Cyber security requirements for business partners of the ROFA GROUP

1. Objectives and goals

Cyber security is an extremely important issue for the ROFA GROUP. To ensure a high level of security, ROFA complies with the requirements of the international standard ISO/IEC 27001 and has established an information security management system (ISMS). The cyber security of ROFA products and services is becoming increasingly important. Appropriate technical and organisational measures based on IEC 62443 must be implemented in order to meet current and future regulatory requirements and customer requirements.

Since cyber security is a team effort, ROFA's goals can only be achieved if all business partners take the issue equally seriously and work closely with the ROFA GROUP. In order to actively support the ROFA GROUP in complying with regulatory requirements and meeting customer requirements, all business partners must meet the following general security requirements.

2. General security requirements

- Appropriate technical and organisational measures must be implemented to ensure the confidentiality, integrity and availability of information and information processing systems. The measures should follow industry best practices and include an appropriate Information Security Management System (ISMS) based on international standards and norms (ISO/IEC 27001, IEC 62443). Existing measures will be adapted to future technical and organisational developments as necessary.
- Personal data shall be processed with care and in compliance with the relevant data protection laws (e.g. EU GDPR).
- Business partners shall ensure that their employees regularly complete appropriate security awareness training.
- Business partners shall immediately inform the ROFA GROUP of any security incidents that have already occurred or are likely to occur, as well as any identified security vulnerabilities or risks that affect or could affect the ROFA GROUP.
- Business partners have concluded the necessary agreements with their subcontractors to comply with the requirements of this document and to ensure an appropriate level of security throughout the supply chain. If such agreements do not exist, they will be concluded within a reasonable period of time.
- In the event of a legitimate interest and at the request of the ROFA GROUP, business partners shall provide written evidence of compliance with the security requirements set out in this chapter and, where applicable, with other contractually binding security requirements within a reasonable period of time.
- If a business partner requires remote access, the ROFA GROUP's standard solutions should be used for this purpose. Any necessary deviations from this must be agreed upon by mutual consent and require approval.
- Business partners shall actively request cyber security policies and guidelines insofar as these may affect their area of activity and shall actively discuss cyber security issues with the ROFA GROUP's contact persons.

3. Specific security requirements

Additional cyber security requirements may apply to selected supplier groups. These specific security requirements are communicated and agreed upon as part of the business partner selection and contract conclusion processes.

Some supplier groups to which specific security requirements may apply are listed below:

- **Suppliers of products or components with digital elements:** In order to meet future legal and regulatory requirements (e.g. EU Cyber Resilience Act) and customer requirements, close cooperation on product security is expected. This includes providing the necessary information to create a "Software Bill of Materials" (SBOM). In addition, information about vulnerabilities in the product should be provided to support the ROFA GROUP in remedying the vulnerability.
- **Machine suppliers:** Security features and additional services (e.g. remote access) that a machine must have or offer are agreed upon when the contract is concluded.
- **Processing** of **personal data on behalf of others:** Before personal data is processed by external service providers, a data processing agreement (DPA) must be concluded.
- **Cloud service providers:** The ROFA GROUP's cloud principles are communicated and agreed upon when the contract is concluded.
- **Business partners with access to ROFA GROUP data, systems or networks** receive instructions to ensure that minimum requirements for technical and organisational security measures are met.
- **OEM suppliers** receive a special OEM specification as part of the contract conclusion.