# CYBER SECURITY

## Anforderungen für Lieferanten

17.09.2025

## Inhalt


1. Einführung ..... 3
2. Anforderungen an alle Lieferanten ..... 3
   2.1 Allgemeine Regelungen ..... 3
   2.2 Allgemeine Anforderungen an die Cyber Security beim Lieferanten ..... 4
   2.3 Regelungen im Zusammenarbeitsverhältnis mit Samhammer in Bezug auf Cyber Security ..... 5
3. Anforderungen an Lieferanten von Service, Lösungen oder Dienstleistungen mit digitalem Bezug ..... 8
   3.1 Allgemeine Anforderungen ..... 8
   3.2 Anforderungen bei der Lieferung von Services, Lösungen oder Dienstleistungen mit digitalen Elementen ..... 9
   3.3 Anforderungen beim Betrieb von digitalen Services ..... 10

## 1. Einführung

Um die Verfügbarkeit, Vertraulichkeit und Integrität von Samhammer Prozessen und Informationen sicherzustellen, sowie, um gesetzlichen Verpflichtungen nachzukommen, legt Samhammer auch bei seinen Lieferanten großen Wert auf ein angemessenes Sicherheitsniveau.

Die Anforderungen im Abschnitt 2 sind daher für alle Lieferanten und Liefergegenstände mit Relevanz zur Informationssicherheit gültig und sollen ein grundlegendes Mindestmaß an Cyber-Security sicherstellen. Abhängig vom Liefergegenstand werden diese Anforderungen in Abschnitt 3 um spezifische Anforderungen für Lieferanten von Service-Lösungen und Dienstleistungen mit digitalem Bezug ergänzt.

Bei einem erhöhten Risiko für Samhammer können individuelle Cyber-Security-Anforderungen definiert und vereinbart werden, welche die in diesem Dokument beschriebenen Mindestanforderungen erweitern oder konkretisieren.

## 2. Anforderungen an alle Lieferanten

### 2.1 Allgemeine Regelungen

**a** Beim Einsatz von externen Mitarbeitern und Subunternehmern stellt der Lieferant sicher, dass alle von ihm einzuhaltenden Verpflichtungen aus diesem Dokument auch von den entsprechenden externen Parteien eingehalten werden.

**b** Sofern Mitwirkungspflichten / Beistellpflichten seitens Samhammer notwendig sind, ist der Lieferant verpflichtet diese explizit und schriftlich zu benennen.

**c** Andere vertragliche Vereinbarungen zwischen Samhammer und dem Lieferanten bleiben unberührt.

## 2.2 Allgemeine Anforderungen an die Cyber Security beim Lieferanten

**a** Das Cyber-Security-Risikomanagement muss in der Organisation des Lieferanten dediziert verortet und systematisch angegangen werden. Ein direkter Berichtsweg der verantwortlichen Stelle zur Geschäftsleitung und ein unternehmensweit veröffentlichtes Bekenntnis dieser zur Wichtigkeit und Organisation der Cyber Security sind zwingend. Idealerweise ist ein Informationssicherheitsmanagementsystem nach ISO 27001 oder analog implementiert.

**b** Der Lieferant ist verpflichtet mindestens zu folgenden Themenbereichen verhältnismäßige technische und organisatorische Maßnahmen zur Risikominderung umzusetzen, sowie deren Wirksamkeit regelmäßig zu überprüfen, und weiterzuentwickeln:

- Zulässiger Gebrauch von Informationssicherheitswerten
- Datenschutz
- Fernzugriff
- Zugriffskontrolle / Multifaktor-Authentifizierung
- Reaktion auf Cyber Security Vorfälle
- Schwachstellen- / Patch-Management
- Verschlüsselungsstandards
- Daten- / Systemklassifizierung
- Schutz vor Schadsoftware
- Anschluss von Drittanbietern
- E-Mail / Instant Messaging
- Physische Sicherheit
- Personalsicherheit
- Netzwerk- / Perimetersicherheit
- Datensicherung / Sicherungskopien
- Sauberer Schreibtisch
- IT Service Continuity Management / Business Continuity Management (ITSCM / BCM)
- Sichere Softwareentwicklung

**c** Alle Mitarbeiter des Lieferanten müssen hinsichtlich etwaiger Risiken im Zusammenhang mit Cyber Security und der geltenden Regelungen regelmäßig, mindestens einmal jährlich, geschult werden.

