Lenze

Cyber Security for your machines:
Let's act together.

Checklist to implement **initial security measures**

Lenze

1 Familiarize yourself with **legal regulations** (e.g. CRA, MVO, RED) and train your employees with regard to relevant cyber security standards (e.g. IEC 62443).

2 Establish **processes for detecting and reporting security vulnerabilities. A PSIRT team** (Product Security Incident Response Team) and a **software bill of materials** (SBOM) of the machine help to identify and handle cyber security incidents in a structured manner and comply with legal reporting obligations.

3 **Systematically analyze potential risks and threats** to your machines and systems. This provides you with a realistic overview and enables you to targeted prioritization of protective measures.

4 Implement **technical protection measures** such as access controls, regular updates and secure interfaces. Ensure a high level of usability – cyber security functions should be intuitive and user-friendly to ensure acceptance and correct use.

5 Actively seek **dialog with your suppliers and customers** to jointly define requirements and understand security concerns. **Open communication** promotes trust and facilitates a joint response to cyber security incidents.

Learn more about our
cyber security solutions