|  |
| --- |
| **Vertragsergänzung IT-Sicherheit** |

Inhaltsverzeichnis

[1 Geltungsbereich und allgemeine Bedingungen 2](#_Toc446665392)

[2 Verfügbarkeit von IT-Sicherheitssystemen 3](#_Toc446665393)

[3 Umgang mit Sicherheitsvorfällen 3](#_Toc446665394)

[4 Umgang mit Sicherheitswarnungen 3](#_Toc446665395)

[5 Datenschutz 4](#_Toc446665396)

[6 IT Service Management 5](#_Toc446665397)

[6.1 Capacity Management 5](#_Toc446665398)

[6.2 Continuity Management 5](#_Toc446665399)

[6.3 Change Management 5](#_Toc446665400)

[6.4 Configuration Management 6](#_Toc446665401)

[6.5 Computer Emergency Response Team (CERT) 6](#_Toc446665402)

[7 Administration 6](#_Toc446665403)

[8 Schutz von Informationen 6](#_Toc446665404)

[9 Datensicherung (Backup) 7](#_Toc446665405)

[10 Security Audits 7](#_Toc446665406)

[11 Reporting 8](#_Toc446665407)

[12 Fachkenntnisse des Service Providers 8](#_Toc446665408)

[13 Subunternehmer 8](#_Toc446665409)

[14 Mitwirkungspflichten des Auftraggebers 8](#_Toc446665410)

[15 Weitere Richtlinien 8](#_Toc446665411)

[16 Ansprechpartner 8](#_Toc446665412)

# Geltungsbereich und allgemeine Bedingungen

Das SSLA regelt die Sicherheit von Informationen und Systemen, die zur Erbringung der im Vertrag zwischen dem Auftraggeber oder Kunden (in diesem Dokument „**Auftraggeber**“ genannt) und dem IT-Dienstleister bzw. Lieferanten (in diesem Dokument „**Service Provider**“ genannt) über IT-Dienstleistung genannten Services erforderlich sind, sowie die Einhaltung von Prozessen, die Überprüfung von Vorgaben und die bei Sicherheitsvorfällen verpflichtenden Kommunikations- und Eskalationswege.

Der Auftraggeber hat einen fachkundigen Ansprechpartner für alle Sicherheitsaspekte zu benennen.

Das SSLA ist Bestandteil des [Vertrags] vom [bitte einfügen].

Ist der Service Provider nicht in der Lage, die in diesem Dokument geforderten Anforderungen umzusetzen, so übernimmt er die vollumfängliche Haftung von durch Sicherheitsvorfälle entstandene Schäden, welche durch die Nicht-Beachtung dieser Anforderungen ermöglicht wurden.

# Verfügbarkeit von IT-Sicherheitssystemen

Eine Mindestverfügbarkeit von 99% pro Monat für alle Systeme, die zur sicheren Erbringung der im Vertrag über Systembetreuung genannten Dienstleistungen und Services erforderlich sind, ist durch den Service Provider sicherzustellen.

# Umgang mit Sicherheitsvorfällen

Ein Sicherheitsvorfall ist ein Ereignis, welches die Verfügbarkeit (availability), Integrität (integrity) oder Vertraulichkeit (confidentiality) von Informationen, Geschäftsprozessen, IT-Diensten, IT-Systemen oder IT-Anwendungen mit mit hohem oder sehr hohem Schutzbedarf derart beeinträchtigt, dass ein großer Schaden entstehen kann.[[1]](#footnote-1)

Ein Sicherheitsvorfall hat eine HOHE Kritikalität, wenn ein oder mehrere Systeme oder Netzwerkkomponenten des Service Providers erfolgreich angegriffen werden oder durch negative Berichterstattung ein Image-Schaden des Auftraggebers herbeigeführt wurde oder wird. Dabei ist es unerheblich, ob der Angriff über das Internet oder die vom Service Provider zu verantwortende Infrastruktur erfolgt, und ob er von Dritten, Angestellten oder Subunternehmers des Service Providers ausgeführt wird.

Der Service Provider hat geeignete Methoden und Systeme einzusetzen, um Angriffe zu erkennen.

