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

Sicherheitsrichtlinie "Outsourcing für Kunden"

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 | ISMS300017 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "Outsourcing für Kunden" | [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](#_Toc79430951)

[Dokumentenhistorie 3](#_Toc79430952)

[Inhaltsverzeichnis 4](#_Toc79430953)

[Allgemeine Festlegungen 5](#_Toc79430954)

[Ziel / Zweck 5](#_Toc79430955)

[Geltungsbereich 5](#_Toc79430956)

[Zuständigkeiten 5](#_Toc79430957)

[Genehmigungs- und Änderungsverfahren 6](#_Toc79430958)

[Aufbau des Dokuments 6](#_Toc79430959)

[Sicherheitsrichtlinie „Outsourcing für Kunden" 7](#_Toc79430960)

[Basismaßnahmen 7](#_Toc79430961)

[Erstellung eines Grobkonzeptes für die Outsourcing-Dienstleistung (OPS.3.1.A1) 7](#_Toc79430962)

[Standardmaßnahmen 7](#_Toc79430963)

[Vertragsgestaltung mit den Outsourcing-Kunden (OPS.3.1.A2) 7](#_Toc79430964)

[Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben (OPS.3.1.A3) 7](#_Toc79430965)

[Festlegung der möglichen Kommunikationspartner (OPS.3.1.A4) 7](#_Toc79430966)

[Regelungen für den Einsatz des Personals des Outsourcing-Dienstleisters (OPS.3.1.A5) 8](#_Toc79430967)

[Regelungen für den Einsatz von Fremdpersonal (OPS.3.1.A6) 8](#_Toc79430968)

[Erstellung eines Mandantenkonzeptes durch die <Institution> (OPS.3.1.A7) 8](#_Toc79430969)

[Vereinbarung über die Anbindung an Netze der Kunden der <Institution> (OPS.3.1.A8) 8](#_Toc79430970)

[Vereinbarung über Datenaustausch zwischen der <Institution> und dem Kunden (OPS.3.1.A9) 9](#_Toc79430971)

[Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb (OPS.3.1.A10) 9](#_Toc79430972)

[Zutritts-, Zugangs- und Zugriffskontrolle (OPS.3.1.A11) 9](#_Toc79430973)

[Änderungsmanagement (OPS.3.1.A12) 9](#_Toc79430974)

[Sichere Migration bei Outsourcing-Vorhaben (OPS.3.1.A13) 10](#_Toc79430975)

[Notfallvorsorge beim Outsourcing (OPS.3.1.A14) 10](#_Toc79430976)

[Geordnete Beendigung eines Outsourcing-Verhältnisses (OPS.3.1.A15) 10](#_Toc79430977)

[Maßnahmen bei erhöhtem Schutzbedarf 10](#_Toc79430978)

[Sicherheitsüberprüfung von Mitarbeitenden (OPS.3.1.A16 - CA) 11](#_Toc79430979)

# Allgemeine Festlegungen

## Ziel / Zweck

Beim Outsourcing für unsere Kunden übernimmt die <Institution> als Outsourcing-Dienstleister Geschäftsprozesse und Dienstleistungen ganz oder teilweise von auslagernden Outsourcing-Kunden. Unabhängig davon, welche Dienstleistungen übernommen werden, ist eine enge Bindung zwischen der <Institution> und ihren Kunden notwendig. Durch diese enge Bindung bleibt die <Institution> als Dienstleister nicht von den Risiken der Outsourcing-Beziehung verschont. Zudem muss die <Institution> die vom Kunden festgelegten risikomindernden Sicherheitsanforderungen umsetzen. Denn es liegt ebenfalls im Interesse der <Institution>, die vereinbarte Leistung zu erbringen und das vereinbarte Sicherheitsniveau einzuhalten. Sollten die an die <Institution> gestellten Anforderungen nicht erfüllt werden, drohen eventuell hohe Vertragsstrafen und gegebenenfalls weitere juristische Folgen. Die nicht Erfüllung von vertraglichen Anforderungen könnte nicht nur finanzielle Auswirkungen haben, sondern auch die Reputation der <Institution> nachhaltig schädigen.

