Product cyber security requirements for suppliers

1. Introduction

Spheros supplies electronic control units and other components with digital elements that become part of vehicles and vehicle systems placed on the market by its customers (“OEMs”). Several of these customers are, in turn, obliged under UN Regulation No. 155 (cyber security and cyber security management system) and UN Regulation No. 156 (software update and software update management system) to obtain vehicle type approval with respect to cyber security, and to implement cyber security engineering consistent with ISO/SAE 21434 “Road vehicles – Cybersecurity engineering”.

These obligations do not stop at the OEM: both UN Regulation No. 155 and ISO/SAE 21434 require the OEM – and, where Spheros acts as a Tier 1 or Tier 2 supplier, Spheros itself – to manage cyber security risk throughout the supply chain and to obtain evidence that suppliers apply appropriate cyber security measures. Spheros passes on the relevant parts of these requirements to its own suppliers through this document, so that Spheros can demonstrate a consistent and traceable cyber security engineering approach towards its customers.

Chapter 2 describes the basic product cyber security requirements that apply to all suppliers who deliver products, components, hardware or software with digital elements that become part of a Spheros product. These requirements are expanded in Chapter 3 to include specific requirements for suppliers of digital products, components or services with a direct cyber security relevance (e.g. control units, embedded software, communication or connectivity modules).

If Spheros identifies an increased cyber security risk for a specific product or component, additional individual cyber security requirements can be defined and agreed between Spheros and the Supplier – for example as part of a dedicated cyber security interface agreement – that extend or specify the minimum requirements set out in this document.

This document applies independently of any specific customer or program. Where a specific Spheros customer (OEM) imposes additional or more specific requirements on a given product, these will be communicated to the affected Suppliers separately.

2. Requirements for all suppliers of products, components, hardware or software with digital elements

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 product 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, including any product-specific cyber security interface agreement that may be concluded separately, shall remain unchanged.

2. general requirements for product cyber security at the supplier

(a) The Supplier's product cyber security risk management should be clearly defined and systematically implemented, consistent with the organizational and project-dependent cyber security management activities described in ISO/SAE 21434. A direct report to the management and a documented commitment to cyber security are necessary. Ideally, a cyber security management system in line with ISO/SAE 21434 and/or the cyber security management system requirements of UN Regulation No. 155 should be implemented.

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

- Threat analysis and risk assessment (TARA) for the delivered product or component
- Security-by-design and a secure development lifecycle for hardware and software
- Access control / multifactor authentication for development, engineering and production environments
- Response to product cyber security incidents
- Vulnerability management, including handling of vulnerability reports from third parties
- Cryptographic key management (generation, storage and distribution of keys used in or for the product)
- Secure software update processes, where applicable to the delivered product (relevant to UN Regulation No. 156)
- Traceability of software components, including open source and third-party software
- Encryption standards
- Protection against malware
- Connection from third-party providers

- Physical security, including security of production and key-handling processes
- Personnel security
- Network / perimeter security
- Data backup / backup copies of cyber security-relevant engineering data
- Secure software development

3. Cyber security rules for working with Spheros

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

(b) In the event of a product cyber security incident affecting a delivered product or component, or confidential Spheros information, the Supplier shall:

- Take immediate action to minimize the damage to Spheros and to the affected product or component
- 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.

(e) Spheros may verify compliance with the Supplier's product cyber security requirements by means of audits, including a review of the Supplier's threat analysis and risk assessment (TARA) and related evidence for the delivered product. 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 cyber 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.

(f) The Supplier must provide Spheros with information on the handling of Spheros data and on the general product cyber security status of the delivered product, 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 cyber security risks, Spheros reserves the right to obtain and evaluate further information based on the evaluation of the information provided.

(g) Spheros may require the Supplier to draw up and implement a concept for remedying product cyber security weaknesses if these are related to the provision of the delivered product or service. The Supplier must immediately take suitable measures and draw up a schedule that

is appropriate to the nature and severity of the weakness. If Spheros draws up its own concept, the Supplier must support Spheros in its implementation.

(h) The Supplier must inform Spheros of significant changes affecting product cyber security, such as changes to the security architecture of the delivered product, changes in technology, or the withdrawal/expiry of relevant certificates (e.g. cyber security or cryptographic 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 that are relevant to product cyber security. This includes software deliveries, digital services/cloud solutions connected to the delivered product, the delivery of hardware with digital elements (e.g. control units, 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 threat analysis and risk assessment (TARA) and, where 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 and/or component, listing all components, interfaces and data flows included. This documentation forms the basis for a cyber security interface agreement between Spheros and the Supplier, where such an agreement is required. User documentation must also be available that describes how the product can be used safely.

(c) Vulnerabilities in the software or component 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 and must be able to provide Spheros, on request, with an overview of the third-party and open source software used (e.g. a software bill of materials). 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 or component must follow a structured change management 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 cyber security support for the delivered product, 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 assured period must be reported to Spheros within a period of time appropriate 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 third-party components that are used in the Supplier’s product. The Supplier must provide appropriate contact options for cyber security queries.

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

3. requirements for the operation of digital services

The following requirements apply to Suppliers who operate digital services connected to a delivered product, that Spheros, its customers, other suppliers or partners use. These include software-as-a-service offerings and fully managed service contracts for infrastructure components (e.g. back-end services for a connected product):

(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:

- Observance of the least privilege and need-to-know principles when assigning authorizations
- Enforce complexity rules for passwords according to current standards
- Securing network access from the Internet through strong authentication (e.g. multi-factor authentication)
- Use of the latest technology against malware at relevant points
- Regular checks for vulnerabilities and prompt implementation of countermeasures and patches
- 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 objective (RPO) and the recovery time objective (RTO).

(d) In principle, Spheros information may only be processed and stored on 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 product cyber security risks that meets at least these requirements:

- Overview of identified risks and measures
- Security audits carried out (e.g. penetration tests)
- Security awareness measures implemented

References

This document reflects, in summarized and non-exhaustive form, requirements derived from UN Regulation No. 155 (uniform provisions concerning the approval of vehicles with regard to cyber security and cyber security management system), UN Regulation No. 156 (uniform provisions concerning the approval of vehicles with regard to software update and software update management system), and ISO/SAE 21434:2021 "Road vehicles – Cybersecurity engineering". It does not replace these documents. In case of any discrepancy, the current official version of the respective regulation or standard prevails.