

FOERSTER CYBERSECURITY POSTURE STATEMENT

Version 4.0

Purpose

This document provides an overview of the cybersecurity measures implemented by Institut Dr. Foerster GmbH & Co. KG (Institut Dr. FOERSTER GmbH & Co. KG is hereinafter referred to as "FOERSTER" throughout this document) to protect its corporate information systems, customer data, intellectual property, and business operations — including FOERSTER AI CLOUD, the Group's platform for the secure transmission and AI-based analysis of machine data from measuring and testing equipment installed at customer sites.

Although FOERSTER is currently not certified according to ISO/IEC 27001, cybersecurity is an integral part of our corporate governance and operational processes. Our security program follows industry best practices and is continuously improved to address evolving cyber threats.

Scope: this statement covers both FOERSTER corporate IT environment and the FOERSTER AI CLOUD platform and addresses the requirements most frequently raised by customers under ISO/IEC 27001, the EU General Data Protection Regulation (GDPR / DSGVO) and the EU Artificial Intelligence Act. It is intended as a standard reference to answer common customer and supplier security questions and does not disclose confidential security architecture, credentials, or other sensitive technical detail.

1 Security Governance

Cybersecurity is supported by executive management and is integrated into the company's business processes.

- The organization has established:
- Defined cybersecurity roles and responsibilities, including a named Information Security Management Officer and an Information Security coordinator.
- Documented IT security policies and procedures
- Management commitment to cybersecurity
- Continuous evaluation and improvement of security controls
- Structured incident response and escalation processes

Cybersecurity is considered an ongoing management responsibility rather than a one-time compliance activity.

2 Organizational Security

FOERSTER has implemented organizational measures to ensure that cybersecurity is embedded throughout the company.

These measures include:

- Mandatory cybersecurity awareness training for all employees
- Mandatory GDPR (DSGVO) and data protection training
- Regular refresher training
- Role-based responsibilities for information security
- Principle of least privilege for system access
- Controlled onboarding and offboarding processes
- Defined user access review procedures

Security awareness is regarded as a key component in preventing cyber incidents.

3 ISO/IEC 27001 Alignment

FOERSTER is not currently certified according to ISO/IEC 27001. Our current strategy is to align our information security management with the principles of the standard, rather than to pursue formal certification in the near term; this is kept under review as FOERSTER.CLOUD and our security program mature.

Already in place:

- An inventory of information assets and a policy for classifying information
- Documented IT security policies and procedures, with defined cybersecurity roles and responsibilities
- Technical controls consistent with ISO/IEC 27001 Annex A, including access control, cryptography, operations security and supplier security (see Technical Security Controls below)
- Not yet formalized — and part of our roadmap toward a standards-aligned ISMS (Information Security Management System):
- A documented, asset-based information security risk assessment and treatment process
- A defined internal ISMS audit program
- Regular management review of the ISMS
- A tested Business Continuity / Disaster Recovery plan
- A Statement of Applicability covering the Annex A control set
- We report this status transparently rather than implying a level of formality we have not yet reached; see Continuous Improvement for the associated roadmap.

4 Technical Security Controls

FOERSTER operates a modern IT infrastructure protected by multiple layers of security controls.

Key technical measures include:

4.1 Identity & Access Management

- Multi-Factor Authentication (MFA)
- Role-Base Access Control
- Centralized identity management
- Strong password policies
- Conditional Access

4.2 Endpoint Protection

- Microsoft 365 E5 Security
- Microsoft Defender security technologies (EDR)
- Enterprise endpoint protection
- Malware protection
- Continuous device monitoring

4.3 Vulnerability & Patch Management

- State-of-the-art patch management process
- Continuous deployment of security updates
- Rapid assessment of newly disclosed vulnerabilities
- Risk-based prioritization of critical patches

4.4 Network & Perimeter Security

- Next Generation Firewalls and intrusion detection systems as technical safeguards
- Physical access controls and monitoring of server rooms and data centers

4.5 Backup and Recovery

- Regular backup procedures
- Backup verification and recovery testing
- Offsite backup storage
- Encryption of data in transit (e.g. TLS 1.2/1.3)
- Encryption of data at rest, currently applied to backup systems and mobile endpoints
- Secure remote access
- Protection of company endpoints

4.6 Security Monitoring

FOERSTER continuously monitors the cybersecurity landscape and evaluates potential impacts on its infrastructure.

