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

Standard "externe Dienstleistersteuerung"

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 Dokumentenvertraulichkeit  offen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS200007 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung (vergeben] |
| Name des Dokuments | Standard "externe Dienstleistersteuerung" | [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](#_Toc75469034)

[Dokumentenhistorie 3](#_Toc75469035)

[Inhaltsverzeichnis 4](#_Toc75469036)

[Allgemeine Festlegungen 5](#_Toc75469037)

[Ziel / Zweck 5](#_Toc75469038)

[Geltungsbereich 5](#_Toc75469039)

[Zuständigkeiten 6](#_Toc75469040)

[Genehmigungs- und Änderungsverfahren 6](#_Toc75469041)

[Standard Externe Dienstleistersteuerung 6](#_Toc75469042)

[Planung der Auslagerung 6](#_Toc75469043)

[Beteiligung von internen Stellen 6](#_Toc75469044)

[Dokumentation der Sicherheitsanforderungen 6](#_Toc75469045)

[Einsatz von Fremdpersonal 7](#_Toc75469046)

[Auswahl eines Dienstleisters 7](#_Toc75469047)

[Umsetzung der Auslagerung 8](#_Toc75469048)

[Vertragsgestaltung 8](#_Toc75469049)

[Festlegung der Kommunikationspartner 8](#_Toc75469050)

[Planung der Migration 9](#_Toc75469051)

[Definition der technischen und organisatorischen Anforderungen 9](#_Toc75469052)

[Durchführung von Änderungen 9](#_Toc75469053)

[Regelung der Dienstleistungsnutzung 9](#_Toc75469054)

[Betrieb der ausgelagerten Dienste 9](#_Toc75469055)

[Regelmäßige Abstimmungsrunden 9](#_Toc75469056)

[Regelmäßige Kontrolle der Service-Erbringung 10](#_Toc75469057)

[Durchführung von Audits beim Dienstleister 10](#_Toc75469058)

[Prüfung des Datenschutzkonzeptes des Dienstleisters 10](#_Toc75469059)

[Beendigung der Auslagerung 10](#_Toc75469060)

[Notfallvorsorge 10](#_Toc75469061)

[Prüfung der Notfallkonzepte des Dienstleisters 10](#_Toc75469062)

[Erstellung interner Notfallkonzepte 10](#_Toc75469063)

# Allgemeine Festlegungen

## Ziel / Zweck

Dieser Standard beschreibt die Auslagerung von Dienstleistungen und die Steuerung der Dienstleistungsverhältnisse. Dabei wird zwischen zwei Dienstleistungsvarianten unterschieden:

* Auslagerung nach individuellen Vorgaben:  
  Durch die expliziten Vorgaben von der <Institution> werden Dienstleistungen an einen externen Dienstleister ausgelagert. In diesem Fall ist die <Institution> sowohl für die Definition aller relevanten technischen, sicherheitsrelevanten und fachlichen Anforderungen verantwortlich als auch für die diesbezügliche Überprüfung sowie Einhaltung. Analog zu den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) wird dies als „Outsourcing“ bezeichnet.
* Auslagerung an bestehende Dienste:  
  Bei dieser Form der Auslagerung werden vorgefertigte Dienstleistungsangebote von externen Service-Anbietern (Dienstleistern) verwendet. Die angebotenen Services können nicht oder nur sehr eingeschränkt angepasst werden. Die <Institution> ist für die Prüfung der gebotenen Leistungen unter sicherheitstechnischer und fachlicher Sicht und für den Abgleich mit den eigenen Anforderungen verantwortlich. Analog zu den Vorgaben des BSI wird dies als Cloud-Nutzung beschrieben. In der Praxis wird zudem nach vier Bereitstellungsmodellen von Cloud-Diensten unterschieden:
  + Private-Cloud: Cloud-Infrastruktur, die ausschließlich von einer einzelnen <Institution> genutzt werden kann.
  + Community-Cloud: Cloud-Infrastruktur, die ausschließlich von einer konkreten Gemeinschaft genutzt werden kann, einschließlich mehrerer Institutionen innerhalb zuvor definierter Gruppen.
  + Public-Cloud: Cloud-Infrastruktur, die von der Öffentlichkeit frei genutzt werden kann.
  + Hybrid/Multi-Cloud: Cloud-Infrastruktur, die sich aus zwei oder mehreren speziellen Cloud-Infrastrukturen zusammensetzt.

