CYBER SECURITY

Guidelines for Suppliers

25.09.2025

Contents

1. Introduction

In order to ensure the availability, confidentiality, and integrity of Samhammer processes and information, as well as to comply with legal obligations, Samhammer also attaches great importance to an appropriate level of security among its suppliers.

The requirements in Section 2 are therefore valid for all suppliers and delivery items relevant to information security and are intended to ensure a basic minimum level of cyber security. Depending on the delivery item, these requirements are supplemented in Section 3 by specific requirements for suppliers of service solutions and services with a digital reference.

In the event of an increased risk for Samhammer, individual cybersecurity requirements may be defined and agreed upon that extend or specify the minimum requirements described in this document.

2. Requirements for all suppliers

2.1 General provisions

a When using external employees and subcontractors, the supplier shall ensure that all obligations to be complied with by the supplier under this document are also complied with by the relevant external parties.

b If Samhammer is required to cooperate or provide assistance in order to comply with the cyber security requirements, the supplier is obliged to specify this explicitly and in writing.

c Other contractual agreements between Samhammer and the supplier remain unaffected.

2.2 General cyber security requirements for the supplier

a Cyber security risk management must be specifically located within the supplier's organization and approached systematically. A direct reporting line from the responsible department to senior management and a company-wide commitment to the importance and organization of cyber security are essential. Ideally, an information security management system in accordance with ISO 27001 or similar should be implemented.

b The supplier is obliged to implement proportionate technical and organizational measures to reduce risk in at least the following areas, as well as to regularly review and further develop their effectiveness:

- Permissible use of information security values
- Data protection
- Remote access
- Access control / multi-factor authentication
- Response to cyber security incidents
- Vulnerability/patch management
- Encryption standards
- Data/system classification
- Protection against malware
- Third-party connections
- Email/instant messaging
- Physical security
- Personnel security
- Network/perimeter security
- Data backup / backup copies
- Clean desk
- IT service continuity management / business continuity management (ITSCM / BCM)
- Secure software development

c All employees of the supplier must be trained regularly, at least once a year, on any risks related to cyber security and the applicable regulations.

2.3 Regulations in the working relationship with Samhammer with regard to cyber security

a The supplier undertakes to inform Samhammer (infosec@samhammer.de) without undue delay if a cyber security incident becomes known that has enabled or could enable unauthorized access to Samhammer information or has or could have a negative impact on the supplier‘s ability to deliver the agreed delivery item (hereinafter referred to as a „cyber security incident“).

b In the event of cyber security incidents affecting Samhammer information, the supplier shall:

- take appropriate and reasonable measures in case of imminent danger to minimize the damage to Samhammer
- document the measures taken in the context of a cyber security incident in a comprehensible manner and provide the documentation to Samhammer upon request
- coordinate the publication of information about a cyber security incident with Samhammer
- immediately report requests from authorities for information or for the transmission of information and coordinate the further course of action with Samhammer
- Subsequently, carry out a sufficient root cause analysis, define and implement preventive measures to prevent similar cases, and inform Samhammer about the action plan and regularly about its status until final implementation.

c If, for example, the supplier is requested by authorities to disclose information to third parties without Samhammer‘s consent, the supplier shall exhaust all legal remedies to prevent the disclosure and inform Samhammer immediately, provided this is legally permissible.

d If the supplier works with Samhammer systems and/or performs activities on Samhammer premises, the supplier undertakes to enforce and comply with the applicable Samhammer cyber security guidelines.

e At Samhammer‘s request at any time, at the latest upon termination of the supply relationship, the supplier must immediately return all assets provided to it by Samhammer for the fulfillment of the supply relationship. If the supplier still has access to Samhammer systems at this point in time, which were set up in connection with the provision of services, they may no longer use the Samhammer systems and must inform Samhammer immediately. Furthermore, the supplier is obliged to return all information/software developed and the agreed documentation to Samhammer upon request, at the latest upon termination of the supply relationship.

f If the supplier or its subcontractors have stored information about Samhammer that is no longer necessary to store, the supplier is obliged to notify Samhammer of this. After approval by Samhammer, the supplier or its subcontractors are obliged to delete the information immediately and securely.

g Samhammer is entitled to verify the supplier‘s compliance with the agreed security standards by conducting regular information security audits. For this purpose, the supplier shall, at Samhammer‘s request, immediately grant Samhammer access to the documents relevant for the audit, including, if necessary, by transmitting these documents. Furthermore, the supplier shall immediately provide Samhammer with the information required for the audit and grant Samhammer access to its premises during normal business hours, insofar as this is necessary for the audit. Samhammer shall announce the visit with reasonable advance notice. In the event of incidents that affect information security, Samhammer shall also be entitled to make unannounced visits. During the audit, Samhammer shall minimize any disruption to operational processes, take appropriate account of the supplier‘s trade secrets, and comply with statutory data protection requirements. Samhammer may also have the audits carried out by a third party, whereby this third party must be bound by professional or contractual confidentiality obligations towards outsiders.

h The supplier undertakes to provide Samhammer with information about the handling of Samhammer data and about information security in general so that Samhammer can classify the status of the supplier. This information is required initially and when new services are purchased from the supplier that require renewed information. This information can be provided via a questionnaire from Samhammer. In order to minimize potential information security risks, Samhammer reserves the right to obtain and evaluate further information based on the evaluation of the information provided.

i Samhammer may require the supplier to work with Samhammer to develop and implement a plan to remedy the breach of information security requirements, insofar as the breach is related to the provision of services to Samhammer. In particular, Samhammer may require the supplier to immediately initiate specific and appropriate remedial measures to remedy the breach of information security requirements. The plan must include a specific timetable. The timetable must be appropriate to the nature and severity of the breach of information security requirements. In the event that Samhammer itself draws up a plan to remedy the breach of the Code of Conduct, the supplier is obliged to support Samhammer in the implementation of this plan to an appropriate extent.

j Furthermore, the supplier undertakes to notify Samhammer of any significant changes that affect information security, such as changes in technology or the withdrawal/expiration of certificates. In the event that this results in significant negative effects on the level of security, Samhammer is entitled to withdraw from the contract on an extraordinary basis.