Dieses Dokument beschreibt die Anforderungen für die <Institution>, damit die <Institution> das Sicherheitsniveau des auslagernden Kunden erfüllen bzw. für den Kunden unkontrollierbare Risiken vermeiden kann, die sich aus der Geschäftsbeziehung ergeben. Den Schwerpunkt dieser Sicherheitsrichtlinie bilden Anforderungen, die sich mit der Planung, Umsetzung, Kontrolle und Steuerung von Informationssicherheitsaspekten im Rahmen eines Outsourcings aus Sicht der <Institution> beschäftigen. Bei der Definition der Anforderungen wurden die Vorgaben aus dem BSI Baustein 3.1 "Outsourcing für Dienstleister" beachtet.

## 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 Kunden“ 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 Kunden"

## Basismaßnahmen

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

### Erstellung eines Grobkonzeptes für die Outsourcing-Dienstleistung (OPS.3.1.A1)

Für jede Outsourcing-Dienstleistung der <Institution> wird ein Grobkonzept erstellt. Alle Rahmenbedingungen des Outsourcings sowie grundsätzliche Regelungen zum Sicherheitsniveau und den Sicherheitsanforderungen des Kunden der <Institution> werden darin erfasst.

## Standardmaßnahmen

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

### Vertragsgestaltung mit den Outsourcing-Kunden (OPS.3.1.A2)

Die <Institution> stellt sicher, dass alle Kundenverträge schriftlich geregelt werden. Alle Verantwortlichkeiten und Mitwirkungspflichten zur Erstellung, Prüfung und Änderung im Rahmen der vereinbarten Dienstleistung werden innerhalb des Vertrags erfasst.

### Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben (OPS.3.1.A3)

Die <Institution> bewertet für jedes Outsourcing-Vorhaben basierend auf den kundenspezifischen Sicherheitsanforderungen den Impact auf die Sicherheit der von der <Institution> betriebenen Lösungen und deren Infrastrukturen sowie auf potenzielle Seiteneffekte zu anderen Verfahren unabhängig ob Kunden-Services oder von der <Institution> selbst konsumierte Services. Die <Institution> bietet ihren Kunden bei Bedarf Unterstützung bei der Benennung der gemeinsamen Sicherheitsziele und Klassifikation für alle schutzbedürftigen Informationen an.

Das Sicherheitskonzept wird nach Finalisierung/Freigabe in die etablierten Dokumentenlenkungsprozesse aufgenommen.

### Festlegung der möglichen Kommunikationspartner (OPS.3.1.A4)

Für die interne und externe Kommunikation von Outsourcing-Projekten wird die <Institution> festlegen, welchen Kommunikationspartnern welche Informationen zugänglich gemacht werden dürfen. In diesem Zusammenhang wird durch die <Institution> ein Prozess etabliert, der die Funktionen der internen und externen Kommunikationspartner überprüft. Dieser Prozess wird ferner sicherstellen, dass die entsprechenden Kommunikationspartner und ihre Berechtigungen jederzeit aktuell dokumentiert sind. Bei Änderungen werden die Berechtigungen angepasst.

### Regelungen für den Einsatz des Personals des Outsourcing-Dienstleisters (OPS.3.1.A5)

Mitarbeitende der <Institution> werden geregelt in ihre Aufgaben eingewiesen und über bestehende Regelungen zur Informationssicherheit des Kunden (Outsourcing-Kunden) unterrichtet. Soweit es gefordert ist, werden die Mitarbeitenden der <Institution> nach Vorgaben des Kunden überprüft. Die Mitarbeitenden der <Institution> werden schriftlich auf die Einhaltung der einschlägigen Gesetze, Vorschriften, Vertraulichkeitsvereinbarungen und internen Regelungen verpflichtet. Es gibt Vertretungsregelungen in allen Bereichen.

### Regelungen für den Einsatz von Fremdpersonal (OPS.3.1.A6)

Werden externe Mitarbeitende von der <Institution> in Schlüsselpositionen eingesetzt, wird der Kunde der <Institution> darüber informiert. Das externe Personal wird schriftlich auf die Einhaltung der einschlägigen Gesetze, Vorschriften und internen Regelungen der <Institution> verpflichtet. Sie werden in ihre Aufgaben und vor allem in die Sicherheitsvorgaben eingewiesen. Kurzfristig oder einmalig eingesetztes Fremdpersonal wird wie ein Besucher behandelt. Die Sicherheitsvorgaben des Kunden der <Institution> sind jedoch auch bei Fremdpersonal zu berücksichtigen. Sofern ein Einsatz externer Mitarbeitende in sicherheitsrelevanten Bereichen/Projekten bzw. für sicherheitsrelevante Themen beabsichtigt wird, müssen diese Mitarbeitende entsprechende Sicherheitsnachweise vorlegen.