This includes:

- Continuous monitoring of relevant cybersecurity intelligence feeds
- Evaluation of newly published vulnerabilities (CVEs)
- Assessment of vendor security advisories
- Continuous review of Microsoft's security recommendations
- Ongoing monitoring of the internal security posture
- Build-out of a dedicated Threat Detection & Response capability, monitored on an ongoing basis
- This enables rapid identification and mitigation of emerging threats.

4.7 Incident Response

FOERSTER maintains defined procedures to observe, document and counter security incidents.

In addition, the company maintains a contractual partnership with SySS GmbH, one of Germany's leading cybersecurity specialists, to provide professional support in the event of significant cybersecurity incidents, including planned periodic penetration testing (SySS is certified by the German Federal Office for Information Security (BSI) as a service provider for IT security penetration testing.)

This partnership strengthens our capability to respond quickly and effectively to sophisticated cyber threats.

5 Data Protection & Privacy

Data protection at FOERSTER is governed by the EU General Data Protection Regulation (GDPR / DSGVO) and the German Federal Data Protection Act (BDSG). Personal data is processed primarily based on contract performance (Art. 6(1)(b) GDPR).

- A Data Protection Officer is appointed and can be reached via datenschutz.de@foerstergroup.com
- A record of processing activities is maintained in accordance with Art. 30 GDPR
- Documented Technical and Organizational Measures (TOMs) are maintained, and a standard Data Processing Agreement (DPA / AVV) is provided to every customer
- A dedicated data protection management policy governs responsibilities and accountabilities within the organization
- A documented process is in place to handle data subject requests (access, rectification, erasure, and similar rights)
- Employees handling personal data are bound to confidentiality and receive regular data protection training
- Sub-processors are selected from an approved supplier list and are contractually bound to equivalent confidentiality and data protection obligations

- Processes are in place to identify, document and report data protection incidents to affected customers without undue delay, in line with Art. 33/34 GDPR
- A documented deletion concept defines retention periods and deletion routines, including for archives and backups

A Data Protection Impact Assessment (DPIA, Art. 35 GDPR) has been completed for our use of Microsoft Copilot. A dedicated DPIA covering FOERSTER.CLOUD's AI-based analysis of customer machine data is planned as part of the platform's continued rollout (see Continuous Improvement).

For the FOERSTER.CLOUD hosting region planned in the United States, an appropriate international data-transfer mechanism (e.g. EU Standard Contractual Clauses) is not yet in place and will be established ahead of that region's launch; as described under FOERSTER.CLOUD, a given customer's data is only ever stored in the region assigned to that customer.

6 FOERSTER AI CLOUD — Secure Machine Data & AI Platform

FOERSTER AI CLOUD is the Group's platform for connecting measuring and testing machines installed at customer sites to a FOERSTER-managed cloud environment, where machine and process data is analysed using artificial intelligence to generate insights such as predictive maintenance indications and quality trend analysis.

6.1 Data Minimization by Design

- Machine data is captured and pre-processed at the customer's site
- Only the data required for the agreed analysis is transmitted to FOERSTER AI CLOUD
- Customers always retain ownership of their data
- Data belonging to different customers is logically separated and never mixed

6.2 Hosting & Data Residency

FOERSTER AI CLOUD is currently hosted in Germany (Frankfurt am Main), with database backups also stored within Germany. The underlying data centre

infrastructure is operated by an EU-based provider under EU/German jurisdiction and is therefore not subject to the US CLOUD Act.

