Cyber Security Anforderungen für Geschäftspartner der ROFA GROUP

1. Zielsetzung und Zielgruppe

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

Da Cyber Security eine Teamleistung ist, können die ROFA Ziele hier nur erreicht werden, wenn alle Geschäftspartner das Thema ebenso ernst nehmen und eng mit der ROFA GROUP zusammenarbeiten. Um die ROFA GROUP 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 (ISO/IEC 27001, IEC 62443) umfassen. 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.
- Geschäftspartner stellen sicher, dass deren Mitarbeitende regelmäßig ein angemessenes Security Awareness Training absolvieren.
- Geschäftspartner informieren die ROFA GROUP unverzüglich über bereits eingetretene oder mögliche Sicherheitsvorfälle sowie erkannte Sicherheitsschwachstellen oder Risiken, die die ROFA GROUP betreffen oder betreffen könnten.
- Geschäftspartner 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 der ROFA GROUP, stellen Geschäftspartner schriftliche Nachweise für die Einhaltung der Sicherheitsanforderungen aus diesem Kapitel sowie gegebenenfalls für weitere vertragliche verbindliche Sicherheitsanforderungen innerhalb eines angemessenen Zeitraums zur Verfügung.
- Benötigt ein Geschäftspartner Fernzugriff, sollten die Standardlösungen der ROFA GROUP hierfür verwendet werden. Erforderliche Abweichungen hiervon sind einvernehmlich abzustimmen und bedürfen einer Genehmigung.

- Cyber Security Policies und Richtlinien werden aktiv durch die Geschäftspartner angefordert, soweit diese deren Tätigkeitsbereich betreffen können und diskutieren aktiv Cyber Security Themen mit den Ansprechpartnern der ROFA GROUP.

3. Spezifische Sicherheitsanforderungen

Für ausgewählte Lieferantengruppen können zusätzliche Cyber Security Anforderungen bestehen. Diese spezifischen Sicherheitsanforderungen werden im Rahmen der Prozesse zur Geschäftspartnerauswahl 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 die ROFA GROUP 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 der ROFA GROUP werden im Rahmen des Vertragsabschlusses kommuniziert und vereinbart.
- **Geschäftspartner mit Zugriff auf Daten, Systeme oder Netzwerke der ROFA GROUP** erhalten Anweisungen, um sicherzustellen, dass Mindestanforderungen für technische und organisatorische Sicherheitsmaßnahmen eingehalten werden.
- **OEM-Lieferanten** erhalten im Rahmen des Vertragsabschlusses eine spezielle OEM Spezifikation.