BASIC REQUIREMENTS FOR INFORMATION SECURITY

(as of October 29, 2025)

Contact details for Schnellecke Group Security:

INFORMATION-SECURITY@SCHNELLECKE.COM

The provisions of this appendix contain the basic requirements of Schnellecke Group AG & Co. KG (the client) regarding the information security of the contractor.
With regard to the contractual relationship, the client considers compliance with the requirements to be the basis for cooperation.

1. BASIC OBLIGATIONS OF THE CONTRACTOR

a. Confidentiality and data protection
The contractor is obligated to treat all information received within the scope of this contract in accordance with its classification (see 1.e.) and to use it exclusively for the contractually agreed purposes. He ensures that all applicable data protection laws, including the GDPR, are complied with.

b. Information security concept
The contractor has an appropriate information security concept, including a description of the technical and organizational implementation of the minimum requirements for information security described in 2.

c. Proof of certificates
The contractor shall provide the client with currently valid certificates (TISAX, ISO27001, SOC2).

d. Ongoing updating and review
The contractor shall carry out ongoing review and adjustment of the information security concept, particularly in the event of changes to legal or regulatory requirements, and shall inform the client thereof (see contact details above).

e. Protection requirements and classification of information
The contractor shall ensure an adequate protection of the client's information, taking into account the requirements of applicable standards, such as ISO27001, and the current state of the art. The protection objectives of confidentiality, availability, and integrity must be taken into account.

f. Deletion and return of information
Upon termination of the contractual relationship, the contractor undertakes to delete/destroy all information received from the client. The only exceptions to this are pieces of information that are subject to a legal or contractual retention obligation.

g. Contact person at the contractor
The contractor shall designate a responsible contact person for information security incidents and notify the client of any changes.

h. Audit right
The client is entitled to review the information security measures, controls, and processes within the contractor's area of responsibility after giving prior notice. The contractor shall facilitate and provide appropriate support for such reviews.

2. MINIMUM REQUIREMENTS FOR TECHNICAL AND ORGANIZATIONAL MEASURES FOR INFORMATION SECURITY

a. Guidelines and organization
The contractor has up-to-date and appropriate information security guidelines and has clearly named and defined responsibilities for information security. In addition, the protection requirements for the contractor's information are systematically determined and inventoried.

b. Review and compliance with guidelines
The information security guidelines are subject to regular and ad hoc reviews. Procedures for compliance with the guidelines are established.

c. Risk management
The contractor systematically assesses, identifies, and addresses information security risks.

d. Security incident management
The contractor has established appropriate procedures for dealing with security incidents, which enable an appropriate response to incidents. In the event of security incidents, the contact person at the client (see contact details above) must be informed immediately.

e. Business continuity
The contractor shall define and implement appropriate measures to limit the impact of threats (e.g., natural disasters, physical attacks, cyber attacks) on service provision. In addition, a business continuity management system with emergency plans and emergency tests shall be established if the subject matter of the contract is classified as critical in terms of availability.

f. Training and awareness
The contractor shall ensure that employees are adequately and regularly trained and sensitized on the topics of cyber and information security.

g. Protection of operating resources and information assets
The supplier shall carry out an inventory of all operating resources and information assets and implement measures to protect them. Regular security checks and maintenance must be carried out.

h. Physical security
The contractor shall have appropriate measures in place for the physical protection of information within its area of responsibility. This includes defined security zones, measures to protect against unauthorized access to the contractor's buildings/rooms, and rules of conduct for employees, in particular "clean desk" requirements.

i. Access and access control
The contractor shall take measures to protect against unauthorized access, unauthorized/accidental alteration or deletion, and unauthorized transmission. He shall implement procedures to ensure that access to sensitive information and and IT systems is only granted to authorized persons.

j. Cryptography
The supplier undertakes to protect all sensitive data during transmission and storage by using encryption technologies. The encryption algorithms and keys used must comply with current security standards.

k. Data backup
The supplier shall regularly create data backups and store them securely. Procedures for restoring data in the event of loss shall be implemented and tested regularly.

l. Vulnerability and patch management
The supplier shall regularly check for security vulnerabilities and remedy them promptly. A patch management process for updating software and systems must be implemented.

m. Logging and monitoring
The supplier shall set up logging and monitoring mechanisms to detect and respond to security incidents. The logs shall be checked regularly for suspicious activity.

n. Network security
The supplier shall set up logging and monitoring mechanisms to detect and respond to security incidents. The logs must be checked regularly for suspicious activity.

o. Subcontractors
The contractor shall review its subcontractors with regard to compliance with information security requirements. He shall conclude valid confidentiality agreements before disclosing sensitive information.