Beckhoff Automation GmbH & Co. KG

Information Security Terms and Conditions for Suppliers (valid from April 2026)

BECKHOFF

1. General provisions

These Information Security Terms and Conditions ("Terms and Conditions") apply to all suppliers ("Supplier") that obtain access to non-public information in the course of their cooperation with Beckhoff Automation GmbH & Co. KG (referred to as the "Buyer"; both parties are referred to collectively as the "Parties"). They are based on the Buyer's Information Security Policy, which defines uniform security standards and is made available on request. Deviating provisions in contracts between the Parties shall take precedence over these Terms and Conditions.

2. Compliance with legal requirements and recognized standards

2.1. The Supplier shall comply with all applicable statutory provisions, in particular those relating to data protection law.

2.2. In the event of doubt, contractual confidentiality and non-disclosure obligations of the Supplier toward the Buyer shall take precedence over the requirements of the German Act on the Protection of Trade Secrets.

2.3. The Supplier shall align its technical and organizational measures with recognized information security standards and best practices, in particular ISO/IEC 27001 or an equivalent standard, without this giving rise to a certification obligation.

3. Use of subcontractors

3.1. If the Supplier intends to entrust subcontractors with work for which the subcontractor obtains access to information pertaining to the Buyer, this requires the prior consent of the Buyer, which may also be granted generally.

3.2. When engaging subcontractors, the Supplier shall ensure that the requirements of this document are duly taken into account and fulfilled through appropriate and equivalent measures.

4. Confidentiality

4.1. The Buyer and the Supplier are obliged to treat all commercial and technical details that are not in the public domain and that become known to them through the business relationship as business secrets.

4.2. Drawings, designs, samples, manufacturing instructions, internal company data, tools, pieces of equipment, and similar items that the Buyer has provided to the Supplier for the purpose of submitting an offer or carrying out a delivery remain the property of the Buyer. They may only be used for the purposes of the respective contract between the Supplier and the Buyer and not for any other purposes of the Supplier; in particular, they may not be provided or otherwise made available to third parties. The reproduction of such items is only permitted within the scope of operational requirements and copyright regulations.

4.3. The Parties may only advertise their business relationship with prior written consent.

5. Technical and organizational measures

5.1. The Supplier shall implement appropriate technical and organizational measures to protect the confidentiality, integrity, and availability of the information and personal data pertaining to the Buyer that it processes in the course of the cooperation.

5.2. These measures include, in particular, access control measures, physical access security, network security, data backup, and recovery and emergency concepts. Upon the Buyer's request, the Supplier shall provide the Buyer with more detailed information on the technical and organizational measures that are suitable for assessing the appropriateness of the technical and organizational measures taken by the Supplier.

5.3. The Supplier shall review the effectiveness of these measures at appropriate intervals and adapt them in the event of changes in the risk situation, technological progress, or new legal requirements.

6. Data processing

If and to the extent that the Supplier processes personal data on behalf of the Buyer, this will take place exclusively on the basis of an agreement regarding the processing of personal data in line with Art. 28 of the GDPR, which shall be concluded separately.

7. Training and awareness

The Supplier shall ensure that all employees who come into contact with information pertaining to the Buyer in the course of the cooperation are regularly trained in relevant aspects of information security and data protection, and are adequately informed about the applicable confidentiality and secrecy obligations toward the Buyer.

8. Security incidents and mandatory reporting requirement

8.1. The Supplier shall maintain a procedure for identifying and dealing with security incidents.

8.2. Security incidents that affect or may affect the confidentiality, integrity or availability of the Customer's information must be reported by the Supplier to the Customer without undue delay. The notification shall be made by email to dataprotection@beckhoff.com.

9. Evidence, inspections

9.1. Upon request, the Supplier shall provide the Buyer with appropriate evidence in writing (email is sufficient) of compliance with these Information Security Terms and Conditions (e.g., self-declarations, certificates, or relevant excerpts from audit reports).

9.2. The Supplier shall support the Buyer to a reasonable extent and by prior agreement in the event that information security inspections are to be conducted by the Buyer or third parties. Support is limited to the Supplier's area of performance. The Supplier's operational processes must be given due consideration.

10. Term

10.1. These Terms and Conditions apply for the duration of the business relationship between the Parties, upon which they are based.

10.2. These confidentiality provisions also apply beyond the end of the contract. Employees of the Supplier must be placed under a corresponding obligation beyond the duration of their employment relationship.