Folgende Reaktionen sind auf Sicherheitsvorfälle gefordert:

| Vorgabe | Hohe Kritikalität | Normale Kritikalität |
| --- | --- | --- |
| Meldung an Auftraggeber[[2]](#footnote-2) | Unverzüglich | Am gleichen Tag |
| Problembehebung | Unverzüglich | Innerhalb einer Woche |

Bei Sicherheitsvorfällen mit hoher Kritikalität kann der Service Provider in Abstimmung mit dem Auftraggeber entscheiden, dass die Verfügbarkeit der potentiell oder akut betroffenen IT-Systeme, Dienste oder Daten einen geringeren Stellenwert als der Schutz der Daten bzw. anderer IT-Systeme und Dienste hat, und die betroffenen IT-Systeme oder Dienste bis zur Lösung des Sicherheitsproblems deaktivieren.

# Umgang mit Sicherheitswarnungen

Der Auftragnehmer muss zur Wahrung der Sicherheit seiner Systeme und der der von ihm beim Auftraggeber betreuten Systeme auf Sicherheitswarnungen („Security Advisories“) verschiedener Organisationen reagieren. Als Quelle für Warnungen vor Verwundbarkeiten sind mindestens die Mailing-Listen und Web-Seiten der Hersteller der eingesetzten Applikationen, Dienste und Betriebssysteme sowie die herstellerunabhängigen Foren der Bugtrack-Mailingliste zu verfolgen.

Bei einer Sicherheitswarnung der Kritikalität HOCH handelt es sich um eine Verwundbarkeit auf einem oder mehreren Systemen oder Netzwerkkomponenten des Service Providers, bei dem die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten bzw. Diensten beim Service Provider oder beim Auftraggeber wesentlich beeinträchtigt, oder durch negative Berichterstattung ein Image-Schaden des Auftraggebers herbeigeführt werden könnte.

Folgende Reaktionen sind auf Sicherheitswarnungen gefordert. Unter Problembehebung ist dabei auch das Einspielen aller relevanten Patches zu verstehen.

| Vorgabe | Hohe Kritikalität | Normale Kritikalität |
| --- | --- | --- |
| Meldung an Auftraggeber[[3]](#footnote-3) | Unverzüglich | Innerhalb eines Tages, falls Systeme des Auftraggebers direkt betroffen sind, sonst über das reguläre Reporting |
| Problembehebung | Unverzüglich, ggf. alternative Schutzmaßnahmen umsetzen, wenn kein Patch verfügbar | Innerhalb einer Woche |

Bei Sicherheitswarnungen mit hoher Kritikalität kann der Service Provider in Abstimmung mit dem Auftraggeber entscheiden, dass die Verfügbarkeit der potentiell oder akut betroffenen IT-Systeme, Dienste oder Daten einen geringeren Stellenwert als der Schutz der Daten bzw. anderer IT-Systeme und Dienste hat und die betroffenen IT-Systeme oder Dienste bis zur Lösung des Sicherheitsproblems deaktivieren.

# Datenschutz

Werden personenbezogene Daten des Auftraggebers, von Mitarbeitern oder Kunden verarbeitet, so sind die gesetzlichen Vorgaben an den Datenschutz einzuhalten.

Bei Ausscheiden eines Mitarbeiters des Service Providers oder sonst einer von ihm zur Leistungserbringung eingesetzten Person, die Zugriffsrechte auf Datenverarbeitungssysteme des Auftraggebers hatte, welche die Einsicht, Eingabe, Änderung oder Löschung personenbezogener Daten ermöglichen, sind folgende Maßnahmen zu treffen:

1. Das Benutzerkonto dieser Person ist umgehend in allen Datenverarbeitungssystemen zu deaktivieren, beziehungsweise für die ausgeschiedene Person unzugänglich zu machen,
2. Alle Passwörter, die der Person im Rahmen ihrer Funktion zugänglich waren sind sofort nach deren Ausscheiden zu ändern,
3. Sämtliche im Besitz der Person befindlichen Unterlagen, die Informationen zu Datenverarbeitungssystemen enthalten, sind vor deren Ausscheiden einzuziehen.

