|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Sicherheitsrichtlinie "Cloud-Nutzung"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeitoffen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300016 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "Cloud-Nutzung" | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version  | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc79386273)

[Dokumentenhistorie 3](#_Toc79386274)

[Inhaltsverzeichnis 4](#_Toc79386275)

[Allgemeine Festlegungen 5](#_Toc79386276)

[Ziel / Zweck 5](#_Toc79386277)

[Geltungsbereich 5](#_Toc79386278)

[Zuständigkeiten 6](#_Toc79386279)

[Genehmigungs- und Änderungsverfahren 6](#_Toc79386280)

[Aufbau des Dokuments 6](#_Toc79386281)

[Sicherheitsrichtlinie „Outsourcing für Dienstleister" 7](#_Toc79386282)

[Basismaßnahmen 7](#_Toc79386283)

[Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben (OPS.2.1.A1) 7](#_Toc79386284)

[Standardmaßnahmen 7](#_Toc79386285)

[Rechtzeitige Beteiligung der Personalvertretung (OPS.2.1.A2) 7](#_Toc79386286)

[Auswahl eines geeigneten Outsourcing-Dienstleisters (OPS.2.1.A3) 7](#_Toc79386287)

[Vertragsgestaltung mit dem Outsourcing-Dienstleister (OPS.2.1.A4) 7](#_Toc79386288)

[Festlegung einer Strategie zum Outsourcing (OPS.2.1.A5) 7](#_Toc79386289)

[Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben (OPS.2.1.A6) 8](#_Toc79386290)

[Festlegung der möglichen Kommunikationspartner (OPS.2.1.A7) 8](#_Toc79386291)

[Regelungen für den Einsatz des Personals des Outsourcing-Dienstleiters (OPS.2.1.A8) 8](#_Toc79386292)

[Vereinbarung über die Anbindung an Netze der Outsourcing-Partner (OPS.2.1.A9) 8](#_Toc79386293)

[Vereinbarung über Datenaustausch zwischen den Outsourcing-Partnern (OPS.2.1.A10) 9](#_Toc79386294)

[Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb (OPS.2.1.A11) 9](#_Toc79386295)

[Änderungsmanagement (OPS.2.1.A12) 9](#_Toc79386296)

[Sichere Migration bei Outsourcing-Vorhaben (OPS.2.1.A13) 10](#_Toc79386297)

[Notfallvorsorge beim Outsourcing (OPS.2.1.A14) 10](#_Toc79386298)

[Geordnete Beendigung eines Outsourcing-Verhältnisses (OPS.2.1.A15) 10](#_Toc79386299)

[Maßnahmen bei erhöhtem Schutzbedarf 10](#_Toc79386300)

[Sicherheitsüberprüfung der Mitarbeiter des Outsourcing-Dienstleisters (OPS.2.1.A16 - CA) 11](#_Toc79386301)

# Allgemeine Festlegungen

## Ziel / Zweck

Beim Outsourcing lagert die <Institution> Geschäftsprozesse und Dienstleistungen ganz oder teilweise zu externen Dienstleistern (Outsourcing-Partnern) aus. Outsourcing kann die Nutzung und den Betrieb von Hard- und Software betreffen, wobei die Leistung in den Räumlichkeiten der <Institution> oder in einer externen Räumlichkeit des Dienstleisters erbracht werden kann. Typische Beispiele sind der Betrieb eines Rechenzentrums, einer Infrastruktur as a Service (IaaS), einer Plattform as a Service (PaaS), von Software as a Service (SaaS), von Anwendungen oder einer Webseite.

Unabhängig davon, was ausgelagert wird, bindet jede Auslagerung die <Institution> an den externen Dienstleister und dessen Dienstleistungsquantität sowie -qualität. Dieses Verhältnis ist insbesondere für die <Institution> nicht nur mit Chancen, sondern auch mit Risiken verbunden. Dazu gehören eine starke Abhängigkeit, der Verlust von eigenem Wissen sowie von Kontroll- und Steuerungsmöglichkeiten. Informationssicherheitsaspekte müssen daher während des kompletten Lebenszyklus einer Auslagerung angemessen berücksichtigt werden.

Ziel dieser Sicherheitsrichtlinie ist es, auf Basis der Vorgaben des BSI Bausteines OPS.2.1 "Outsourcing für Kunden" sicherzustellen, dass alle Sicherheitsziele der <Institution> auch nach der Auslagerung von Geschäftsprozessen oder Dienstleistungen an einen Dienstleister erfüllt werden. Das vereinbarte Sicherheitsniveau soll trotz Outsourcing dauerhaft aufrechterhalten bzw. verbessert werden. Durch das Outsourcing dürfen keine unkontrollierbaren Risiken für die <Institution> hinsichtlich der Informationssicherheit, dem Datenschutz und dem Notfallmanagement entstehen. Den Schwerpunkt dieser Sicherheitsrichtlinie bilden Anforderungen, die im Rahmen jeder Phase eines Outsourcing-Vorhabens beachtet bzw. erfüllt werden sollten.

