1. Introduction

IT security serves to protect all IT assets such as computer systems, networks, digital devices and data of institutions or companies from unauthorized access, data breaches, cyber attacks and other malicious activities. Information is protected as a valuable and important part of Klüh's corporate assets.

The IT security policy is a requirement of ISO 27001. All requirements, such as the protection of data and documents, must be ensured at a basic level. In the area of critical infrastructure, this level is raised so that affected components, interfaces and processes are aligned with the highest level of protection. Particularly high requirements are placed on the clear and unambiguous description of the transitions and boundaries between the requirement levels.

2. Scope of application

The security policy applies to the IT infrastructure of all German companies and affects all associated areas, systems and processes. Coordination with the international units is ongoing.

3. Security objectives

Integrity, confidentiality, availability and authenticity are the foundations of our IT security policy. These objectives serve to protect all stakeholders. They are based on the principles of ISO 27001 and the BSI standard with the restrictions set out above.

4. Risk management

Process risks are systematically identified and documented in the opportunity and risk matrix provided by quality management (identification, assessment and treatment of risks). The matrix is regularly reviewed as part of the definition of processes for the application of a risk-based approach in accordance with ISO standards.

5. Organization of information security

The Information Security Officer (ISO) heads a committee that assesses risks and opportunities and analyzes and evaluates attacks. The ISO ensures that the committee is available 24/7 for the Klüh organization and stakeholders (authorities, customers).

The composition of the committee is approved by the holding company management. In addition to the reports to the holding company management, minutes are distributed to the compliance and data protection officers. The data protection officers in turn share their information with the ISO.

6. Asset management

The ISO and its committee ensure the identification and classification of information and IT resources. At the same time, they define measures for the appropriate safeguarding of assets.

7. Access control

Together with the data protection officers, the ISO and its committee determine the access authorizations and controls for systems and data in accordance with the specifications of the holding company management.

8. Encryption and data security

The ISO and its committee are responsible for defining encryption standards and procedures and for ensuring the integrity and confidentiality of data.

9. Incident management

The ISO and its committee are responsible for clarifying procedures for reporting and processing security incidents. The same applies to the integration of incident response plans in accordance with the ISO 27001 and BSI standards in the various fields of application.

10. Communication and training

If necessary, training programs for employees in the area of information security are set in consultation with the participants of the data protection meeting. The same applies to the establishment of communication mechanisms for security-relevant information.

11. Monitoring and evaluation

Since the introduction of the ISO 9001 system, Klüh has driven forward the implementation of control mechanisms for monitoring information security. These instruments are adopted by the ISO and its committee, regularly evaluated and brought up to date with the latest security policy.
The ISO is supported in this by the Head of Quality Management and the Data Protection Officer.

12. Documentation and records

The requirements for the documentation of safety measures are defined as part of the management system. The Head of Quality Management ensures the availability of records for audits and inspections.