# IT Service Management

Um die Einhaltung der in diesem Dokument genannten Vorgaben und Anforderungen kontinuierlich sicherzustellen, verpflichtet sich der Service Provider dazu, die folgenden Aspekte[[4]](#footnote-4) zu beachten:

## Capacity Management

Der Service Provider stellt sicher, dass auch in Zeiten erhöhten Serviceaufkommens genügend Ressourcen zur Verfügung stehen, damit alle Leistungen in dem vertraglich vereinbarten Umfang erbracht werden können, ohne dass sicherheitsrelevante Aufgaben vernachlässigt werden. Mit Ressourcen sind an dieser Stelle neben Personal auch Hardware, Anbindungen an Netze und Kommunikationsmittel gemeint.

In besonderem Maße hat der Service Provider sicherzustellen, dass bei Sicherheitsvorfällen und Sicherheitswarnungen mit hoher Kritikalität ausreichend Personal mit dem entsprechenden Fachwissen zur Verfügung steht.

Bei Problemen im Bereich der Kapazität ist eine gesonderte Meldung mit Begründung für den Zustand an den Auftraggeber vorzunehmen.

## Continuity Management

Der Service Provider verpflichtet sich zu einer kontinuierlichen Risikoanalyse im Rahmen seines Geschäftsbetriebs. Er hat dem Auftraggeber jederzeit auf Anforderung folgende Informationen bzw. Nachweise vorzulegen:

1. Notfallplan, der in Kraft tritt, wenn der Service Provider von einem Katastrophenfall betroffen ist (Erdbeben, Flutkatastrophe, Flugzeugabsturz, Feuer, etc.),
2. Nachweis über erfolgte Tests im Bereich der Notfall-Vorsorge und deren Ergebnisse,
3. Analyse der aktuell für den Service Provider relevanten Risiken inklusive des beschlossenen Maßnahmenplans,
4. Nachweis über durch den Service Provider ergriffene Maßnahmen zur Reduzierung von Risiken bzw. über die Versicherung von Restrisiken.

## Change Management

Der Service Provider muss sämtliche Änderungen an Systemen und Diensten, die Auswirkungen auf die Sicherheit der Systeme oder auf die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten und Diensten haben können, im Rahmen eines „Request for Change“ beim Auftraggeber beantragen. Der „Request for Change“ muss mindestens die folgenden Informationen enthalten:

1. Beschreibung der durchzuführenden Arbeiten
2. Sicherheitsimplikationen: Welche Auswirkungen auf die Verfügbarkeit und Sicherheit von IT-Systemen und Diensten hat eine Ablehnung des Antrags?
3. Auswirkungen: Welche möglichen Auswirkungen hat die Implementierung der Änderung auf IT-Systeme oder Dienste?

Für Änderungen, die im Rahmen der Bearbeitung eines Sicherheitsvorfalls oder einer Sicherheitswarnung mit hoher Kritikalität erforderlich sind, kann der „Request for Change“ auch nachträglich gestellt werden.

## Configuration Management

Der Service Provider ist verpflichtet, eine Inventarisierung aller Systeme („CMDB“) fortlaufend so zu pflegen, dass die Abhängigkeiten der einzelnen Systeme untereinander klar ersichtlich sind und detailliert nachvollzogen werden können, um im Falle eines Sicherheitsvorfalls die betroffenen Systeme umgehend identifizieren und die tatsächliche Gefährdung einschätzen zu können.

## Computer Emergency Response Team (CERT)

Der Service Provider muss ein mit qualifiziertem Fachpersonal besetztes Computer Emergency Response Team (CERT) besitzen. Das CERT hat drei Aufgaben:

1. Verfolgen von Sicherheitswarnungen,
2. Bewertung von Sicherheitswarnungen bezüglich der Relevanz und Priorität für die eingesetzten IT-Systeme, Anwendungen und Dienste,
3. Koordinierung von Arbeiten und Notfallmaßnahmen im Falle von Sicherheitsvorfällen.