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Das Dokument „Sicherheitsrichtlinie Outsourcing für Dienstleister“ wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

* Kapitel Basismaßnahmen: Beschreibung der Kernmaßnahmen, die für das Anforderungsmanagement zwingend erforderlich sind.
* Kapitel Standardmaßnahmen: Definition von Maßnahmen zur Erreichung eines vollumfänglichen Standardabsicherungsschutzniveaus für einen Schutzbedarf von „Normal“ in den Informationssicherheitsschutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.
* Kapitel Maßnahmen bei erhöhtem Schutzbedarf: Erläuterung von Maßnahmen die einen erhöhten Schutzbedarf (Schutzbedarfe „Hoch“, „Sehr hoch“) gewährleisten. Der Einsatz ist je Anwendungsfall im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen.

# Sicherheitsrichtlinie „Outsourcing für Dienstleister"

## Basismaßnahmen

Die nachfolgenden Basismaßnahmen sind vorrangig zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

### Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben (OPS.2.1.A1)

Alle Sicherheitsanforderungen für ein Outsourcing-Vorhaben müssen auf Basis der übergreifenden Strategie der <Institution> festgelegt sein. Beide Outsourcing-Parteien müssen sich vertraglich dazu verpflichten, den IT-Grundschutz oder ein vergleichbares Schutzniveau einzuhalten. Alle Schnittstellen zwischen dem Outsourcing-Dienstleister und der <Institution> sind zu identifizieren und entsprechende Sicherheitsanforderungen zu definieren. In den Sicherheitsanforderungen ist festzulegen, welche Berechtigungen wie Zutritts-, Zugangs- und Zugriffsrechte sich jeweils gegenseitig eingerichtet werden.

## Standardmaßnahmen

Gemeinsam mit den Basismaßnahmen sind die folgenden Standardmaßnahmen zum Erzielen eines normalen Schutzbedarfs zu betrachten und sollten grundsätzlich umgesetzt werden.

### Rechtzeitige Beteiligung der Personalvertretung (OPS.2.1.A2)

Die Personalvertretung der <Institution> sollte rechtzeitig über ein Outsourcing-Vorhaben seitens der <Institution> informiert werden. Idealerweise wird die Personalvertretung bereits in der Angebotsphase mit beteiligt. Je nach Outsourcing-Vorhaben sollten die gesetzlichen Mitwirkungsrechte beachtet werden.

### Auswahl eines geeigneten Outsourcing-Dienstleisters (OPS.2.1.A3)

Für die Auswahl des Outsourcing-Dienstleisters sollte ein Anforderungsprofil mit den Sicherheitsanforderungen an das Outsourcing-Vorhaben erstellt werden. Außerdem sollten Bewertungskriterien für den Outsourcing-Dienstleister und dessen Personal vorliegen. Diese sollten auf dem Anforderungsprofil basieren.

### Vertragsgestaltung mit dem Outsourcing-Dienstleister (OPS.2.1.A4)

Alle Aspekte des Outsourcing-Vorhabens sollten mit dem Outsourcing-Dienstleister schriftlich geregelt sein. Außerdem sind mit dem Outsourcing-Dienstleister alle Rollen und Mitwirkungspflichten zur Erstellung, Prüfung und Änderung des Sicherheitskonzepts zu regeln. Die Rechte und Pflichten der Vertragsparteien sind schriftlich zu regeln. Um die Anforderungen regelmäßig überprüfen zu können, muss der Outsourcing-Dienstleister der <Institution> Audits ermöglichen.

### Festlegung einer Strategie zum Outsourcing (OPS.2.1.A5)

Es sollte eine Strategie zum Outsourcing festgelegt werden. Diese Strategie sollte neben den wirtschaftlichen, technischen, organisatorischen und rechtlichen Rahmenbedingungen auch die relevanten Aspekte für Informationssicherheit, dem Datenschutz und das Notfallmanagement berücksichtigen. Es sollte definiert werden, welche Geschäftsprozesse, Aufgaben oder Anwendungen generell für ein Outsourcing in Frage kommen. Die <Institution> sollte ausreichende Fähigkeiten, Kompetenzen und Ressourcen bei sich behalten, um die Anforderungen an die Informationssicherheit bei jedem Outsourcing-Vorhaben selbst bestimmen und kontrollieren zu können. In der Strategie zum Outsourcing sollten die Ziele, Chancen und Risiken des Outsourcing-Vorhabens beschrieben werden.

### Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben (OPS.2.1.A6)

Die <Institution> erstellt für jedes Outsourcing-Vorhaben ein Sicherheitskonzept basierend auf den relevanten Sicherheitsanforderungen. Ebenso sollte jeder Outsourcing-Dienstleister ein individuelles Sicherheitskonzept für das jeweilige Outsourcing-Vorhaben vorlegen. Beide Sicherheitskonzepte sollten miteinander abgestimmt werden. Das Sicherheitskonzept des Outsourcing-Dienstleisters und dessen Umsetzung sollten zu einem gesamten Sicherheitskonzept zusammengeführt bzw. mittels GAP-Analyse Abweichungen dargestellt werden. Die <Institution> oder unabhängige Dritte sollten regelmäßig überprüfen und verifizieren, ob die Ergebnisse aus dem Sicherheitskonzept noch gültig sind.

### Festlegung der möglichen Kommunikationspartner (OPS.2.1.A7)

Es ist festzulegen, welche internen und externen Kommunikationspartner welche Informationen über das jeweilige Outsourcing-Projekt übermitteln und erhalten dürfen. Es sollte ein Prozess etabliert werden, mit dem die Funktion der Kommunikationspartner auf beiden Seiten geprüft wird. Die zulässigen Kommunikationspartner mit den jeweiligen Berechtigungen sind immer aktuell zu dokumentieren.

### Regelungen für den Einsatz des Personals des Outsourcing-Dienstleiters (OPS.2.1.A8)

Die Mitarbeiter des Outsourcing-Dienstleisters sollten schriftlich dazu verpflichtet werden, einschlägige Gesetze, Vorschriften sowie die internen Vorgaben der <Institution> einzuhalten. Die Mitarbeiter des Outsourcing-Dienstleisters sind geregelt in ihre Aufgaben eingewiesen und über bestehende Regelungen zur Informationssicherheit zu unterrichten. Für die Mitarbeiter des Outsourcing-Dienstleisters sollten Vertretungsregelungen existieren. Es sollte ein Verfahren festgelegt werden, das klärt, wie das Auftragsverhältnis mit den Mitarbeitern des Outsourcing-Dienstleisters beendet wird. Fremdpersonal des Outsourcing-Dienstleisters, das kurzfristig oder nur einmal eingesetzt wird, sollte wie ein Besucher seitens der <Institution> behandelt werden.

### Vereinbarung über die Anbindung an Netze der Outsourcing-Partner (OPS.2.1.A9)

Bevor die Infrastrukturen der <Institution> an die Infrastrukturen des Outsourcing-Dienstleisters angebunden werden, sind alle sicherheitsrelevanten Aspekte in einer Vereinbarung schriftlich zu regeln. In der Vereinbarung ist zu definieren, auf welche Infrastrukturbereiche und -dienste der Outsourcing-Dienstleister bei der <Institution> zugreifen darf. Die betroffenen Bereiche sollten geeignet voneinander getrennt werden. Es sollte geprüft und dokumentiert werden, dass die Vereinbarungen für die Anbindung bzw. Einbindung eingehalten werden. Auf beiden Seiten sind Ansprechpartner für organisatorische und technische Fragen zu benennen. Das geforderte Sicherheitsniveau sollte nachweislich beim Outsourcing-Dienstleister eingefordert und geprüft werden, bevor die Netzanbindung zum Outsourcing-Dienstleister aktiviert wird. Gibt es Sicherheitsprobleme auf einer der beiden Seiten, sollte festgelegt sein, wer darüber zu informieren ist und welche Eskalationsschritte einzuleiten sind.

### Vereinbarung über Datenaustausch zwischen den Outsourcing-Partnern (OPS.2.1.A10)

Für den regelmäßigen Datenaustausch mit festen Kommunikationspartnern sollten die erforderlichen Sicherheitsmaßnahmen vereinbart werden. Außerdem sollten Datenformate und Vorgehensweisen zum sicheren Datenaustausch festgelegt werden. Sowohl für organisatorische als auch technische Probleme sind Ansprechpartner anzugeben. Auch für sicherheitsrelevante Ereignisse beim Datenaustausch mit Dritten sind Ansprechpartner zu benennen. Beim Datenaustausch mit Dritten sind Verfügbarkeiten und Reaktionszeiten zu vereinbaren. Es sollte festgelegt werden, welche ausgetauschten Daten zu welchen Zwecken genutzt werden dürfen.

### Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb (OPS.2.1.A11)

Es sollte ein Betriebskonzept für das Outsourcing-Vorhaben erstellt werden, das auch die Sicherheitsaspekte (Informationssicherheit, Datenschutz und Notfallmanagement) berücksichtigt. Die Sicherheitskonzepte der Outsourcing-Partner sollten regelmäßig daraufhin überprüft werden, ob sie aktuell und zueinander konsistent sind. Der Status der vereinbarten Sicherheitsmaßnahmen sollte regelmäßig kontrolliert werden. Zwischen den Outsourcing-Partnern sollte regelmäßig kommuniziert werden. Vorschläge zu Änderungen und Verbesserungen sollten regelmäßig besprochen und abgestimmt werden.