### Erstellung eines Mandantenkonzeptes durch die <Institution> (OPS.3.1.A7)

Durch ein Mandantenkonzept wird sichergestellt, dass Anwendungs- und Datenkontexte verschiedener Kunden der <Institution> sauber und sicher getrennt sind. Das Mandantenkonzept wird durch die <Institution> erstellt und dem Kunden der <Institution> zur Verfügung gestellt. Dieses bietet für den Schutzbedarf des Outsourcing-Kunden angemessene Sicherheit. Die benötigten Mechanismen zur Mandantentrennung werden durch die <Institution> ausreichend umgesetzt.

### Vereinbarung über die Anbindung an Netze der Kunden der <Institution> (OPS.3.1.A8)

Insofern sich durch das Outsourcing-Vorhaben technische Schnittstellen zwischen den Vertragsparteien ergeben, stellt die <Institution> sicher, dass alle sicherheitsrelevanten Aspekte bezüglich der Netzanbindung schriftlich festgehalten werden. Diese Vereinbarung definiert dabei, auf welche Dienste und Bereiche der <Institution> beim Kunden zu gegriffen werden darf. Im Rahmen der Vereinbarung werden sowohl bei der <Institution> als auch beim Kunden verantwortliche Ansprechpartner für die organisatorischen und technischen Aspekte benannt. Für jedes Vorhaben (Verfahren) werden für jede Vertragspartei außerdem Ansprechpartner und Eskalationswege definiert, die im Falle von Sicherheitsvorfällen bzw. Notfällen zu berücksichtigen sind. Bevor eine Netzanbindung an den Kunden erfolgt, wird das Schutzniveau nachweißlich durch die <Institution> eingefordert und überprüft.

### Vereinbarung über Datenaustausch zwischen der <Institution> und dem Kunden (OPS.3.1.A9)

Werden durch das Outsourcing-Vorhaben Daten über feste Kommunikationspartner ausgetauscht werden, vereinbart und dokumentiert die <Institution> mit dem Kunden (Outsourcing-Kunden) entsprechende Sicherheitsmaßnahmen. In diesem Zusammenhang wird ebenso festgelegt, welche Daten zu welchem Zweck ausgetauscht werden. Die Vorgaben der Sicherheitsvereinbarung berücksichtigen dabei zu benutzende Dateiformate und Vorgehensweisen zum sicheren Austausch, Ansprechpartner für organisatorische und technische Probleme sowie Ansprechpartner, die unter anderem im Falle von Sicherheitsvorfällen beim Datenaustausch agieren. Die <Institution> berücksichtigt zu gewährleistende Verfügbarkeitsaspekte und Reaktionszeiten innerhalb der Sicherheitsvorgaben. Die geeignete Auftragsdatenverarbeitung gemäß den geltenden Datenschutzgesetzen wird in den Dienstleistungsverhältnissen gewährleistet.

### Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb (OPS.3.1.A10)

Für jedes Outsourcing-Vorhaben ist vom Kunden der <Institution> ein Konzept, welches alle relevanten Sicherheitsaspekte berücksichtigt, zu definieren. Die <Institution> gewährleistet, dass beide Vertragsparteien ihre Sicherheitskonzepte regelmäßig auf Aktualität und gegenseitige Konsistenz überprüfen. Die Umsetzung und der Status vereinbarter Sicherheitsmaßnahmen werden regelmäßig durch die <Institution> kontrolliert. Im Rahmen einer kontinuierlichen Verbesserung findet eine regelmäßige Kommunikation und Abstimmung von Änderungen zwischen den Vertragsparteien statt.

Es sollten regelmäßige gemeinsame Übungen und Tests zur Aufrechterhaltung des Sicherheitsniveaus durchgeführt werden. Die Vertragsparteien tauschen sich regelmäßig sowie anlassbezogen bzgl. des Umgangs mit Sicherheitsrisiken aus. Über einen geregelten Prozess wird gewährleistet, dass ein angemessener Informationsfluss zu Sicherheitsvorfällen zwischen den Vertragsparteien vorliegt.