## 2.3 Regelungen im Zusammenarbeitsverhältnis mit Samhammer in Bezug auf Cyber Security

**a** Der Lieferant verpflichtet sich, Samhammer (infosec@samhammer.de) ohne schuldhaftes Zögern zu informieren, sofern ein Cyber-Security-Vorfall bekannt wird, der unberechtigten Zugriff auf Samhammer Informationen ermöglicht hat oder ermöglichen könnte oder negative Auswirkungen auf die Lieferfähigkeit des Lieferanten hinsichtlich des vereinbarten Liefergegenstands hat oder haben könnte (nachfolgend „Cyber Security-Vorfall“).

**b** Bei Cyber-Security-Vorfällen, die Informationen von Samhammer betreffen, wird der Lieferant:

- bei Gefahr in Verzug geeignete und angemessene Maßnahmen ergreifen, um den Schaden für Samhammer so gering wie möglich zu halten
- die im Rahmen eines Cyber-Security-Vorfalls ergriffenen Maßnahmen nachvollziehbar dokumentieren und die Dokumentation Samhammer auf Anfrage bereitstellen
- die Veröffentlichung der Informationen über einen Cyber-Security-Vorfall mit Samhammer abstimmen
- die Anfragen von Behörden zu Auskünften über oder für die Übermittlung von Informationen unverzüglich anzeigen und die weitere Vorgehensweise mit Samhammer abstimmen
- im Nachgang eine ausreichende Ursachenanalyse durchführen, vorbeugende Maßnahmen zur Verhinderung ähnlicher Fälle definieren und umsetzen sowie Samhammer über den Maßnahmenplan, als auch regelmäßig über den Status dessen, bis zur endgültigen Umsetzung informieren.

**c** Sollte der Lieferant z. B. durch Behörden dazu aufgefordert werden, Samhammer Informationen ohne Einverständnis von Samhammer an Dritte weiterzugeben, wird der Lieferant jeglichen Rechtsweg ausschöpfen, um die Weitergabe zu verhindern und Samhammer unverzüglich darüber informieren, sofern dies gesetzlich zulässig ist.

**d** Sofern der Lieferant mit Samhammer Systemen arbeitet und / oder Tätigkeiten auf dem Samhammer Gelände verrichtet, verpflichtet sich der Lieferant, die dafür gültigen Samhammer Cyber-Security-Richtlinien einzufordern und einzuhalten.

**e** Auf jederzeit mögliches Verlangen von Samhammer, spätestens bei Beendigung des Lieferverhältnisses, hat der Lieferant umgehend alle Assets zurückzugeben, die ihm von Samhammer zur Erfüllung des Lieferverhältnisses zur Verfügung gestellt wurden. Sollte der Lieferant zu diesem Zeitpunkt noch Zugriff auf Samhammer Systeme haben, welche im Zusammenhang mit der Leistungserbringung eingerichtet wurden, darf er die Samhammer Systeme nicht mehr nutzen und muss Samhammer umgehend darüber informieren. Ferner ist der Lieferant verpflichtet Samhammer sämtliche erarbeiteten Informationen / Software sowie die vereinbarte Dokumentation auf Verlangen, spätestens bei Beendigung des Lieferverhältnisses, zurückzugeben.

**f** Sollte der Lieferant oder dessen Subunternehmer gespeicherte Informationen über Samhammer haben, für die keine Speichernotwendigkeit mehr besteht, ist der Lieferant verpflichtet dies Samhammer anzuzeigen. Nach etwaiger Genehmigung durch Samhammer ist der Lieferant oder dessen Subunternehmen verpflichtet die Informationen unverzüglich und sicher zu löschen.