Die Outsourcing-Partner sollten regelmäßig gemeinsame Übungen und Tests durchführen, um das Sicherheitsniveau aufrechtzuerhalten. Informationen über Sicherheitsrisiken und wie damit umgegangen wird, sollten regelmäßig zwischen den Outsourcing-Partnern ausgetauscht werden. Es sollte ein Prozess festgelegt werden, der den Informationsfluss bei Sicherheitsvorfällen sicherstellt, welche die jeweiligen Vertragspartner betreffen.

### Änderungsmanagement (OPS.2.1.A12)

Die <Institution> sollten über größere Änderungen rechtzeitig vorab informiert werden. Eine Dokumentation aller wesentlichen Änderungen bezüglich Planung, Test, Genehmigung und Dokumentation sollte von der <Institution> regelmäßig eingefordert werden. Bevor Änderungen durchgeführt werden, sollten gemeinsam mit dem Outsourcing-Dienstleister Rückfall-Lösungen erarbeitet werden.

### Sichere Migration bei Outsourcing-Vorhaben (OPS.2.1.A13)

Für die Migrationsphase sollte ein Team aus qualifizierten Mitarbeitern zusammen mit dem Informationssicherheitsmanagementteam der <Institution> und des Outsourcing-Dienstleisters eingerichtet werden. Es sollte für die Migrationsphase ein vorläufiges Sicherheitskonzept erstellt werden, in dem auch die Test- und Einführungsphase betrachtet wird. Außerdem sollte sichergestellt sein, dass produktive Daten in der Migrationsphase nicht ungeschützt als Testdaten verwendet werden. Alle Änderungen sollten dokumentiert werden. Nach Abschluss der Migration sollte das Sicherheitskonzept aktualisiert werden. Es sollte sichergestellt sein, dass alle Ausnahmeregelungen am Ende der Migrationsphase aufgehoben werden. Bei Änderungen in der Migrationsphase sollte geprüft werden, inwieweit die vertraglichen Grundlagen angepasst werden müssen.

### Notfallvorsorge beim Outsourcing (OPS.2.1.A14)

Es sollte ein Notfallvorsorgekonzept existieren, das die Komponenten bei der <Institution>, beim Outsourcing-Dienstleister sowie die zugehörigen Schnittstellen und Kommunikationswege umfasst. Im Notfallvorsorgekonzept zum Outsourcing sollten die Zuständigkeiten, Ansprechpartner und Abläufe zwischen der <Institution> und dem Outsourcing-Dienstleister geregelt sein. Die <Institution> sollte kontrollieren, ob der Outsourcing-Dienstleister die Notfallmaßnahmen umsetzt. Es sollten dazu gemeinsame Notfallübungen von der <Institution> und Outsourcing-Dienstleister durchgeführt werden.

###  Geordnete Beendigung eines Outsourcing-Verhältnisses (OPS.2.1.A15)

Der Vertrag mit dem Outsourcing-Dienstleister sollte alle Aspekte zur Beendigung des Dienstleistungsverhältnisses regeln, sowohl für eine geplante als auch für eine ungeplante Beendigung des Vertrags. Die Geschäftstätigkeit der <Institution> sollte nicht beeinträchtigt werden, wenn das Dienstleistungsverhältnis mit dem Outsourcing-Dienstleister beendet wird.

Die <Institution> sollte alle Informationen und Daten nach der Beendigung zurückerhalten. Der Outsourcing-Dienstleister muss alle Datenbestände der <Institution> nach erfolgter Rückgabe innerhalb von 30 Tagen sicher löschen.

## Maßnahmen bei erhöhtem Schutzbedarf

Gemeinsam mit den Basismaßnahmen und den Standardmaßnahmen sind zum Erzielen eines erhöhten Schutzbedarfs die hier aufgeführten Maßnahmen zu betrachten und sollten grundsätzlich umgesetzt werden. Ist dies aus wirtschaftlichen bzw. organisatorischen Gründen nicht möglich, so ist dies mit dem Sicherheitsmanagement zur weiteren Begegnung von Risiken für die Infrastruktur der <Institution> zu begründen und abzustimmen. Im Folgenden werden die Maßnahmen bei erhöhtem Schutzbedarf aufgeführt. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

### Sicherheitsüberprüfung der Mitarbeiter des Outsourcing-Dienstleisters (OPS.2.1.A16 - CA)

Mit externen Outsourcing-Dienstleistern sollte seitens der <Institution> vertraglich vereinbart werden, dass die Vertrauenswürdigkeit des eingesetzten Personals geeignet überprüft wird. Dazu sollten gemeinsam Kriterien festgelegt werden.