### Zutritts-, Zugangs- und Zugriffskontrolle (OPS.3.1.A11)

Sowohl für die Mitarbeitenden von der <Institution> und für die Kunden der <Institution> sind Zutritts-, Zugangs- und Zugriffsberechtigungen zu regeln. Ebenfalls sind die Berechtigungen für interne Revisoren, externe Auditoren und andere Prüfer festzuhalten. Es werden nur die für die Ausführung der Aufgaben notwendigen Rechte nach dem Minimalprinzip vergeben. Die Vergabe, Verwaltung sowie Entzug von Berechtigungen folgen einem geregelten Prozess.

### Änderungsmanagement (OPS.3.1.A12)

Innerhalb der <Institution> existieren Richtlinien für die Durchführung von Änderungen an IT-Komponenten, Software oder Konfigurationsdaten. Es ist geregelt, dass bei der Durchführung von Änderungen auch Sicherheitsaspekte berücksichtigt werden. Alle Änderungen werden geplant, getestet, genehmigt und dokumentiert. Art und Umfang der Dokumentationen werden mit den Kunden der <Institution> abgestimmt. Ebenfalls sind Rückfall-Lösungen zu erarbeiten. Bei größeren, sicherheitsrelevanten Änderungen wird das Informationssicherheitsmanagement des Kunden der <Institution> schon im Vorfeld beteiligt.

### Sichere Migration bei Outsourcing-Vorhaben (OPS.3.1.A13)

Für die Migrationsphase wird ein Informationssicherheitsmanagementteam bestehend aus qualifizierten Mitarbeitenden beider Vertragsparteien zusammengestellt. Dieses ist dafür verantwortlich ein Sicherheitskonzept einzuführen. Nach dem Abschluss der Migration wird durch das Informationssicherheitsmanagementteam sichergestellt, dass das vorläufige Sicherheitskonzept aktualisiert wird und jegliche Ausnahmeregelungen aufgehoben werden. Bei Änderungen in der Migrationsphase wird geprüft, inwieweit ein Anpassungsbedarf an den vertraglichen Grundlagen und bestehenden Dokumenten besteht.

### Notfallvorsorge beim Outsourcing (OPS.3.1.A14)

Für jede Outsourcing-Dienstleistung wird ein Notfallvorsorgekonzept definiert. Diese umfassen jegliche Komponenten und Schnittstellen der <Institution> und den Kunden. Im Rahmen des Notfallvorsorgekonzepts werden die entsprechenden Zuständigkeiten, Ansprechpartner und Abläufe zwischen den Vertragsparteien festgehalten. Der <Institution> gewährleistet, dass die Umsetzung von festgelegten Notfallmaßnahmen angemessen, mittels Durchführung gemeinsamer Notfallübungen, kontrolliert werden.

### Geordnete Beendigung eines Outsourcing-Verhältnisses (OPS.3.1.A15)

Alle Aspekte im Rahmen der Beendigung des Dienstleistungsverhältnisses werden vertraglich erfasst. Somit stellt die <Institution> sicher, dass jede planmäßige und außerplanmäßige Beendigung des Outsourcing-Verhältnisses die Geschäftsfähigkeit der <Institution> sowie des Kunden nicht beeinträchtigt.

Über geregelte Vereinbarung wird sichergestellt, dass die <Institution> nach der Beendigung eines Dienstleistungsverhältnisses alle Informationen und Daten zurück an den Kunden übergibt und verbliebene Datenbestände sicher vernichtet. Dies wird im Umkehrschluss auch von beauftragten Dienstleistern gefordert. Sofern aus wirtschaftlichen Aspekten eine sichere Vernichtung von rein kundenspezifischen-Informationen nicht möglich ist, stellt die <Institution> sicher, dass diese Informationen im Rahmen der sicheren Löschung von Speichermedien mit vernichtet werden.

Alle Berechtigungen, die im Rahmen des Outsourcing-Projekts eingerichtet wurden, werden überprüft und, wenn erforderlich, gelöscht.

## 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 von Mitarbeitenden (OPS.3.1.A16 - CA)

Die <Institution> hält im Rahmen des Dienstleistungs-Vertrages fest, dass die Vertrauenswürdigkeit der Mitarbeitenden angemessen zu überprüfen ist. Die dafür zugrundeliegenden Bewertungskriterien werden durch die beiden Vertragsparteien festgelegt.