**g** Samhammer ist berechtigt, die Einhaltung der vereinbarten Sicherheitsstandards durch den Lieferanten, durch regelmäßige Informationssicherheits-Audits zu überprüfen. Hierzu gewährt der Lieferant Samhammer auf Verlangen von Samhammer unverzüglich Einsicht in die für die Prüfung relevanten Dokumente, gegebenenfalls auch durch Übermittlung dieser Dokumente. Des Weiteren erteilt der Lieferant Samhammer unverzüglich die für die Prüfung erforderlichen Auskünfte und gewährt Samhammer während der üblichen Geschäftszeiten Zutritt zu seinen Räumlichkeiten, soweit für die Prüfung erforderlich. Samhammer wird den Besuch mit einer angemessenen Vorlaufzeit ankündigen. Bei Auftreten von Ereignissen, die die Informationssicherheit beeinflussen, ist Samhammer auch zu unangekündigten Besuchen berechtigt. Samhammer wird bei der Auditierung die Beeinträchtigung der Betriebsabläufe so gering wie möglich halten, in angemessenem Umfang Rücksicht auf die Geschäftsgeheimnisse des Lieferanten nehmen und den gesetzlichen Datenschutz wahren. Samhammer darf die Audits auch von einem Dritten ausüben lassen, wobei dieser Dritte von Berufs wegen oder vertraglich gegenüber Außenstehenden zur Verschwiegenheit verpflichtet sein muss.

**h** Der Lieferant verpflichtet sich, Samhammer Auskunft über den Umgang mit den Daten von Samhammer und im Generellen zur Informationssicherheit zu geben, damit Samhammer den Status des Lieferanten einordnen kann. Diese Auskunft ist initial erforderlich und wenn neue Services oder Dienste vom Lieferanten bezogen werden, die eine erneute Auskunft erfordern. Diese Auskunft kann über einen Fragebogen von Samhammer erfolgen. Um potenzielle Informationssicherheits-Risiken zu minimieren, behält sich Samhammer das Recht vor, basierend auf der Auswertung der Auskunft, weitere Informationen einzuholen und zu bewerten.

**i** Samhammer kann von dem Lieferanten verlangen, dass dieser gemeinsam mit Samhammer ein Konzept zur Beseitigung der Verletzung der Informationssicherheitsanforderungen erstellt und umsetzt, soweit die Verletzung im Zusammenhang mit der Leistungserbringung für Samhammer steht. Insbesondere kann Samhammer von dem Lieferanten verlangen, dass dieser unverzüglich konkrete und angemessene Abhilfemaßnahmen zur Beseitigung der Verletzung der Informationssicherheitsanforderungen einleitet. Das Konzept muss einen konkreten Zeitplan beinhalten. Der Zeitplan muss zu der Art und Schwere der Verletzung der Informationssicherheitsanforderungen angemessen sein. Für den Fall, dass Samhammer selbst ein Konzept zur Beseitigung der Verletzung des Verhaltenskodex erstellt, ist der Lieferant verpflichtet, Samhammer bei der Umsetzung dieses Konzepts in angemessenem Umfang zu unterstützen.

**j** Weiter verpflichtet sich der Lieferant wesentliche Änderungen mit Auswirkung auf Informationssicherheit, wie beispielsweise Technologiewechsel oder der Entzug / Ablauf von Zertifikaten an Samhammer zu melden. Für den Fall, dass dadurch wesentliche negative Auswirkungen auf das Sicherheitsniveau resultieren, ist Samhammer berechtigt vom Vertrag außerordentlich zurücktreten.