# Administration

Bei der Administration von wesentlichen, zentralen Sicherheitskomponenten (Firewall, Gateway-Viren-Scanner, Intrusion Detection Systemen, Benutzerverwaltung, usw.) muss das Mehraugenprinzip angewendet werden. Durch organisatorische und/oder technische Maßnahmen ist sicherzustellen, dass ein einzelner Administrator nicht berechtigt bzw. in der Lage ist, die Zugriffsrechte anderer Anwender zu erhöhen oder Sicherheitskomponenten außer Kraft zu setzen. Bei der Änderung von Regelwerken zentraler Sicherheitskomponenten (z.B. Firewall, Viren-Scanner) ist vor der Aktivierung eines neuen Regelwerks durch einen zweiten Administrator die korrekte Umsetzung des Request for Change zu verifizieren.

Werden Systeme aus der Ferne administriert, so gelten folgende zusätzliche Anforderungen:

1. Die gesamte Remote-Administrationssitzung muss verschlüsselt erfolgen,
2. Es dürfen zu keinem Zeitpunkt Authentifikationsinformationen (z. B. Benutzername/Passwort) im Klartext über das Internet oder ein anderes Weitverkehrsnetz übertragen werden,
3. Für die Authentifikation eines Administrators sind jeweils mindestens zwei Faktoren einzusetzen,
4. Remote-Administrationszugriffe sind zu protokollieren.

# Schutz von Informationen

Der Service Provider hat Verhaltensrichtlinien zum Zwecke des Sicherns von Informationen des Auftraggebers und seiner Kunden für seine Mitarbeiter aufzustellen. Die technischen Sicherheitsmaßnahmen zum Informationsschutz müssen dem State-of-the-Art (entsprechend ISO 27001 Anhang A) entsprechen. Für Systeme, die für die Erbringung der Dienstleistung für den Auftraggeber vom Internet aus erreichbar sein müssen (exponierte Systeme), sind darüber hinaus die folgenden Anforderungen umzusetzen:

1. Alle Betriebssysteme sind zu härten: Sämtliche nicht benötigten Dienste auf dem exponierten System müssen deaktiviert werden. Außerdem sind nicht erforderliche Benutzerkonten zu löschen.
2. Die Betriebssysteme, Dienste und Anwendungen sind auf aktuellem Stand zu halten. Alle verfügbaren und sicherheitsrelevanten Patches sind – nach vorheriger Funktionsprüfung – umgehend zu installieren.
3. Durch ein mehrstufiges Firewall-System (Stateful Inspection + Paketfilter) ist der Zugang vom Internet auf das exponierte System auf die für die Erbringung des Dienstes benötigten Kommunikationsprotokolle einzuschränken.

# Datensicherung (Backup)

Die Datensicherung ist regelmäßig durchzuführen. Zur Realisierung ist eine dem aktuellen Stand der Technik entsprechende Backup-Lösung einzusetzen. Der Service Provider stellt sicher, dass alle deutschen gesetzlichen Bestimmungen bezüglich der Aufbewahrungsfristen von Daten strengstens eingehalten und überwacht werden. Diese sind im Anhang zusammengefasst.

Der Service Provider ist verpflichtet, alle Datensicherungen von Systemen auf deren erfolgreichen Ablauf, Vollständigkeit und Fehlerfreiheit hin zu überprüfen. Das Ergebnis der jeweiligen Überprüfung ist in geeigneter Form zu dokumentieren. Um die Konsistenz der Datensicherungen und ein reibungsloses Rücksichern im Schadensfall sicherzustellen, ist der Service Provider verpflichtet, mindestens alle 6 Monate einen Disaster Recovery Test durchzuführen.

Soweit möglich sind die Daten auf dem Datenträger mit einem auf dem aktuellen Stand der Technik befindlichen System zu verschlüsseln. Datenträger sind grundsätzlich in dafür geeigneten Schutzschränken zu lagern. Außerhalb der Geschäftsräume des Service Providers dürfen Datenträger nur bei einer Bank oder einem nachweislich auf die Lagerung von Datenträgern spezialisierten Unternehmen gelagert werden. Ausnahmen sind in Absprache mit dem Auftraggeber möglich.

Sobald Datenträger nicht mehr benutzt werden, sind sie zu zerstören oder die Daten müssen so gelöscht werden, dass keine Daten mehr zugänglich sind.

