curiosity

Curiosity Security & Compliance Overview

Version 1.0

1. Overview

Curiosity GmbH provides enterprise AI software for industrial knowledge management and data analysis. Security, data protection, and operational resilience are core to our product design and delivery model. This document summarizes our governance framework, security controls, and compliance approach. Detailed policies are available upon request to prospective customers and partners.

2. Company Information

Curiosity GmbH
Munich, Germany
Managing Directors: Leon Zucchini, Rafael Fernandes de Oliveira

3. Governance & Accountability

Information security and data protection are overseen by the Managing Directors.
Operational security controls are implemented and maintained by the CTO.
Security policies are reviewed annually or upon material business or infrastructure change.

4. Risk Management

Curiosity maintains a documented risk register covering:

- Cybersecurity risks
- Operational risks
- Compliance risks
- Financial and reputational risks

Risks are assessed based on likelihood and impact. High-risk items require mitigation plans and executive oversight.

5. Security Architecture

5.1. Deployment Models

Curiosity supports:

- Customer-hosted deployments (on-prem or private cloud)
- Curiosity-managed cloud deployments

Infrastructure responsibilities are clearly defined contractually depending on deployment model.

5.2. Access Control

- Role-based access control
- Least privilege principle
- Multi-factor authentication for production and administrative systems
- Formal joiner / mover / leaver process

curiosity

5.3. Encryption

- Data encrypted in transit using modern TLS
- Data encrypted at rest in production systems
- Encrypted backups

5.4. Infrastructure Security

- Secure cloud configuration
- Network-level protection mechanisms
- Restricted administrative access
- Logging of security-relevant events

5.5. Secure Development

- Version-controlled codebase
- Mandatory peer review for production changes
- Separation of development and production environments
- Controlled deployment processes

5.6. Vulnerability Management

- Regular application of security updates
- Prioritization of high-severity vulnerabilities
- Monitoring of third-party dependencies

6. Incident Response

Curiosity maintains a documented Incident Response Policy.
Security incidents are:

- Reported immediately
- Assessed for impact
- Contained and remediated
- Documented and reviewed

Where required, affected customers are notified in accordance with contractual and legal obligations.

7. Business Continuity & Disaster Recovery

Curiosity maintains documented backup and recovery procedures.
For primary production systems:

- Recovery Time Objective (RTO): Target within 24 hours
- Recovery Point Objective (RPO): Target within 24 hours

Backup restoration procedures are periodically tested.
Customer-hosted deployments follow recovery responsibilities defined in contract.

curiosity

8. Data Protection & GDPR

Curiosity processes personal data in compliance with GDPR and applicable German law.

8.1. Role Clarity

- Curiosity acts as data controller for internal business data.
- Curiosity acts as data processor when processing customer data within its software.

Processing activities as processor are governed by a Data Processing Agreement (DPA).

8.2. Subprocessors

- Used only where necessary
- Bound by contractual data protection obligations
- Disclosed in accordance with the DPA

9. Data Subject Rights

Curiosity supports applicable data subject rights in accordance with legal obligations and contractual roles.

10. Ethics & Compliance

Curiosity maintains policies covering:

- Anti-bribery and anti-corruption
- Conflict of interest
- Export control and sanctions compliance
- Confidential reporting of misconduct

11. Further Information

Detailed security policies, subprocessors, and contractual documentation are available to prospective customers and partners upon request via our Trust Center.