Information Security

Certified Information Security and Data Protection at KISTERS

Data Center | Products | Software as a Service | Software Development

Given the increasing influence of IT on business and administrative processes, secure information processing has become a key to corporate success. Therefore, KISTERS provides secure products to our customers and partners, realises safe operation of SaaS solutions in the certified KISTERScloud and protects the data of customers and partners to the highest possible degree.

Objectives and Levels of information security at KISTERS

To that end, we are advancing information security in various areas with high priority:

- By an **information security management system ISMS** certified according to ISO 27001 that formalizes all measures applied today
- In the **products**: First and foremost in the SCADA solutions which, as key elements of „critical infrastructures“, are subject to special requirements on information security. And abobe that in the SaaS solution for smart meter gateway administration that complies to TR-03139-6 of the German Federal Office for Information Security
- In the **data center**, that is certified for SaaS services, ASP services and data services even for mission-critical solutions
- In **support**
- In **software development** in general
- And, of course, in the continuous raising of awareness and training of our **employees** to information security issues

Certifications

Through organizational and technical measures, as well as the constant monitoring of infrastructure, processes, products and employees from the perspective of information security, we are on a very **high level of security**. We proof this with several certifications:

TÜVRheinland ZERTIFIZIERT
Management System
ISO/IEC 27001:2013
www.tuv.com
ID 9108638538

TÜVIT
TÜV NORD GROUP
TSI.STANDARD
Infrastructure
2022
tuvit.de
ID: 66812.22

- **ISO 27001 for information security management systems** for
  - the complete business unit „KISTERScloud Services“ (all aspects of KISTERScloud Services, from the technical infrastructure, through the operational processes to the employees)
  - the support of the business units Energy, Water, Monitoring, EHS
  - the software development of the business units Energy and Water
- **BSI TR-03109-6** for the SaaS solution for smart meter gateway administration. This allows an official use of the system for measuring point operators.
- **TÜV TSI** certification for the KISTERS Data Center in our headquarter in Aachen (Germany)

KISTERS

Information Security is our top priority.

Measures

In the implementation and certification of information security, we are putting our special focus on

— Data center KISTERS AG
— KISTERScloud-Services
— Customer Support
— Software development process
— Products / customer solutions

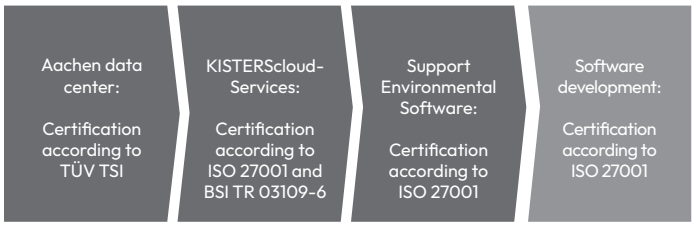
Security of the KISTERS data center

In our state-of-the-art certified data center in Aachen, we operate both our own IT and the SaaS solutions for our customers. Maximum security is required here. To ensure that your data is securely stored and accessible, we implement a comprehensive security concept consisting of, among other things:

— Physical security in the KISTERS data center
  - Through integration in buildings and security infrastructure
  - High-availability concept for complete server and access architecture
  - Safeguarding the power supply via UPS and ESPS
  - Air conditioning and fire prevention
  - Access protection with room and building surveillance
— Secure, high-performance access via the Internet
  - Broadband Internet connection secured by backup line
  - Access to SaaS solutions using TLS and VPN
— Modern storage and high availability concept
  - Redundant drive connection for the application server
  - Server clustering and database clustering
  - Server connection to high-availability SSD drive systems
  - 24/7 monitoring systems

In this way, we ensure that your data is safe in our data center, and it meets all of the requirements of data protection:

— **Availability**: guaranteed access to the data within an agreed timeframe; prevention of system failures
— **Integrity**: traceability of all changes to the data, no unnoticed changes
— **Authenticity**: verifiability of the authenticity and credibility of a person, a service, or data
— **Liability** / accountability: recognition of the author of changes; non-repudiation



— **Confidentiality**: reading and modification of the data only by authorized users (both for access to stored data as well as during data transfer)
— **Non-repudiation** (authenticity / traceability): proof that a message has been sent and received

Security of KISTERS software

In the development of our software solutions we are guided by the Secure Software Development Lifecycle (S-SDLC) and relevant "best practices" (BSI, NIST, OWASP, etc.). This means that we consider the security of a product from the conception to the delivery and maintenance. This is confirmed by corresponding extensions of the ISO 27001 certification.

According to these security standards, we write secure code, avoid typical vulnerabilities during coding, perform code reviews with a security focus, and also test our software under stress conditions. In this way, we ensure that **you are provided with reliable software solutions**.

Officer for information security and data protection

To coordinate the **implementation, continuous improvement and documentation** of all of the measures described above, we have created a staff position "Head of Information Security". The Chief Information Security Officer (CISO) and Data Protection Officer (DPO), works closely with the teams responsible for the KISTERS infrastructure and product development – with the ambition to offer you, our customers and partners, the highest security possible.

KISTERS AG
Pascalstr. 8+10
52076 Aachen
Germany

Phone +49 2408 9385 0
Fax +49 2408 9385 555

info@kisters.eu
www.kisters.eu

KISTERS