# Security Audits

Der Auftraggeber hat das Recht, jederzeit Security Audits durchzuführen. Die Durchführung der Security Audits wird mit einer Vorlaufzeit von mindestens 7 Tagen seitens des Auftraggebers bekannt gegeben.

Der Service Provider ist verpflichtet, durch regelmäßige Penetrationstests die Informationen in der CMDB dokumentierten IT-Systeme, Anwendungen und Dienste zu verifizieren und seine Systeme auf Sicherheitsschwachstellen zu untersuchen.

Werden im Rahmen der Untersuchungen Sicherheitsschwachstellen aufgedeckt, müssen diese unverzüglich vom Service Provider beseitigt werden. Dazu ist dem Auftraggeber binnen einer Frist von 1 Woche ein Konzept zur Beseitigung der Sicherheitsschwachstellen vorzulegen.

# Reporting

Der Service Provider ist verpflichtet, ein monatliches Security-Reporting durchzuführen. Das Reporting enthält mindestens Informationen über alle im Berichtszeitraum bearbeiteten:

1. Request for Changes,
2. Sicherheitsvorfälle,
3. Sicherheitswarnungen und
4. Security Audits.

# Fachkenntnisse des Service Providers

Der Service Provider hat dafür Sorge zu tragen, dass die mit der Betreuung von Systemen gemäß Vertrag über Systembetreuung betrauten Mitarbeiter für die entsprechenden Systemtypen und herstellerspezifischen Softwaremodule qualifiziert und ggf. zertifiziert sind. Dies gilt insbesondere für solche Mitarbeiter, die mit der Administration von sicherheitsrelevanten Systemen betraut sind (z.B. Firewall, zentraler Virenschutz und Intrusion Detection Systeme).

# Subunternehmer

Bei Einsatz von Subunternehmern und Erfüllungsgehilfen zur Erbringung der Services und Dienstleistungen gemäß Vertrag über Systembetreuung haftet der Service Provider grundsätzlich unbeschränkt als Generalunternehmer gegenüber dem Auftraggeber und seiner Kunden in Bezug auf Sicherheitsverletzungen oder Imageschäden.

# Mitwirkungspflichten des Auftraggebers

Der Auftraggeber verpflichtet sich, dem Service Provider alle zur Einhaltung der Anforderungen aus diesem Dokument erforderlichen Daten, Informationen und Dokumente zur Verfügung zu stellen.

Der Auftraggeber trägt dafür Sorge, dass gemäß insbesondere im Falle eines Sicherheitsvorfalls ein qualifizierter und autorisierter Ansprechpartner zur Verfügung steht.

# Weitere Richtlinien

Im Falle von länderübergreifendem Service-Providing müssen die Richtlinien und Gesetze aller beteiligten Länder eingehalten werden.

# Anhang A

**Verpflichtende Angaben für eine Sicherheitsmeldung an den Auftraggeber:**

1. **ID**

<*Bitte vergeben Sie eine ID für die Meldung, z.B. FIRMA-2016-01*>

1. **Historie**

Version - Datum - Ersteller - Kurzbeschreibung

<*Bei einem Update einer Sicherheitsmeldung erstellen Sie bitte keine neue Meldung, sondern erstellen Sie ein Update einer bestehenden Meldung – auch wenn eine neue Lage mit höherem Risiko eingetreten ist*.>

1. **Betroffene IT-Systeme bzw. IT-Dienste**

<*Hier sind die \_betroffenen\_ Systeme bzw. Dienste zu nennen, also, diejenigen, auf die sich das Risiko auswirkt - das sind in der Regel nicht die, bei denen das Problem auftritt. Beispiel: Das Problem tritt auf bei Apache Webserver, betroffen im Sinne des Risikos sind etwa alle Webdienste*.>

1. **Typ**

Sicherheitsvorfall oder Sicherheitswarnung.

1. **Kritikalität**

NORMAL oder HOCH.

