SCHOTT

Information Security Requirements for Suppliers

This document specifies information security requirements applicable to suppliers that provide goods or services to SCHOTT. These information security requirements are consistent with the International Organization for Standardization (ISO) 27001.

The key words "MUST", "MUST NOT", "REQUIRED", "SHOULD", “SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

- **Information Security Policy**: Suppliers must maintain a structured and actively managed approach to information security, including documented policies, defined processes, and continuous improvement. Suppliers should align their approach with recognized frameworks (e.g., ISO/IEC 27001, NIST Cybersecurity Framework).
- **Information Security Organization**: Suppliers must formally define and assign responsibility for information security to a qualified role (e.g., Information Security Officer).
- **Supplier Relationships**: Suppliers must ensure non-disclosure and confidentiality agreements with any contractors or other third parties that have access to suppliers’ network and maintain a documented third-party risk management program. Suppliers must ensure that subcontractors follow SCHOTT requirements.
- **Asset Management**: Suppliers must maintain an inventory of hardware, software, and virtual assets, along with documentation of baseline system and security configurations, including configuration changes for components.
- **Human Resources Security**: Suppliers must provide information security training to employees, conduct background checks where appropriate, and have disciplinary processes for policy violations. Employees must be contractually bound to confidentiality.
- **Physical and Environmental Security**: Suppliers must implement physical access controls, lock data centers and IT rooms, and ensure facilities are resilient to disasters.
- **Operations Security**: Suppliers must have standard operating procedures, a change management process, and anti-malware software installed on systems. Data and configuration backups must be performed and tested regularly based on business

requirements for data availability. Suppliers must implement a vulnerability management program that follows globally recognized standards.

- **Access Control**: Suppliers must control access to computer systems, require positive identification and authentication, and manage elevated privileges actively. Suppliers must limit access to their network to only those employees, contractors, and other users who have a business need for access.

- **Cryptography**: Suppliers must encrypt SCHOTT data in transfer and at rest. Suppliers must use non-proprietary and up-to-date encryption algorithms and ensure encryption keys are protected from unauthorized access.

- **Development and Support Processes**: Suppliers must have a System Development Lifecycle (SDLC) for the development and deployment of Systems and Applications, which incorporates activities and deliverables to ensure security requirements are met.

- **Information Security Incident Management**: Suppliers must have a formal security incident monitoring, reporting, and response capability to identify, report and appropriately respond to known or suspected security incidents. Suppliers must report relevant security incidents that might affect SCHOTT data or the delivery process to SCHOTT without undue delay.

- **Business Continuity Management (BCM)**: Suppliers must implement a Business Continuity and Disaster Recovery Plan to ensure continuity of delivering products and services to SCHOTT in the event of a major incident. The plan must be tested on a regular basis.

- **Compliance**: Suppliers must comply with legal and regulatory requirements and allow and support periodic self-assessments to ensure compliance. Suppliers must accept the SCHOTT network access terms including the liability clauses to get access to SCHOTT networks and systems.

Revision History

Version	Changes	Date
01	Initial Release	06-16-2026