## 3. Anforderngen an Lieferanten von Service, Lösungen oder Dienstleistungen mit digitalem Bezug

### 3.1 Allgemeine Anforderungen

Ergänzend zu Abschnitt 2 gelten die folgenden Regelungen für alle Lieferanten von Services, Lösungen oder Dienstleistungen mit digitalem Bezug. Unter anderem kann dies die Lieferung von Software, das Anbieten von digitalen Services / Cloud-Lösungen, der Betrieb von Samhammer IT- und Kommunikationssystemen / -anwendungen, die Lieferung von IT-Systemkomponenten mit digitalen Elementen (z. B. Softwarelösungen, digitale Schnittstellen) als auch die Auftragsentwicklung von Software sein. Ausgenommen sind Entwicklungsdienstleistungen direkt innerhalb der Samhammer Entwicklungsprozesse und mit Samhammer Systemen: diesbezüglich sind die Samhammer internen Entwicklungsvorgaben einzuholen und einzuhalten.

**a** Jegliche vom Lieferanten entwickelte Software, die eine Relevanz für den Liefergegenstand hat (insbesondere auch hardwarenahe Software, embedded Software, Hilfsprogramme), ist einer Risiko-Analyse zu unterziehen und gemäß dem Security-by-Design-Ansatz unter Beachtung des aktuellen Stands der Technik zu konzipieren. Die Entwicklung muss in einem sicheren Entwicklungsprozess erfolgen. Dies umfasst neben der systematischen und regelmäßigen Überprüfung nach Schwachstellen (z. B. durch SAST- oder DAST-Lösungen sowie Fuzzing / Robustness Testing Tools) und deren Behandlung auch die regelmäßige, mindestens jährliche, Schulung von Entwicklern zu sicherheitsbezogenen Aspekten der Softwareentwicklung.

**b** Für die Software ist eine technische Dokumentation inklusive der Auflistung der enthaltenen Lösungen (Software Bill of Material – „SBOM“) zu erstellen und aktuell zu halten sowie eine User-Dokumentation, welche beschreibt, wie die Software sicher eingesetzt und genutzt werden kann.

**c** Schwachstellen, die im Lebenszyklus der Software auftreten, müssen hinsichtlich ihrer Ausnutzbarkeit sowie Auswirkungen bewertet (idealerweise nach CVSS) und angemessen behandelt werden.

**d** Bei der Integration von Fremdsoftware (inkl. Open-Source) in die eigene Software, ist die Einhaltung der genannten Anforderungen durch den Lieferanten sicherzustellen. Ebenso ist der Lieferant dafür verantwortlich, dass ggf. notwendige Lizenzierungen erfolgen und die Licence Compliance gegeben ist.

**e** Änderungen mit Auswirkungen auf die Software müssen einem strukturierten Prozess folgen. Zudem finden auch bei etwaigen Änderungen auf die Software die Cyber Secucrity Anforderungen aus diesem Dokument Anwendung.

### 3.2 Anforderungen bei der Lieferung von Service, Lösungen oder Dienstleistungen mit digitalen Elementen

Sofern der Lieferant Services / Lösungen mit digitalen Elementen liefert, gelten zusätzlich die folgenden Anforderungen:

**a** Vor dem Zustandekommen des Kaufvertrags meldet der Lieferant Samhammer, in welchem Zeitraum er kostenlose Updates für die Behebung von Schwachstellen zur Verfügung stellen wird (nachfolgend „zugesicherter Zeitraum“).

**b** Der Lieferant stellt sicher, dass das Service / die Lösung bei Auslieferung frei von bekannten ausnutzbaren Schwachstellen ist.

**c** Ausnutzbare Schwachstellen, die innerhalb des zugesicherten Zeitraums bekannt werden, müssen Samhammer in angemessener Zeit mit relevanten Zusatzinformationen gemeldet und praktikable Mitigationsmöglichkeiten (Patches, Konfigurationsänderungen) zur Verfügung gestellt werden. Dabei ist sicherzustellen, dass die Mitigation der Schwachstellen mit angemessenem Aufwand erfolgen kann, über Fernverbindungen / online möglich ist und bestehende Daten und Funktionen nicht einschränkt. Dies gilt insbesondere - aber nicht ausschließlich – auch für Lösungen, die zum Einbau in unsere Services gedacht sind. Für Rückfragen stellt der Lieferant entsprechende Kontaktmöglichkeiten zur Verfügung.

