Krones AG
Böhmerwaldstraße 5
93073 Neutraubling

Cyber Security Requirements for suppliers of the Krones Group

1 Objectives, target audience and scope

Cyber security is a significant topic for the Krones Group. To ensure a high level of cyber security, Krones adheres to the requirements set by the ISO/IEC 27001 standard and has implemented a Cyber Security Management System (CSMS). In particular, the cyber security of products and services supplied by the Krones Group becomes more and more important. Appropriate technical and organizational measures (e.g., based on IEC 62443) must be implemented to meet the current and future regulatory requirements as well as the requirements of Krones' customers.
As cyber security is a team effort, Krones' goals can only be achieved if all business partners of Krones take cyber security as seriously as the Krones Group and collaborate closely.
To actively support the Krones Group complying with regulatory requirements and meeting the requirements of Krones' customers, all business partners need to meet the following general security requirements.

2 General security requirements

- Technical and organizational measures shall be in place to ensure confidentiality, integrity and availability of data and IT systems. The implemented measures should follow industry best practices and shall include an appropriate Information Security Management System (ISMS) in accordance with standards such as ISO/IEC 27001 or IEC 62443 (if applicable). If necessary, existing measures will be adjusted to the further technical and organizational developments.
- Personal data shall be processed with care and in compliance with relevant data protection laws (e.g., EU GDPR).
- The external party ensures that its employees receive an appropriate (depending on operation area) security awareness training on a regular basis.
- The external party shall inform the Krones Group immediately about all relevant cyber security incidents (actual and suspected) and identified security vulnerabilities or risks if the Krones Group is or is likely to be materially affected.
- The external party has agreements or will have agreements, within a reasonable time, with all subcontractors in place, that correspond to the requirements in this document, ensuring an appropriate level of cyber security in their supply chain.
- In case of justified interest and on request by the Krones Group, the external party shall provide written evidence for compliance with the security requirements in this section and further contractual binding security requirements (if applicable, *see Section 3 Specific security requirements*) within a reasonable period of time.
- If remote access by an external party is necessary, the standard Krones Group solution should be used. Any necessary deviation shall be aligned and approved by the Krones Group.
- The external party will actively ask for specific cyber security policies or guidelines that might affect their scope of operation and actively discuss security topics with the Krones Group counterpart.

3 Specific security requirements

Additional cyber security requirements might exist for some supplier groups. These specific security requirements will be communicated and agreed as part of the supplier selection and contracting process.

Contact: cyber.security@krones.com

Some supplier groups where specific security requirements might be applicable, are listed below:

- Supplier of products or components with digital elements: Joint work on product security is expected to meet future legal and regulatory requirements (e.g., EU Cyber Resilience Act) as well as customer demands. This includes providing the necessary information and data to create software bill of materials (SBOM). In addition, information about vulnerabilities in the product should be provided to help the Krones Group in remediating the vulnerabilities.
- Supplier of machinery and equipment: Security features and machine related services (e.g., remote services) will be agreed as part of the contracting process.
- External parties processing personal data: Prior to processing personal data by external parties, a commissioned data processing agreement is concluded.
- Cloud service provider: Krones Cloud Principles will be communicated and agreed as part of the contracting process.
- External parties with access to Krones data, systems or networks will receive instructions to ensure minimum requirements for technical and organizational security measures.
- OEM suppliers will receive a dedicated OEM specification as part of the contracting process.

Version: 1.1, March 2023

Contact: cyber.security@krones.com