IT security policy (status 04 | 2024)

The main driver of 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 security policy is therefore checked against the requirements of Klüh's opportunity and risk matrix on a regular basis. In addition, periodic reviews and updates are carried out as part of the PDCA (Plan-Do-Check-Act) cycle to ensure that the security policy remains effective. From now on, the entire IT will be audited annually by the central QM department and not, as previously, on a random basis.

The cornerstones 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 deemed as a valuable and important part of Klüh's corporate assets.
Die IT-Sicherheitspolitik ist eine Anforderung aus der ISO 27001. Alle Anforderungen, wie der Schutz von Daten und Dokumenten, sind grundsätzlich auf einem Basisniveau sicherzustellen. Im Umfeld von kritischer Infrastruktur wird dieses Niveau angehoben, damit betroffene Komponenten, Schnittstellen und Prozesse auf das höchste Schutzniveau ausgerichtet sind. Besonders hohe Ansprüche werden dabei an die klare und eindeutige Beschreibung der Übergänge und Abgrenzungen zwischen den Anspruchsniveaus gestellt.

2. Area of application:
The security policy applies to the IT infrastructure of all German companies and affects all associated areas systems and processes. There is ongoing coordination with the international units.

3. Security objectives:
The foundations of our IT security policy are integrity, confidentiality, availability and authenticity. They serve to protect all stakeholders. The principles of ISO 27001 and the BSI standard apply 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 establishment of new processes in line with ISO standards in order to apply a risk-based approach.

5. Organization of information security:
The Information Security Officer (ISO) heads a committee that assesses risks and opportunities and analyzes and evaluates attacks. The ISB 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 Management Board, minutes are distributed to the Compliance Officer and the Data Protection Officer. The data protection officers in turn share their information with the ISB.

6. Asset-Management:
The ISB and its committee ensure the identification and classification of information and IT resources. At the same time, they define measures for appropriate safeguarding of assets.

7. Access control:
The ISB and its committee, together with the data protection officers, determine the access authorizations and control for systems and data in accordance with the specifications of the holding company management.

8. Encryption and data security:
The ISB and its committee are responsible for defining encryption standards and procedures and for ensuring the integrity and confidentiality of data.

9. Incident-Management:
The ISB 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:
Training programs for employees in the area of information security are defined, if necessary, 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:
Klüh has driven forward the implementation of control mechanisms for monitoring information security since the introduction of the ISO 9001 system. 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 process by the Head of QM and the Data Protection Officer.

12. Documentation and records:
The requirements for the documentation of safety measures are established as part of the management system. The Head of QM ensures the availability of records for audits and inspections.