As FOERSTER AI CLOUD grows, additional hosting regions are planned: a dedicated region in the United States to serve customers in America, followed by a region in Asia to serve customers in that market. Each region will host only the data of the customers assigned to it — data does not move between regions — and overall platform administration and governance will continue to be performed under FOERSTER's EU-based corporate control, regardless of the hosting region.

6.3 Technical Security Architecture

- Encrypted transport (TLS) between machines, users and the platform
- Encryption of stored data
- Strict, logical separation between customer accounts (multi-tenant isolation), with no shared data across customers
- Outbound-only connections from machines and edge devices at the customer site — no inbound access into the customer's network is required, and no VPN needs to be installed
- Modern authentication (single sign-on / OIDC), with optional federation to the customer's own identity provider
- Role-based, least-privilege access for administration
- A controlled, auditable software delivery process for platform updates

6.4 Certifications of the Underlying Infrastructure

The data centres underlying FOERSTER.CLOUD are certified to:

- ISO/IEC 27001 based on IT-Grundschutz (BSI), specifically covering the compute, storage and container services used by the platform
- ISO/IEC 27001 at group level
- BSI C5 (Cloud Computing Compliance Criteria Catalogue)
- ISO 50001 (energy management)

- FOERSTER AI CLOUD as a platform is on a roadmap toward alignment with these same standards, and an external penetration test of the platform is planned together with SySS GmbH.

6.5 Data Portability & Deletion

Customer data can be exported in open, standard formats — proprietary formats without an open export path are not used. Upon termination of the contractual relationship, customer data is deleted from the platform within the retention period agreed in the applicable Data Processing Agreement.

6.6 Regulatory Alignment

The platform's compliance approach considers, among others: GDPR, the EU Data Act (data portability and the ability to switch providers), the Cyber Resilience Act (for connected edge components), and the NIS2 Directive.

7 EU AI Act & Responsible AI

The artificial intelligence used in FOERSTER AI CLOUD to analyse machine and process data — for example to generate predictive maintenance indications and quality trend insights — has been assessed under the EU Artificial Intelligence Act and classified as a limited-risk AI system. It is not a safety component of a product, and it is not used to make decisions about people (such as employment or access decisions), so it does not fall under the Act's high-risk categories.

- Our own, purpose-trained models are used for this analysis — we do not rely on a third-party general-purpose AI model for FOERSTER AI CLOUD machine-data analysis
- Customers and users are informed when they are working with AI-generated results, in line with the Act's transparency requirements (Art. 50)
- AI-generated outputs, such as maintenance recommendations, are reviewed by qualified personnel before they inform any action — human oversight is built into the process
- An internal AI usage / Responsible AI policy governs how AI is developed and used within FOERSTER

- Technical documentation covering the purpose, functioning and limitations of the AI system is maintained
- Measures are in place to safeguard the quality of input and training data and to mitigate bias

8 What We Do / What We Don't Do

To make our security posture easy to assess, we summarize below what customers can rely on FOERSTER to do — and where we deliberately draw the line.

8.1 What We Do

- Follow documented, management-supported cybersecurity governance and policies
- Maintain an inventory of information assets and an information classification policy
- Enforce multi-factor authentication, least-privilege access and centralized identity management across our corporate IT
- Patch and update systems continuously, prioritized by risk
- Encrypt data in transit, and are extending encryption at rest across all systems
- Keep regular, tested backups stored in a secure, separate location
- Continuously monitor for threats and vulnerabilities, and are building out a dedicated Threat Detection & Response capability
- Investigate, document and remediate every security incident
- Work with SySS GmbH, an established German cybersecurity specialist, for incident response support and penetration testing
- Maintain a record of processing activities, a documented data-subject-rights process, and provide a standard Data Processing Agreement (AVV) and a named Data Protection Officer to every customer
- Classify the AI system behind FOERSTER AI CLOUD as limited risk under the EU AI Act, apply human oversight to its outputs, and document its purpose and limitations

