



# Zertifizierte Informationssicherheit und Datenschutz bei KISTERS

Rechenzentrum | Produkte | Software as a Service | Software-Entwicklung



Eine erfolgreiche Digitalisierung von Geschäfts- und Verwaltungsprozessen ist ohne Informationssicherheit und Datenschutz nicht möglich. Wir bei KISTERS legen daher großen Wert auf die Entwicklung sicherer Produkte, bieten Ihnen den sicheren Betrieb von SaaS-Lösungen (Software as a Service) mit den zertifizierten KISTERScloud-Services und sorgen für den Schutz der Daten von Kunden und Partnern.

## Ziele und Ebenen der IT-Security bei KISTERS

Deshalb bringen wir bei KISTERS die Informationssicherheit mit hoher Priorität weiter voran, und zwar auf verschiedenen Ebenen:

- Durch ein **Informationssicherheits-Managementsystem (ISMS)**, das nach ISO 27001 zertifiziert ist, und das im Sinne der Norm kontinuierlich weiterentwickelt wird
- In den **Produkten**, allem voran in den SCADA-Lösungen, die als Kernelemente von „Kritischen Infrastrukturen“ besonderen Anforderungen an die Informationssicherheit unterliegen, sowie in den SaaS-Lösungen aus der KISTERScloud, die auch nach SOC2 Typ 2 und BSI C5 Typ 2 testiert ist



- Im **Rechenzentrum**, das für SaaS-Services als „Trustet Site Infrastructure“ auch für unternehmenskritische Lösungen zertifiziert ist
- Im **Support**
- In sicheren **Softwareentwicklungsprozessen**
- und natürlich in der Sensibilisierung und Schulung unserer **Mitarbeiter:innen** hinsichtlich Informationssicherheit und Datenschutz

## Zertifizierungen und Testate

Durch organisatorische und technische Maßnahmen sowie die ständige Überprüfung von Infrastruktur, Prozessen, Produkten und Mitarbeiter:innen aus der Sicht der Informationssicherheit verbessern wir fortlaufend unser hohes Sicherheitsniveau. Dies belegen wir mit mehreren Zertifizierungen und Testaten:



- **ISO 27001 für das Informationssicherheits-Management** für
  - den gesamten Geschäftsbereich KISTERScloud Services (alle Aspekte der KISTERScloud Services, von der technischen Infrastruktur über die Betriebsprozesse bis hin zum Personal)
  - die Softwareentwicklung und den Support der Geschäftsbereiche Energie, HydroMet (ehem. Wasser und Monitoring), EHS, IT-Viewer
- **SOC 2 Typ 2 und BSI C5 Typ 2** für den gesamten Geschäftsbereich KISTERScloud Services
- **BSI TR-03109-6** für die Software-as-a-Service-Lösung und Business Process Outsourcing für die Smart Meter Gateway Administration und passive/aktive Marktteilnehmer. Dies ermöglicht eine offizielle Nutzung des Systems für Messstellenbetreiber.
- **TÜV TSI-Zertifizierung** für das KISTERS Data Center in Aachen

# Informationssicherheit hat bei uns höchste Priorität.

## Maßnahmen

Bei der Implementierung und Zertifizierung der Informationssicherheit legen wir besonderes Augenmerk auf die Schwerpunkte

- Rechenzentrum der KISTERS AG
- KISTERScloud-Services
- Kunden-Support
- Software-Entwicklungsprozess
- Produkte/Kundenlösungen

## Sicherheit des KISTERS Data Centers

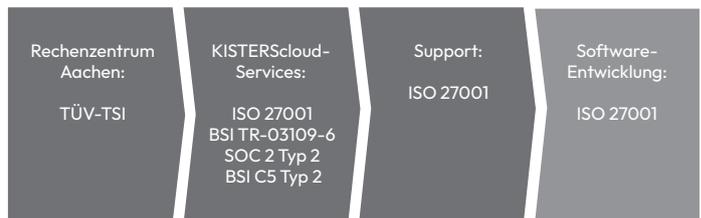
In unserem hochmodernen zertifizierten Rechenzentrum in Aachen betreiben wir sowohl unsere eigene IT als auch die SaaS-Lösungen für unsere Kunden. Höchste Sicherheit ist hier gefordert. Damit Ihre Daten bei uns sicher gespeichert und zugreifbar sind, investieren wir fortlaufend in ein umfangreiches Sicherheitskonzept.

Es besteht u.a. aus:

- Physikalische Sicherheit im KISTERS Rechenzentrum
  - Moderne Gebäudetechnik und Sicherheitsinfrastruktur
  - Hochverfügbarkeitskonzept für komplette Server- und Zugriffsarchitektur
  - Absicherung der Stromversorgung über USV und NEA
  - Klimatisierung und Brandschutz
  - Zutrittsschutz mit Raum- und Gebäudeüberwachung
- Sicherer und performanter Zugriff über das Internet
  - Breitbandige Internetanbindung abgesichert über Backup-Leitung und DDoS-Schutz
  - Zugriff auf die SaaS-Lösungen über TLS und VPN
- Modernes Storage- und Hochverfügbarkeitskonzept
  - Mehrpfadige Plattenanbindung der Applikations-Server
  - Server- und Datenbank-Clustering
  - Anbindung der Server an hochverfügbare SSD-Plattensysteme
  - 24/7-Monitoring der Systeme

So erreichen wir, dass Ihre Daten in unserem Rechenzentrum sicher sind, weil es allen Anforderungen des Datenschutzes entspricht:

- **Vertraulichkeit:** Lesen und modifizieren der Daten nur durch autorisierte Benutzer (sowohl beim Zugriff auf gespeicherte Daten wie auch während der Datenübertragung)
- **Integrität:** Nachvollziehbarkeit aller Änderungen an den Daten, keine unbemerkten Veränderungen
- **Verfügbarkeit:** gewährleiteter Zugriff auf die Daten innerhalb eines vereinbarten Zeitraums; Verhinderung von Systemausfällen
- **Authentizität:** Überprüfbarkeit der Echtheit und Glaubwürdigkeit einer Person, eines Dienstes oder von Daten



## Sicherheit von KISTERS Software

Bei der Entwicklung unserer Softwarelösungen arbeiten wir nach unserem Secure Software Development Lifecycle (S-SDLC) und nach maßgeblichen „Best Practices“ (BSI, NIST, OWASP usw.). Das bedeutet, dass wir die Sicherheit eines Produktes von der Konzeption bis zur Auslieferung und Wartung berücksichtigen. Wir vermeiden typische Sicherheitslücken bei der Codierung, führen Code Reviews mit Security-Fokus durch und testen unsere Software auch unter Stressbedingungen, u.a. auch durch Penetrationstests. So sorgen wir dafür, dass Sie sichere Software-Lösungen erhalten.

## CISO-Team für Informationssicherheit und Datenschutz

Die Koordination der Umsetzung, kontinuierlichen Verbesserung und Dokumentation der Maßnahmen zur Informationssicherheit, zum Business Continuity Management und zum Datenschutz obliegt der Stabsstelle des Chief Information Security Officers (CISO) und seinem Team. Unser CISO-Team arbeitet eng mit den Verantwortlichen für die KISTERS Infrastruktur und Produktentwicklung zusammen – mit dem Ziel, Ihnen als Kunden und Partnern höchstmögliche Sicherheit zu bieten.