1. **Auswirkungen und Konsequenzen**

<*Hier sind die Auswirkungen zu beschreiben, sowie Informationen zusammen zu tragen, welche Konsequenzen der Angriff / die Schwachstelle hat bzw. haben kann*.>

1. **Ergriffene Maßnahmen bzw. Empfehlungen**

<*Hier sind die ergriffenen Maßnahmen zu beschreiben, und ggf. Empfehlungen an den Auftraggeber, was zu berücksichtigen ist um mit dem erhöhten Risiko angemessen umzugehen, bis das Problem behoben ist.*>

1. **Voraussichtlicher Zeitpunkt der Problembehebung**

<*Hier ist eine Schätzung abzugeben, ab welchem Datum wieder ein Normalbetrieb möglich sein sollte*.>

1. **Weiterführende Informationen**

<*Verweis auf Schwachstellenmeldungen etc. mit Link falls verfügbar*.>

# Anhang B

**Aufbewahrungsfristen für Informationen und Dokumente[[5]](#footnote-5):**

**6 Jahre:** Nach § 257 Abs. 1 Nr. 2 und 3 HGB sind empfangene [Handelsbriefe](https://de.wikipedia.org/wiki/Handelsbrief), Wiedergaben ([Kopien](https://de.wikipedia.org/wiki/Fotokopie), Durchschriften) abgesandter Handelsbriefe, Geschäftspapiere und sonstige Unterlagen mit kaufmännischer und steuerlicher Bedeutung sechs Jahre aufzubewahren. Dies gilt auch für E-Mail-Kommunikation und Transaktionen in Web-Portalen.

**10 Jahre:** Nach § 257 Abs. 1 Nr. 1 und 4 HGB sind [Handelsbücher](https://de.wikipedia.org/wiki/Handelsbuch), [Inventare](https://de.wikipedia.org/wiki/Inventar), Personalakten, [Eröffnungsbilanzen](https://de.wikipedia.org/wiki/Er%C3%B6ffnungsbilanz), [Jahresabschlüsse](https://de.wikipedia.org/wiki/Jahresabschluss), Einzelabschlüsse nach [§ 325](http://www.gesetze-im-internet.de/hgb/__325.html) Abs. 2a HGB, [Lageberichte](https://de.wikipedia.org/wiki/Lagebericht), sowie die zu ihrem Verständnis erforderlichen [Arbeitsanweisungen](https://de.wikipedia.org/wiki/Arbeitsanweisung) und sonstigen Organisationsunterlagen zehn Jahre aufzubewahren. Das gilt auch für [Buchungsbelege](https://de.wikipedia.org/wiki/Buchungsbeleg) zu den nach [§ 238](http://www.gesetze-im-internet.de/hgb/__238.html) Abs. 1 HGB zu führenden Büchern. Eingangs- und Ausgangsrechnungen sind ebenfalls zehn Jahre aufzubewahren ([§ 14b](http://www.gesetze-im-internet.de/ustg_1980/__14b.html) [Umsatzsteuergesetz](https://de.wikipedia.org/wiki/Umsatzsteuergesetz)). Die betrifft auch elektronische Rechnungen.

**Dauerhaft:** In der Wirtschaft gibt es zwar aus handels- und steuerrechtlicher Sicht keine längeren Aufbewahrungsfristen über 10 Jahre hinaus, doch ist es allgemein üblich, [Gesellschafterverträge](https://de.wikipedia.org/wiki/Gesellschaftervertrag), Grundstücksunterlagen, Baupläne, [Patente](https://de.wikipedia.org/wiki/Patent), Gerichtsurteile oder [Personalakten](https://de.wikipedia.org/wiki/Personalakte) ebenfalls dauerhaft aufzubewahren.

1. Analog zu https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/\_content/m/m06/m06122.html [↑](#footnote-ref-1)
2. Zu den Vorgaben, was gemeldet werden soll, s. Anhang. [↑](#footnote-ref-2)
3. Zu den Vorgaben, was gemeldet werden soll, s. Anhang. [↑](#footnote-ref-3)
4. Diese sind Teil eines ITIL konformen Service Managements. [↑](#footnote-ref-4)
5. <https://de.wikipedia.org/wiki/Aufbewahrungsfrist>  
   https://www.hk24.de/produktmarken/beratung-service/recht\_und\_steuern/steuerrecht/abgabenordnung/aufbewahrungsfristen/1157174 [↑](#footnote-ref-5)