- Keep FOERSTER AI CLOUD customer data logically separated per tenant, and minimize what leaves the customer's site
- Host FOERSTER AI CLOUD with an EU-based provider that is not subject to the US CLOUD Act, and keep platform governance under FOERSTER's EU entity even as the platform expands to new regions

8.2 What We Don't Do

- We are not currently ISO/IEC 27001 certified as a company, and our risk assessment, internal audit and business continuity processes are not yet formalized to that standard — see ISO/IEC 27001 Alignment for the current state and roadmap
- We have not yet completed a Data Protection Impact Assessment specifically for FOERSTER AI CLOUD (one has been completed for our use of Microsoft Copilot); this is planned ahead of broader rollout
- We do not yet have an international data-transfer mechanism (such as EU Standard Contractual Clauses) in place for the planned US FOERSTER AI CLOUD region — this will be established before that region serves customers
- We do not use a third-party general-purpose AI model for FOERSTER AI CLOUD machine-data analysis; we use our own, purpose-trained models
- We do not require inbound VPN or remote-access connections into customer networks for FOERSTER AI CLOUD — all machine connections are outbound-only
- We do not mix or share data between different customers' tenants
- We do not use customer data for purposes beyond the agreed service without a separate agreement
- We do not permit self-registration or uncontrolled account creation on our platforms
- We do not grant FOERSTER staff physical access to third-party data centres; physical security is handled by certified data centre providers
- We do not store a given customer's data outside the hosting region assigned to that customer

9 Continuous Improvement

Cybersecurity is continuously reviewed and enhanced.

Current strategic initiatives include:

- Further alignment with the requirements of the EU NIS2 Directive
- Continuous enhancement of cybersecurity governance
- Building a documented ISMS risk assessment and treatment process, an internal audit program, regular management review, a tested Business Continuity / Disaster Recovery plan, and a Statement of Applicability, as steps toward a possible future ISO/IEC 27001 certification decision
- Expansion of threat detection capabilities, including advanced Network Detection and Response (NDR) technologies
- Broader rollout of encryption at rest across all storage systems
- External penetration testing of corporate IT and FOERSTER AI CLOUD together with SySS GmbH
- A dedicated Data Protection Impact Assessment for FOERSTER AI CLOUD, and formalization of a Privacy-by-Design/-Default policy building on the existing safe-room principle
- Putting an appropriate international data-transfer mechanism in place ahead of the planned US FOERSTER AI CLOUD hosting region
- Geographic expansion of FOERSTER AI CLOUD to the United States and, subsequently, Asia, with equivalent security and data-residency controls in each region
- Ongoing investment in security awareness and technical protection

10 Compliance

FOERSTER has implemented documented cybersecurity and data protection policies covering:

- Information Security
- Asset Management & Information Classification
- Access Control
- Password Management
- Patch Management
- Backup and Recovery
- Remote Access
- Malware Protection
- Security Awareness
- Incident Management
- Data Protection Management
- AI Usage / Responsible AI
- Security controls are regularly reviewed and continuously improved.

11 Commitment

FOERSTER is committed to maintaining a high level of cybersecurity through organizational, technical, and procedural controls, across both its corporate IT environment and FOERSTER AI CLOUD.

Our objective is to ensure the confidentiality, integrity, and availability of our information systems and the data entrusted to us, while continuously improving our cybersecurity posture in accordance with recognized industry best practices.

Institut Dr. Foerster GmbH & Co. KG

In Laisen 70, 72766 Reutlingen, Germany

This document is intended to provide customers with a high-level overview of FOERSTER's cybersecurity posture, including FOERSTER AI CLOUD. It does not disclose confidential security architecture, operational procedures, or sensitive technical information.

This document was drafted with the support of artificial intelligence (AI). Its content has been independently reviewed, verified for accuracy, and approved by two authorized representatives of FOERSTER prior to its release.