INFOSHEET ➜ INFORMATION SECURITY

SECURITY
INFORMATION SECURITY CONCEPT

Today's threat landscape is becoming increasingly complex and diverse. Now more than ever, you need a good combination of technology and processes to achieve your business goals.

The protection of customer data at SPIE ICS AG is not a theory but is based on best practice IT security management. All security processes of SPIE ICS AG are documented and available on our process management portal. This is in accordance with the standards ISO 9001, ISO/IEC 20000-1 and ISO/IEC 27001 in which we are duly certified.

This ensures end-to-end security throughout the life cycle of all data relating to:

CONFIDENTIALITY
Only persons with the appropriate authorizations have access to the data.

INTEGRITY
Ensuring the accuracy and completeness of the information and its processing methods.

AVAILABILITY
Ensure that authorized users have access to information and associated assets when needed.

RISK MANAGEMENT
The Compliance Board of SPIE ICS meets regularly to address risk management in an ongoing process.

Identified risks are addressed with the appropriate measures and control elements. Your customer data is thus always protected in a structured manner.

ABOUT SPIE ICS

Our values (performance, proximity and responsibility) and our extensive portfolio of solutions and established processes make us the ideal partner for small, medium-sized and large companies.

We are one of the few providers in Switzerland that can offer you first-class global and local geographical coverage.

Our services are based on industry best practices, current certifications and modern process-oriented methodology.

IPMA Hermes PRINCE2 ITIL

Zertifiziertes Managementsystem SQS ISO/IEC 20000-1

Zertifiziertes Managementsystem SQS ISO/IEC 27001

Zertifiziertes Managementsystem SQS ISO 9001

PROCEDURAL CONTROLS

Only authorized users have access to information and related assets and this is managed with the following:

- **Policies** and security guidelines ensure that all SPIE employees follow the rules for handling data with high sensitivity.
- **Workflows** ensure efficient processing, and that data is stored, transmitted, shared according to the wishes of our customers.

- **Non-disclosure agreements** oblige our employees to protect our customer data.
- **Change Management** ensures that the confidentiality, integrity and availability of our customer data and information systems are maintained.
- **List of authorized users** clearly identify the authorized employees who work for a specific customer.
- **Background checks** of employees are carried out as part of the internal HR process. When required by the customer, additional safety checks are applied.
- **Education** and security awareness campaigns are specifically tailored to the needs of our business.

TECHNICAL CONTROLS

SPIE ICS Infrastructure

A modern and secure infrastructure guarantees a high security standard:

- Locations are connected by encrypted links
- Firewall, proxy, zoning and other technical measures

- 2-factor authentication is used if necessary
- Backup, escalation and disaster recovery procedures are available.

Least Privilege

Role Based Access Control ensures that only authorized users can access and modify data.

Cryptography

- Cryptography at rest – all SPIE ICS laptops have encrypted hard drives.
- Cryptography in transit – Interfaces for data exchange between us and our customer are provided via encrypted protocols such as TLS. According to our Information Security Policy, E-mails are also encrypted if they are confidential to customers.

VIRTUAL SECURITY TEAM

In addition to the afore mentioned, SPIE ICS AG has a "Virtual Security Team" in which security know-how is exchanged on an interdisciplinary basis. This diverse set of professional skills, promotes security and serves to protect our customers' valuable information resources.

CONTACT US

SPIE ICS AG
Freiburgstrasse 251
CH-3018 Berne

Phone +41 58 301 11 11
info.ch@spie.com
www.spie.ch