Otto Krahn Holding

Otto Krahn Holding, Mühlenhagen 35, 20539 Hamburg

Information Security Statement der Otto Krahn Group

1. Einleitung

Unsere Unternehmensgruppe verpflichtet sich zum Schutz von Informationen und IT-Systemen durch ein etabliertes Informationssicherheitsmanagementsystem (ISMS), das auf den Prinzipien von ISO 27001 basiert. Darüber hinaus erfüllen wir die Anforderungen von IATF 16949, ISO 9001 und der aktuellen NIS2-Richtlinie, um die höchsten Sicherheitsstandards zu gewährleisten, insbesondere in Produktionsumgebungen.

2. Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeiter, Kunden, Lieferanten und Dritte, die Zugang zu den ITSystemen oder Daten der Otto Krahn Group und aller verbundenen Unternehmen haben, einschließlich, aber nicht beschränkt auf OK Holding, ALBIS, MOCOM, KRAHN Chemie, Krahn Ceramics. Sie umfasst jede Interaktion mit unserer digitalen Infrastruktur, Anwendungen und Informationsressourcen, unabhängig vom Standort oder Gerät.

3. Organisation und Verantwortung für Informationssicherheit

Wir haben eine Informationssicherheitsorganisation etabliert, zu der auch Cybersicherheit gehört. Eine benannte verantwortliche Person (i.d.F. IT Security Manager) koordiniert alle Sicherheitsmaßnahmen und fungiert als Ansprechpartner.

Kontakt für Informationssicherheit und Cybersicherheit:
IT Security Manager der Otto Krahn Group
***E-Mail**: infosec@ottokrahn.group*

4. . Sicherheitsmaßnahmen

- Technische Schutzmaßnahmen umfassen Firewalls, aktuelle Antivirensoftware, Datenverschlüsselung, Multi-Faktor-Authentifizierung (MFA) für alle kritischen Systeme und Zugriffskontrollen nach dem Prinzip der geringsten Privilegien.

- Wir folgen den IATF 16949-spezifischen Cybersicherheitsanforderungen, einschließlich multidisziplinärer Risikobewertungen für Produktionsprozesse, Notfallplänen für Cybervorfälle, die die Fertigungsinfrastruktur mit einbeziehen, und regelmäßigen Audits zur Überprüfung der Wirksamkeit.

- Regelmäßige Mitarbeiterschulungen und Sensibilisierungsprogramme werden durchgeführt, um eine starke Sicherheitskultur aufrechtzuerhalten.

5. Incident Management

Es existiert ein klar definierter Prozess zur Meldung und Behandlung von Sicherheitsvorfällen. Cybersicherheitsvorfälle müssen sofort der zuständigen Organisationseinheit gemeldet werden, um eine schnelle und koordinierte Reaktion zu gewährleisten.

6. Datenschutz

Personenbezogene Daten werden gemäß geltenden gesetzlichen Standards wie der DSGVO geschützt. Weitere Details finden Sie in unserer Datenschutzrichtlinie auf der Website.

7. ISMS-Implementierung

Unser ISMS wurde gemäß den ISO/IEC 27001-Prinzipien entwickelt und betrieben und kontinuierlich gepflegt und verbessert. Obwohl wir keine formale Zertifizierung besitzen, entsprechen unsere Praktiken anerkannten internationalen Standards und bewährten Branchenpraktiken.

Darüber hinaus integrieren wir Verpflichtungen, die sich aus der nationalen Umsetzung der EU-NIS2-Richtlinie ergeben, wie risikobasierte Cybersicherheitsmaßnahmen, Lieferkettensicherheit, Vorfallberichterstattung innerhalb gesetzlicher Fristen und Governance-Verantwortlichkeiten auf Managementebene. Dieser integrierte Ansatz gewährleistet die Einhaltung gesetzlicher Anforderungen und Standards und stärkt die Widerstandsfähigkeit in allen Einheiten der Otto Krahn Group.

8. Überprüfung und Verbesserung

Unsere Cybersicherheitsrichtlinie sowie das Information Security Statement und die damit verbundenen Maßnahmen werden regelmäßig überprüft und aktualisiert, um sich an neue Bedrohungen und rechtliche Anforderungen anzupassen.

Dieses Information Security Statement wurde vom Management der Otto Krahn Group Holding überprüft und formell genehmigt. Die Genehmigung gilt für alle verbundenen Unternehmen innerhalb der Otto Krahn Group.