Der Standard für die externe Dienstleistersteuerung umfasst insbesondere die Anforderungen je Lebenszyklus einer Auslagerung und die zu treffenden Maßnahmen.

## 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

Der Standard externe Dienstleistersteuerung 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>.

# Standard Externe Dienstleistersteuerung

## Planung der Auslagerung

### Beteiligung von internen Stellen

Bei jeder Auslagerung von Software, Hardware oder sonstigen Dienstleistungen ist rechtzeitig zu klären, welche internen Stellen, in welchem Umfang einzubinden sind. Es sind mindestens der <Datenschutzbeauftragte> und <Informationssicherheitsbeauftragter> von Anfang an mit einzubinden. Die bestehenden Vorgaben für Bestellungen und Beauftragungen sind einzuhalten.

### Dokumentation der Sicherheitsanforderungen

Alle definierten Sicherheitsanforderungen werden durch einen vorher festgelegten Fachverantwortlichen dokumentiert und mit dem <Informationssicherheitsbeauftragter> abgestimmt. Der Schutzbedarf der verarbeiteten Daten ist zu beachten.

Falls durch die Dienstleister nicht alle Sicherheitsanforderungen umgesetzt werden, sind die daraus resultierenden Risiken von den Fachverantwortlichen mit Unterstützung des <Informationssicherheitsbeauftragter> zu identifizieren und zu bewerten. Die Risiko Behandlungsmethoden oder Übernahmen müssen wirtschaftlich angemessen sein und sind zu dokumentieren.

Bei organisatorischen oder technischen Änderungen einer bestehenden Auslagerung sind die Sicherheitsanforderungen zu überprüfen und bei Bedarf anzupassen.

### Einsatz von Fremdpersonal

Sofern im Rahmen der beauftragten Dienstleistungen Mitarbeiter eines Dienstleisters über einen längeren Zeitraum in den Räumlichkeiten der <Institution> tätig werden, sind diese auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen zu verpflichten. Zu diesem Zweck sind Vertraulichkeitsvereinbarungen (non-disclosure agreements, NDA) auszufüllen und bei Notwendigkeit Sicherheitsüberprüfungen von einzelnen Mitarbeitern einzuholen.

Das Fremdpersonal wird angemessen in die betreuten Aufgaben, benötigten Anwendungen, hausinternen Regelungen und Vorschriften zur Informationssicherheit (ISMS-Dokumenten-Framework) eingewiesen.

Für alle relevanten externen Mitarbeitenden gibt es eine Vertretungsregelung, die vertraglich vereinbart wird, um einen etwaigen Ausfall zu kompensieren.

Bei der Beendigung des Auftragsverhältnisses hat eine geregelte Übergabe der Arbeitsergebnisse und der erhaltenen Unterlagen und Betriebsmittel zu erfolgen. Es sind außerdem sämtliche eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen beziehungsweise zu löschen. Außerdem wird der Ausscheidende explizit darauf hingewiesen, dass die Vorgaben der Vertraulichkeitsvereinbarung auch nach Beendigung der Tätigkeit bestehen bleiben.

Kurzfristig oder einmalig zum Einsatz kommendes Fremdpersonal ist wie ein Besucher zu behandeln.

## Auswahl eines Dienstleisters

Die Auswahl eines Dienstleisters erfolgt unter Einbeziehung der definierten Anforderungen nach den Vorgaben dieses Standards und den Vorgaben für Bestellungen und Beauftragungen in der <Institution>. Ergänzend zu diesem Standard sind bei der Auswahl eines Dienstleisters mindestens die folgenden Aspekte zu berücksichtigen:

* Der Schutzbedarf der zu erbringenden Dienstleistung beziehungsweise der bei der Dienstleistungserbringung verarbeiteten Informationen
* Die Vorgaben von ausländischem Recht hinsichtlich Informationsverarbeitung (insbesondere bei Datenschutz, Kryptographie, etc.), sofern relevant
* Vorhandene sicherheitsrelevante Zertifikate (z. B. ISO 27001 nativ oder auf der Basis von BSI IT-Grundschutz)
* Referenzen bezüglich ähnlicher Dienstleistungen

## Umsetzung der Auslagerung

### Vertragsgestaltung

Es sind grundsätzlich Dienstleister zu bevorzugen, die eine sichere Datenhaltung innerhalb Deutschlands, der Schweiz bzw. der EU gewährleisten und vertraglich zusichern. Denn der Datenschutz selbst mit seinen Regelungen und der Umgang mit personenbezogenen Daten (EU-DSGVO/BDSG-neu) sowie die Datenhaltung werden zunehmend existenziell.

