Krones AG
Böhmerwaldstraße 5
93073 Neutraubling

# Cyber Security Anforderungen für Lieferanten des Krones Konzerns

## 1 Zielsetzung und Zielgruppe

Cyber Security ist ein äußerst wichtiges Thema für den Krones Konzern. Zur Sicherstellung eines hohen Sicherheitsniveaus erfüllt Krones die Anforderungen des internationalen Standards ISO/IEC 27001 und hat ein Cyber Security Management System (CSMS) etabliert. Insbesondere die Cyber Security der Krones Produkte und Dienstleistungen gewinnt dabei zunehmend an Bedeutung. Geeignete technische und organisatorische Maßnahmen (z.B. basierend auf der IEC 62443 Norm) müssen umgesetzt werden, um aktuelle und zukünftige regulatorische Anforderungen sowie Kundenanforderungen zu erfüllen.

Da Cyber Security eine Teamleistung ist, können die Krones Ziele hier nur erreicht werden, wenn alle Geschäftspartner das Thema ebenso ernst nehmen und eng mit dem Krones Konzern zusammenarbeiten. Um den Krones Konzern aktiv bei der Einhaltung der regulatorischen Anforderungen sowie der Erfüllung der Kundenanforderungen zu unterstützen, müssen alle Geschäftspartner die folgenden allgemeinen Sicherheitsanforderungen erfüllen.

## 2 Allgemeine Sicherheitsanforderungen

- Um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und informationsverarbeitenden Systemen zu gewährleisten, müssen entsprechende technische und organisatorische Maßnahmen umgesetzt sein. Die Maßnahmen sollten Best Practices aus der Industrie folgen und ein angemessenes Information Security Management System (ISMS) basierend auf internationalen Standards und Normen (wie z.B. ISO/IEC 27001 oder IEC 62443) umfassen (falls anwendbar). Bestehende Maßnahmen werden bei Bedarf an zukünftige technische und organisatorische Entwicklungen angepasst.
- Personenbezogene Daten werden mit Sorgfalt und unter Einhaltung der relevanten Datenschutzgesetze (z.B. EU-DSGVO) verarbeitet.
- Lieferanten stellen sicher, dass deren Mitarbeitende regelmäßig ein angemessenes (abhängig vom jeweiligen Einsatzgebiet) Security Awareness Training absolvieren.
- Lieferanten informieren den Krones Konzern unverzüglich über bereits eingetretene oder mögliche Sicherheitsvorfälle sowie erkannte Sicherheitsschwachstellen oder Risiken, die den Krones Konzern betreffen oder betreffen könnten.
- Lieferanten haben die notwendigen Vereinbarungen mit deren Unterauftragnehmern geschlossen, um den Anforderungen dieses Dokuments zu entsprechen und ein angemessenes Sicherheitsniveau in der gesamten Lieferkette zu gewährleisten. Sind entsprechende Vereinbarungen nicht vorhanden, werden diese innerhalb eines angemessenen Zeitraums geschlossen.
- Bei berechtigtem Interesse und auf Anfrage des Krones Konzerns, stellen Lieferanten schriftliche Nachweise für die Einhaltung der Sicherheitsanforderungen aus diesem Kapitel sowie gegebenenfalls für weitere vertragliche verbindliche Sicherheitsanforderungen (siehe Kapitel *3 Spezifische Sicherheitsanforderungen)* innerhalb eines angemessenen Zeitraums zur Verfügung.
- Benötigt ein Lieferant Fernzugriff, sollten die Standardlösungen des Krones Konzerns hierfür verwendet werden. Erforderliche Abweichungen hiervon sind einvernehmlich abzustimmen und bedürfen einer Genehmigung durch den Krones Konzern.
- Cyber Security Policies und Richtlinien werden aktiv durch die Lieferanten angefordert, soweit diese deren Tätigkeitsbereich betreffen können und diskutieren aktiv Cyber Security Themen mit den Ansprechpartnern des Krones Konzerns.


Contact: cyber.security@krones.com

## 3 Spezifische Sicherheitsanforderungen

Für ausgewählte Lieferantengruppen können zusätzliche Cyber Security Anforderungen bestehen. Diese spezifischen Sicherheitsanforderungen werden im Rahmen der Prozesse zur Lieferantenauswahl und zum Vertragsabschluss kommuniziert und vereinbart.

Einige Lieferantengruppen, für die spezifische Sicherheitsanforderungen gelten können, werden nachfolgend aufgeführt:

- Lieferanten von Produkten oder Komponenten mit digitalen Elementen: Um die zukünftigen gesetzlichen und regulatorischen Anforderungen (z.B. EU Cyber Resilience Act) sowie Kundenanforderungen zu erfüllen, wird eine enge Zusammenarbeit bezüglich Produktsicherheit erwartet. Hierzu gehört die Bereitstellung der notwendigen Informationen zur Erstellung einer „Software Bill of Materials“ (SBOM). Zusätzlich soll über Schwachstellen im Produkt informiert werden, um den Krones Konzern bei der Behebung der Schwachstelle zu unterstützen.
- Maschinenlieferanten: Sicherheitseigenschaften sowie zusätzlichen Services (z.B. Fernzugriff), die eine Maschine aufweisen bzw. anbieten muss, werden im Rahmen des Vertragsabschlusses vereinbart.
- Verarbeitung personenbezogener Daten im Auftrag: Vor der Verarbeitung von personenbezogenen Daten durch externe Dienstleister, muss eine Vereinbarung zur Auftragsverarbeitung (AV-Vereinbarung) geschlossen werden.
- Cloud-Dienstleister: Die Cloud-Prinzipen des Krones Konzerns werden im Rahmen des Vertragsabschlusses kommuniziert und vereinbart.
- Lieferanten mit Zugriff auf Daten, Systeme oder Netzwerke des Krones Konzerns erhalten Anweisungen, um sicherzustellen, dass Mindestanforderungen für technische und organisatorische Sicherheitsmaßnahmen eingehalten werden.
- OEM-Lieferanten erhalten im Rahmen des Vertragsabschlusses eine spezielle OEM Spezifikation.

Version: 1.1, März 2023



Contact: cyber.security@krones.com