Information Security

Certified Information Security and Data Protection at KISTERS

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

Successful digitalisation of business and administrative processes is virtually impossible without information security and data protection. We at KISTERS therefore put great emphasis on the development of secure products, offer the secure operation of SaaS solutions (Software as a Service) with certified KISTERScloud services and ensure the protection of the data of customers and partners.

Objectives and areas of information security at KISTERS

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

- By an **information security management system (ISMS)** which is certified according to ISO 27001 and continuously enhanced in line with the standard
- In the **products**, above all in the SCADA solutions, which as core elements of 'critical infrastructures' are subject to special information security requirements, as well as in the SaaS solutions from the cloud, which is also certified according to SOC 2 Type 2 and BSI C5 Type 2.

- In the **data center**, which is certified for SaaS services as a 'Trusted Site Infrastructure', also for business-critical solutions
- In **support**
- In **secure software development processes**
- And, of course, in the continuous raising of awareness and training of our **staff** to information security issues and data protection

Certifications and attestations

Through organizational and technical measures, as well as the permanent monitoring of infrastructure, processes, products and staff from the perspective of information security, we are continuously improving our high level of security. We confirm this with several external certifications and attestations:

- **ISO 27001 for the information security management** for
  - the entire business unit KISTERScloud Services (all aspects of KISTERScloud Services, from the technical infrastructure, through the operational processes to our staff).
  - Software development and support for the business units Energy, HydroMet (formerly Water and Monitoring), EHS and IT Viewer
- **SOC 2 Type 2** and **BSI C5 Type 2** for our KISTERScloud Services
- **BSI TR-03109-6** for the SaaS solution and Business Process Outsourcing for smart meter gateway administration and passive/active market participants. This allows an official use of the system for metering 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

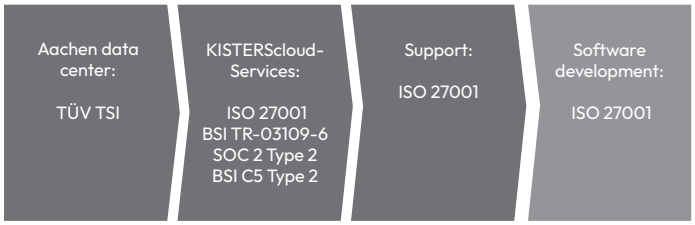
Security of the KISTERS data center

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 securing buildings and technical 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 and DDoS protection
  - Access to SaaS solutions using TLS and VPN
- Modern storage and high availability concept
  - Redundant storage connection for the application servers
  - Server clustering and database clustering
  - Connection of servers to high-availability SSD drive systems
  - 24/7 system monitoring

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

- **Confidentiality**: reading and modification of the data only by authorized users (both for access to stored data as well as during data transfer)
- **Integrity**: traceability of all changes to the data, no unnoticed changes
- **Availability**: guaranteed access to the data within an agreed timeframe; prevention of system failures
- **Authenticity**: verifiability of the authenticity and credibility of a person, a service, or data



Security of KISTERS software

When developing our software solutions, we work according to our 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.

We avoid typical vulnerabilities during coding, perform code reviews with a security focus, and also test our software under stress conditions including penetration tests. In this way, we ensure that **you are provided with reliable software solutions**.

CISO team for information security and data protection

Our Chief Information Security Officer (CISO) and his team are responsible for the coordination of the implementation, continuous improvement and documentation of all measures for information security, business continuity management and data protection. Our CISO team works closely with the staff responsible for the KISTERS infrastructure and product development - with the aim of offering you, our customers and partners, the highest possible level of security.

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
Empowering decisions of tomorrow