Ausnahmen für die Datenhaltung und Datenverarbeitung sind unter Berücksichtigung der verarbeiteten Daten mit dem <Datenschutzbeauftragter> und <Informationssicherheitsbeauftragter> abzustimmen.

Der beauftragte Dienstleister ist darüber hinaus vertraglich zu folgendem zu verpflichten:

* Die Daten gemäß geltenden Gesetzen und Vorschriften zu verarbeiten
* Die relevanten Informationssicherheitsvorgaben der <Institution> einzuhalten
* Zu garantieren, dass die Sicherheitsprozesse und der sichere Systembetriebs dem Schutzbedarfs und mindestens den hier definierten Sicherheitsanforderungen entsprechend:
  + Sichere Abgrenzung bei gemeinsamer Nutzung von Cloud-Diensten mit anderen Institutionen (z. B. eine geeignete Mandantentrennung)
  + Festlegen der Anforderungen an die Kommunikation (z. B. Protokolle) und Verschlüsselung
  + die Anforderungen an das Berechtigungsmanagement abzustimmen
  + die Datensicherung entsprechend den Anforderungen umzusetzen
  + eine lesende Schnittstelle auf die Überwachung des Dienstes einzurichten und
  + sich an den Empfehlungen des BSI im Leitfaden Cloud ([Link#1](https://www.isaca.de/sites/default/files/broschuere_leitfaden_c5_0.pdf) und [Link#2](https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Anforderungskatalog/Anforderungskatalog_Cloud_Computing.html)) zu orientieren
* Zu garantieren, dass die Verfügbarkeitsanforderungen der bereitgestellten Dienste (Service Level Agreements) inklusive Incident-Handling und der Servicezeiten den vereinbarten Werten entsprechen
* Prozessschnittstellen zu den internen Betriebs- und Sicherheitsprozessen inklusive der Ansprechpartner und Stellvertreter festlegen
  + im Änderungsmanagement, im Risikomanagement beziehungsweis im (Security) Incident Management/Sicherheitsvorfallsmanagement
* Erstellung von Reports zur Qualität der erbrachten Dienstleistung
* Einen Sicherheitsbericht über Vorfälle, Updates und Angriffe liefern
* Unterauftragnehmer nur in Abstimmung mit der <Institution> einzusetzen und bei diesen die Vorgaben von der <Institution> verpflichtend einzuhalten und zu prüfen
* Ein Audit- bzw. Revisionsrecht, das auch bei Vorfällen greift, einzuräumen
* Bei der Beendigung des Vertrages die Migration zu unterstützen
* Eine vorzeitige Vertragsbeendigung in kritischen Fällen zu berücksichtigen

### Festlegung der Kommunikationspartner

Es sind für alle auszutauschenden Informationen die jeweiligen Kommunikationspartner oder IT-Systeme sowie die Art der Informationsübermittlung zu definieren. Mit dem Dienstleister muss geklärt werden, ob ein Datenaustausch mit Dritten erlaubt ist und wie dieser dann stattfinden darf.

### Planung der Migration

Sofern Daten zur Auslagerung übernommen werden, ist die Migration dieser Daten in einem Migrationskonzept zu dokumentieren. Die fachlichen Verantwortlichen müssen die korrekte Migration der Daten abnehmen und bestätigen.

### Definition der technischen und organisatorischen Anforderungen

Für jede Auslagerung ist zu definieren, ob zusätzliche technische Änderungen notwendig sind. Dies betrifft insbesondere die Bereitstellung von Schnittstellen, einer ausreichenden Netzanbindung sowie die Umsetzung der Administrationsaufgaben.