3. Requirements for suppliers of digitally related services or solutions

3.1 General requirements

In addition to Section 2, the following provisions apply to all suppliers of digitally related services or solutions. Among other things, this may include the delivery of software, the provision of digital services/cloud solutions, the operation of Samhammer IT and communication systems/applications, the delivery of IT system components with digital elements (e.g., software solutions, digital interfaces), and the development of software on commission. This does not include development services directly within Samhammer development processes and with Samhammer systems: in this regard, Samhammer‘s internal development specifications must be obtained and complied with.

a Any software developed by the supplier that is relevant to the delivery item (in particular hardware-related software, embedded software, and utility programs) must be subjected to a risk analysis and designed in accordance with the security-by-design approach, taking into account the current state of the art. Development must take place in a secure development process. In addition to systematic and regular checks for vulnerabilities (e.g., using SAST or DAST solutions and fuzzing/robustness testing tools) and their treatment, this also includes regular, at least annual, training of developers on security-related aspects of software development.

b Technical documentation for the software, including a list of the solutions contained therein (Software Bill of Material – „SBOM“), must be created and kept up to date, as well as user documentation describing how the software can be used and operated securely.

c Vulnerabilities that arise during the software lifecycle must be assessed in terms of their exploitability and impact (ideally according to CVSS) and dealt with appropriately.

d When integrating third-party software (including open source) into your own software, the supplier must ensure compliance with the above requirements. The supplier is also responsible for obtaining any necessary licenses and ensuring license compliance.

e Changes that affect the software must follow a structured process. In addition, the cybersecurity requirements in this document also apply to any changes made to the software.

3.2 Requirements for the delivery of services or solutions with digital elements

If the supplier provides services/solutions with digital elements, the following requirements also apply:

a Before the purchase contract is concluded, the supplier shall notify Samhammer of the period during which it will provide free updates to remedy vulnerabilities (hereinafter referred to as the „guaranteed period“).

b The supplier shall ensure that the service/solution is free of known exploitable vulnerabilities upon delivery.

c Exploitable vulnerabilities that become known within the guaranteed period must be reported to Samhammer within a reasonable time with relevant additional information and practicable mitigation options (patches, configuration changes) must be provided. It must be ensured that the mitigation of vulnerabilities can be carried out with reasonable effort, is possible via remote connections/online, and does not restrict existing data and functions. This applies in particular—but not exclusively—to solutions that are intended for integration into our services. The supplier shall provide appropriate contact options for any queries.

d In the event of cyber security incidents arising from the exploitation of vulnerabilities at Samhammer or in Samhammer services for which the supplier is responsible, the supplier shall support Samhammer with its knowledge and experience in order to minimize the damage.

e The user documentation, including information on the „intended use“ and „security best practices“ of the application, must be made available to Samhammer.

3.3 Requirements for the operation of digital services

The following requirements apply to suppliers who operate digital services that Samhammer uses for itself, its customers, other suppliers, or its partners. In addition to software-as-a-service offerings, this also includes, for example, full-managed service contracts for infrastructure components.

a The supplier undertakes to maintain an information security management system in accordance with ISO 27001 or equivalent standards, which covers the part of its organization relevant to the supply relationship.

b Samhammer information, the IT systems necessary for the contractual service, and data transfers must be secured by appropriate protective measures that take into account the current state of the art. This includes, in particular, but is not limited to:

- Compliance with the least privilege and need-to-know principles when assigning authorizations
- enforcing complexity rules for passwords in accordance with state-of-the-art rules for length and complexity
- Securing network access from the internet via strong authentication (e.g., multi-factor authentication)
- Using the latest technologies to combat malware in all relevant areas
- Regular testing for vulnerabilities and prompt implementation of countermeasures/installation of patches

c Unless otherwise agreed by the parties, the supplier shall define data backup and recovery processes and communicate the recovery point objective (RPO) and recovery time objective (RTO) to Samhammer.

d The supplier shall inquire about Samhammer's protection requirements for the processed/stored information. As a general rule, Samhammer information may only be processed and stored in premises that offer adequate protection against environmental influences and unauthorized access. In addition, the recovery processes and emergency procedures must be tested at least once a year and Samhammer must be provided with suitable evidence of this.

e The supplier is obliged to centrally log security-related events and to regularly examine the logs for anomalies.

f The supplier is obliged to maintain a reporting system for customer-relevant information security risks that meets at least the following requirements:

- Provision via a regular reporting cycle, at least once a year
- Overview of the identified customer-relevant risks and the measures taken to address them
- Security audits performed (e.g., penetration tests)
- Security awareness measures carried out

In case of discrepancies or ambiguities, the German version of this agreement shall prevail and be legally binding.