Otto Krahn Holding, Mühlenhagen 35, 20539 Hamburg

Information Security Statement of the Otto Krahn Group

1. Introduction

Our corporate group is committed to protecting information and IT systems through an established Information Security Management System (ISMS) based on the principles of ISO 27001. Additionally, we comply with requirements of IATF 16949, ISO 9001, and the current NIS2 directive to ensure the highest security standards, especially in production environments.

1. Scope

This policy applies to all employees, customers, suppliers, and third parties who have access to the IT systems or data of Otto Krahn Group and all its affiliated companies, including but not limited to OK Holding, ALBIS, MOCOM, KRAHN Chemie, Krahn Ceramics. It covers any interaction with our digital infrastructure, applications, and information assets, regardless of location or device.

1. Organization and responsibility for information security

We have established an information security organization, which includes Cybersecurity. A designated responsible person (e.g., IT Security Manager) coordinates all security measures and serves as a contact point.

Contact for Information Security and Cybersecurity Matters:
IT Security Manager of the Otto Krahn Group
***E-Mail**: infosec@ottokrahn.group*

2. .Security Measures

- Technical protections include firewalls, up-to-date antivirus software, data encryption, multi-factor authentication (MFA) for all critical systems, and least privilege access controls.
- We follow IATF 16949-specific cybersecurity requirements, including multidisciplinary risk assessments for production processes, emergency plans for cyber incidents affecting manufacturing infrastructure, and regular audits to verify effectiveness.
- Regular employee training and awareness programs are conducted to maintain a strong information security culture.

3. Incident Management

A clearly defined process exists for reporting and handling security incidents. Cybersecurity incidents must be reported immediately to the organizational unit responsible for swift and coordinated response.

4. Data protection

Personal data is protected according to applicable legal standards such as the GDPR. Further details are available in our privacy policy on the website.

5. ISMS-Implementaton

Our ISMS is developed and operated in accordance with ISO/IEC 27001 principles and is continuously maintained and improved. While we do not hold formal certification, our practices align with recognized international standards and industry best practices.

Furthermore, we incorporate obligations arising from the national implementation of the EU NIS-2 Directive, such as risk-based cybersecurity measures, supply chain security, incident reporting within statutory timelines, and governance responsibilities at management level. This integrated approach ensures compliance with legal requirements and standards, strengthening resilience across all entities of the Otto Krahn Group.

Review and Improvement

This cybersecurity policy as well as this Information security statement and related measures are regularly reviewed and updated to adapt to emerging threats and legal requirements.

This information security statement has been reviewed and formally approved by the Management of Otto Krahn Group Holding. The approval applies to all affiliated companies within the Otto Krahn Group.