Alle technischen Anforderungen sind zu dokumentieren und es sind entsprechende Maßnahmen umzusetzen.

Eine Anbindung an die Netze Dritter darf nur in Abstimmung mit dem <Informationssicherheitsbeauftragter> erfolgen.

### Durchführung von Änderungen

Im Verfahren zur Durchführung von Änderungen sind alle relevanten Änderungen an zuständige Dienstleister zu übermitteln und sicher umzusetzen. Darüber hinaus wird durch dieses Verfahren auch sichergestellt, dass die Änderungen seitens der <Institution> nachgehalten, getestet und abgenommen werden.

### Regelung der Dienstleistungsnutzung

Sofern Daten zur Auslagerung übernommen werden, ist die Migration dieser Daten in einem Migrationskonzept zu dokumentieren. Die fachlichen Verantwortlichen müssen die korrekte Migration der Daten abnehmen und bestätigen.

Hinsichtlich jeder Auslagerung ist transparent zu regeln, wie diese Dienstleistung durch Mitarbeitende in Anspruch genommen werden darf (z. B. Zugriff auf die jeweilige Webanwendung, Abrufe von externen Mitarbeitenden).

Es ist zudem für jede Auslagerung zu prüfen, inwieweit Informationen zur sicheren Nutzung des Dienstes durch die Mitarbeitenden bereitzustellen sind.

## Betrieb der ausgelagerten Dienste

### Regelmäßige Abstimmungsrunden

Es werden mit dem Dienstleister regelmäßige Abstimmungsrunden vereinbart, in denen ein Austausch über den aktuellen Zustand des Dienstes und die zukünftigen Änderungen stattfindet.

### Regelmäßige Kontrolle der Service-Erbringung

Es findet eine regelmäßige Kontrolle der vertraglich vereinbarten Reports, Benutzermeldungen und Sicherheitsvorfälle statt, um mögliche Schwachstellen frühzeitig zu erkennen. Die Ergebnisse dieser Kontrollen sind schriftlich zu dokumentieren.

### Durchführung von Audits beim Dienstleister

In Abstimmung mit dem <Informationssicherheitsbeauftragter> sollen regelmäßige Audits beim Dienstleister durchgeführt werden. Dort sind insbesondere die Aktualität und Qualität der Sicherheitskonzepte des Dienstleisters sowie die Umsetzung der vereinbarten Maßnahmen zu beachten.

### Prüfung des Datenschutzkonzeptes des Dienstleisters

Das Datenschutzkonzept und die TOMs des Dienstleisters werden regelmäßig überprüft, ob diese für die geforderte Verfügbarkeit, Vertraulichkeit und Integrität angemessen sind.

## Beendigung der Auslagerung

Die folgenden Punkte sind mindestens zur Beendigung der Auslagerung vertraglich mit dem Dienstleister vereinbart und zu berücksichtigen:

* Eigentumsrechte an Hard- und Software
* Die Weiterverwendung der vom Dienstleister eingesetzten Tools, Prozeduren, Skripte, Batchprogramme
* Dokumentation der IT-Systeme, deren Komponenten, der Anwendungen und Arbeitsabläufe
* Bereitstellung der verarbeiteten Daten und Dokumente in einem geeigneten Format durch den Dienstleister
* Sichere und dokumentierte Löschung aller personenbezogenen Datenbestände beim Dienstleister nach Beauftragungsende
* Einweisung der Personen, die die Dienstleistung übernehmen
* Definition einer Übergangsfrist für die Migration der jeweiligen Dienstleistung, die Beantwortung von Fragen und weiterer Unterstützung

## Notfallvorsorge

### Prüfung der Notfallkonzepte des Dienstleisters

Die Notfallkonzepte des Dienstleisters werden regelmäßig überprüft, ob diese für die geforderte Verfügbarkeit angemessen sind.

### Erstellung interner Notfallkonzepte

In Abstimmung mit dem Notfallmanagement von der <Institution> wird geprüft, ob die Notfallkonzepte seitens des Dienstleisters erstellt werden müssen.

In diesem Zusammenhang wird auch geprüft, ob von den ausgelagerten Diensten zusätzliche interne Datensicherungen bei der <Institution> vorgehalten werden müssen.