Cyber security requirements for suppliers

1. Introduction

The Spheros Group wants to ensure that its suppliers maintain an appropriate level of security in their network and information systems in order to protect the availability, confidentiality and integrity of their related processes and information and to fulfill legal obligations.

Chapter 2 describes basic cyber security requirements that apply to all suppliers and delivery items. These requirements are expanded in Chapter 3 to include specific requirements for digital products, components and services.

If there is an increased risk, additional individual cyber security requirements can be defined and agreed that extend or specify the minimum requirements.

2. Requirements for all suppliers

1. general regulations

(a) The Supplier shall ensure that it, its employees, external employees and any subcontractors comply with all obligations under this document.

(b) If, in the Supplier's view, cooperation by Spheros is necessary for the Supplier to comply with the cyber security requirements, the Supplier shall notify Spheros of this in writing (e-mail shall suffice).

(c) Other contractual agreements between Spheros and the Supplier shall remain unchanged.

2. general requirements for cyber security at the supplier

(a) The supplier's cyber security risk management should be clearly defined and systematically implemented. A direct report to the management and a commitment to cyber security are necessary. Ideally, an information security management system (ISMS) in accordance with ISO 27001 or similar should be implemented.

(b) The Supplier shall implement appropriate, state-of-the-art technical and organizational risk mitigation measures in the following areas:

- Permissible use of information security values
- Remote access
- Access control / multifactor authentication
- Response to (product) cyber security incidents
- Vulnerability / patch management
- Encryption standards
- Data / system classification
- Protection against malware
- Connection from third-party providers
- E-mail / instant messaging
- Physical security
- Personnel security
- Network / perimeter security
- Data backup / backup copies
- IT Service Continuity Management / Business Continuity Management (ITSCM / BCM)
- Secure software development

(c) The Supplier must train its employees and external persons or subcontractors employed by it at least once a year on the (product) cyber security requirements and the applicable regulations.

3. Cyber security rules for working with Spheros

(a) The Supplier must inform Spheros (cybersecurity@spheros.com) immediately if a cyber security incident occurs that enables unauthorized access to Spheros information or manipulation of the product or could impair the Supplier's ability to deliver.

(b) In the event of cyber security incidents involving confidential Spheros information, the Supplier shall:

- Take immediate action to minimize the damage to Spheros
- Document all measures taken and provide the documentation to Spheros
- Carry out a root cause analysis, define and implement preventive measures and inform Spheros about the action plan and status until final implementation

(c) If the Supplier is requested by public authorities to disclose confidential Spheros information without consent, the Supplier shall inform Spheros immediately, if permitted by law.

(d) If the Supplier works with Spheros systems or operates on Spheros premises, it must comply with the applicable cyber security guidelines of Spheros

(g) Spheros may verify compliance with the Supplier's safety standards by means of safety audits. The Supplier must grant Spheros access to relevant documents or transmit them upon request. In addition, the Supplier must provide necessary information and grant Spheros access to its production and operating facilities during business hours, if necessary. Spheros shall announce the visit in advance, unless there are events that affect information security, in which case unannounced visits are possible. Spheros shall carry out the audit as sparingly as possible for the Supplier's operating procedures and shall safeguard the Supplier's data protection and business secrets. Spheros may also commission third parties with the audits, who are obliged to maintain confidentiality.

(h) The Supplier must provide Spheros with information on the handling of Spheros data and on general information security so that Spheros can assess the Supplier's status. This information is required for the first request and for new products or services. It can be provided via a Spheros questionnaire. In order to minimize information security risks, Spheros reserves the right to obtain and evaluate further information based on the evaluation of the information provided.

(i) Spheros may require the Supplier to draw up and implement a concept for remedying information security breaches if these are related to the provision of services. The Supplier must immediately take suitable measures and draw up a schedule that is appropriate to the nature and severity of the breach. If Spheros draws up its own concept, the Supplier must support Spheros in its implementation.

(j) The Supplier must inform Spheros of significant changes affecting information security, such as changes in technology or the withdrawal/expiry of certificates. If these changes significantly impair the security level, Spheros may withdraw from the contract extraordinarily.

3. requirements for suppliers of digital products, components or services

1. general requirements

In addition to Chapter 2, the following rules apply to suppliers of digital products, components or services. This includes software deliveries, digital services/cloud solutions, the operation of Spheros IT and communication systems, the delivery of hardware with digital elements (e.g. controllers, components with integrated control) and the contract development of software. Development services within the Spheros development processes and with Spheros systems are excluded and are subject to the internal specifications of Spheros.

(a) All relevant software and components of the supplier must be subjected to a risk analysis and, if necessary, developed according to the security-by-design approach. Development must be secure, including regular vulnerability testing and remediation.

(b) Technical documentation must be created and kept up to date for the software, listing all components and data flows included. User documentation must also be available that describes how the software can be used safely.
(c) Vulnerabilities in the software must be assessed for their exploitability and impact (ideally according to CVSS) and dealt with accordingly.

(d) When integrating third-party software (including open source) into its own software, the Supplier must ensure that all of the above requirements are met. The Supplier shall also be responsible for procuring the necessary licenses and ensuring license conformity, or for informing Spheros of any further licenses required.

(e) Changes to the software must follow a structured process. The cyber security requirements from this document continue to apply.

2. requirements for the delivery of products or components with digital elements

If the supplier delivers products or components with digital elements, the following additional requirements apply:

(a) Before the purchase agreement is concluded, the Supplier shall inform Spheros how long it will provide free updates, for example to rectify vulnerabilities (hereinafter referred to as the "assured period").

(b) The Supplier warrants that the product or component has no known exploitable vulnerabilities upon delivery.

(c) Vulnerabilities that become known within the guaranteed period must be reported to Spheros within a reasonable period of time according to the criticality of the vulnerability and practicable solutions (patches, configuration changes) must be provided. The solutions must be feasible with reasonable effort and must not impair existing data and functions. This also applies to components that are used in our products. The supplier must provide appropriate contact options for queries.

(d) The user documentation, including information on the intended use and the security provisions, must be provided to Spheros.

3. requirements for the operation of digital services

The following requirements apply to suppliers who operate digital services that Spheros, its customers, other suppliers or partners use. These include software-as-a-service offerings and fully managed service contracts for infrastructure components:

(a) The Supplier shall operate an information security management system in accordance with ISO 27001 or an equivalent standard covering the relevant part of its organization.

(b) Spheros information, the IT systems and data transmissions must be secured with modern protective measures. These include:

4. Observance of the least privilege and need-to-know principles when assigning authorizations
5. Enforce complexity rules for passwords according to current standards
6. Securing network access from the Internet through strong authentication (e.g. multi-factor authentication)
7. Use of the latest technology against malware at relevant points
8. Regular checks for vulnerabilities and prompt implementation of countermeasures and patches
9. Client separation of services and data (e.g. through suitable access control measures)

(c) Unless otherwise agreed, the Supplier shall define data backup and recovery processes and inform Spheros of the recovery point in time (RPO) and the recovery time objective (RTO).

(d) In principle, Spheros information may only be processed and stored in secure premises. The recovery and emergency processes must be tested at least once a year and proof must be provided to Spheros.

(e) The Supplier is obliged to centrally log security-relevant events and to regularly examine the logs for anomalies.

(f) The Supplier shall maintain a reporting system for customer-relevant information security risks that meets at least these requirements:

- Regular reporting cycle, at least once a year
- Overview of identified risks and measures
- Security audits carried out (e.g. penetration tests)
- Security awareness measures implemented