**d** Bei Cyber Security Vorfällen, die durch die Ausnutzung vom Lieferanten zu verantwortender Schwachstellen bei Samhammer oder in Samhammer Services entstehen, wird der Lieferant Samhammer mit seinem Wissen und Erfahrung unterstützen, den Schaden möglichst gering zu halten.

**e** Die User-Dokumentation inklusive Angaben zu „intended use“ und „security best practices“ der Anwendung ist Samhammer zur Verfügung zu stellen.

### 3.3 Anforderungen beim Betrieb von digitalen Services

Die folgenden Anforderungen gelten für Lieferanten, die digitale Services betreiben, welche Samhammer für sich, seine Kunden, andere Lieferanten oder seine Partner nutzt. Hierzu gehören neben Software-as-a-Service-Angeboten z. B. auch Full-Managed-Service-Verträge für Infrastrukturkomponenten.

**a** Der Lieferant verpflichtet sich ein Informationssicherheitsmanagementsystem gemäß ISO 27001 oder gleichwertiger Standards zu unterhalten, welches den für die Lieferbeziehung relevanten Teil seiner Organisation abdeckt.

**b** Die Samhammer Informationen, die zur vertragsgegenständlichen Leistung notwendigen IT- Systeme sowie die Datenübertragungen müssen über angemessene Schutzmaßnahmen, die den aktuellen Stand der Technik beachten, abgesichert werden. Dazu gehören insbesondere aber nicht abschließend:

- die Beachtung der Least-Privilege und Need-to-Know Prinzipien bei der Berechtigungsvergabe
- das Erzwingen von Komplexitätsregeln für Passwörter gemäß state-of-the-art Regeln für Länge und Komplexität
- die Absicherung der Netzwerkzugänge aus dem Internet über eine starke Authentifizierung (z.B. Multi-Faktor-Authentifizierung)
- der Einsatz von aktuellen Technologien gegen Schadsoftware an allen relevanten Stellen
- die regelmäßige Prüfung auf Schwachstellen und zeitnahe Implementierung von Gegenmaßnahmen / Installation von Patches

**c** Sofern die Parteien nichts anderes vereinbart haben, definiert der Lieferant Datensicherungs- und Wiederherstellungsprozesse und kommuniziert den Wiederherstellungszeitpunkt (RPO) sowie die Wiederherstellungsdauer (RTO) an Samhammer.

**d** Der Lieferant hat den Schutzbedarf der verarbeiteten / gespeicherten Informationen seitens Samhammer zu erfragen. Grundsätzlich dürfen Samhammer Informationen nur in Räumlichkeiten verarbeitet und gespeichert werden, die einen angemessenem Schutz vor Umwelteinflüssen und dem Zutritt / Zugriff Unberechtigter bieten. Zudem sind die Wiederherstellungsprozesse und Notfallprozesse mindestens einmal jährlich zu testen und Samhammer ein geeigneter Nachweis darüber bereitzustellen.

**e** Der Lieferant ist verpflichtet sicherheitsrelevante Ereignisse zentral zu protokollieren und die Protokolle regelmäßig auf Auffälligkeiten hin zu untersuchen.

**f** Der Lieferant ist verpflichtet ein Berichtswesen über kundenrelevante Informationssicherheitsrisiken zu unterhalten, dass mindestens den folgenden Anforderungen genügt:

- Bereitstellung über einen regelmäßigen Berichtszyklus, mindestens einmal jährlich
- Übersicht über die identifizierten kundenrelevanten Risiken und deren Maßnahmen
- Durchgeführte Sicherheitsaudits (z.B. Penetrationstests)
- Durchgeführte Security-Awareness-Maßnahmen