|  |  |
| --- | --- |
| 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 Dokumentenvertraulichkeit  offen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300015 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments |  | [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](#_Toc79332388)

[Dokumentenhistorie 3](#_Toc79332389)

[Inhaltsverzeichnis 4](#_Toc79332390)

[Allgemeine Festlegungen 5](#_Toc79332391)

[Ziel / Zweck 5](#_Toc79332392)

[Geltungsbereich 5](#_Toc79332393)

[Zuständigkeiten 6](#_Toc79332394)

[Genehmigungs- und Änderungsverfahren 6](#_Toc79332395)

[Aufbau des Dokuments 6](#_Toc79332396)

[Sicherheitsrichtlinie „Cloud-Nutzung" 7](#_Toc79332397)

[Basismaßnahmen 7](#_Toc79332398)

[Erstellung einer Cloud-Nutzungs-Strategie (OPS.2.2.A1) 7](#_Toc79332399)

[Service-Definition für Cloud-Dienste durch den Anwender (OPS.2.2.A3) 8](#_Toc79332400)

[Festlegung von Verantwortungsbereichen und Schnittstellen (OPS.2.2.A4) 8](#_Toc79332401)

[Standardmaßnahmen 8](#_Toc79332402)

[Planung der sicheren Migration zu einem Cloud-Dienst (OPS.2.2.A5) 9](#_Toc79332403)

[Planung der sicheren Einbindung von Cloud-Diensten (OPS.2.2.A6) 9](#_Toc79332404)

[Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung (OPS.2.2.A7) 10](#_Toc79332405)

[Sorgfältige Auswahl eines Cloud-Diensteanbieters (OPS.2.2.A8) 10](#_Toc79332406)

[Vertragsgestaltung mit dem Cloud-Diensteanbieter (OPS.2.2.A9) 10](#_Toc79332407)

[Sichere Migration zu einem Cloud-Dienst (OPS.2.2.A10) 11](#_Toc79332408)

[Erstellung eines Notfallkonzeptes zu einem Cloud-Dienst (OPS.2.2.A11) 11](#_Toc79332409)

[Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb (OPS.2.2.A12) 12](#_Toc79332410)

[Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung (OPS.2.2.A13) 13](#_Toc79332411)

[Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses (OPS.2.2.A14) 13](#_Toc79332412)

[Maßnahmen bei erhöhtem Schutzbedarf 13](#_Toc79332413)

[Portabilität von Cloud-Diensten (OPS.2.2.A15 - A) 14](#_Toc79332414)

[Durchführung eigener Datensicherungen (OPS.2.2.A16 - IA) 14](#_Toc79332415)

[Einsatz von Verschlüsselung bei Cloud-Nutzung (OPS.2.2.A17 - IA) 14](#_Toc79332416)

[Einsatz von Verbunddiensten (OPS.2.2.A18 - CIA) 14](#_Toc79332417)

[Sicherheitsüberprüfung von Mitarbeitern (OPS.2.2.A19 - CIA) 14](#_Toc79332418)

# Allgemeine Festlegungen

## Ziel / Zweck

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.

Cloud Computing bietet viele Vorteile: Die IT-Dienste können bedarfsgerecht, skalierbar und flexibel genutzt und je nach Funktionsumfang, Nutzungsdauer und Anzahl der Benutzer abgerechnet werden. Auch kann auf spezialisierte Kenntnisse und Ressourcen des Cloud-Dienstleisters zugegriffen werden, wodurch interne Ressourcen für andere Aufgaben freigesetzt werden können. In der Praxis zeigt sich jedoch häufig, dass sich die Vorteile, die die <Institution> von der Cloud-Nutzung erwarten, nicht vollständig auswirken. Die Ursache dafür ist meistens, dass wichtige kritische Erfolgsfaktoren im Vorfeld der Cloud-Nutzung nicht ausreichend betrachtet werden. Daher müssen Cloud-Dienste strategisch geplant sowie (Sicherheits-)Anforderungen, Verantwortlichkeiten und Schnittstellen sorgfältig definiert und vereinbart werden.

Auch das Bewusstsein und Verständnis für die notwendigerweise geänderten Rollen, sowohl auf Seiten der IT-Verantwortlichen innerhalb der <Institution> als auch der Mitarbeitenden der <Institution> sind ein wichtiger Erfolgsfaktor.

Zusätzlich sollte bei der Einführung von Cloud-Diensten auch das Thema Governance (Cloud Governance) berücksichtigt werden. Kritische Bereiche sind beispielsweise die Vertragsgestaltung, die Umsetzung von Mandantenfähigkeit, die Sicherstellung von Portabilität unterschiedlicher Services, die Abrechnung genutzter Service-Leistungen, das Monitoring der Service-Erbringung, das Sicherheitsvorfallsmanagement, das Notfallmanagement und zahlreiche Datenschutzaspekte.

Diese Sicherheitsrichtlinie beschreibt Anforderungen, durch die sich Cloud-Dienste sicher nutzen lassen. Er richtet sich an alle, die solche Dienste bereits nutzen oder sie zukünftig einsetzen wollen. Bei der Erstellung dieser Sicherheitsrichtlinie wurden die Vorgaben des BSI Bausteines OPS.2.2 "Cloud-Nutzung" 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 Cloud-Nutzung“ 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 „Cloud-Nutzung"

## Basismaßnahmen

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

### Erstellung einer Cloud-Nutzungs-Strategie (OPS.2.2.A1)

In der Cloud-Nutzungs-Strategie der <Institution> sind gültige Ziele, Chancen und Risiken definiert, die die <Institution> mit der Cloud-Nutzung verbindet. Ausgehend von der grundsätzlichen Entscheidung für Cloud-Dienste ist dabei festzuhalten, in welchem Umfang klassische IT durch Cloud-Dienste abgelöst werden soll. Es ist zu erarbeiten, welche Dienste für eine Cloud-Nutzung grundsätzlich infrage kommen. Jede Cloud-Nutzung ist dabei einzeln zu bewerten und gemäß den Vorgaben dieser Sicherheitsrichtlinie umzusetzen.

Für jede Cloud-Nutzung sind die rechtlichen und organisatorischen Rahmenbedingungen sowie die technischen Anforderungen zu untersuchen, die sich aus der Nutzung von Cloud-Diensten ergeben. Die Ergebnisse dieser Untersuchung werden in einer Machbarkeitsstudie dokumentiert.

In der <Institution> wird festgelegt, welche Dienste in welchem Bereitstellungsmodell zukünftig von einem Cloud-Dienstleister bezogen werden sollen. Zudem ist sichergestellt, dass bereits in der Planungsphase zur Cloud-Nutzung alle grundlegenden technischen und organisatorischen Sicherheitsaspekte ausreichend berücksichtigt werden.

Für jeden geplanten Cloud-Dienst ist eine individuelle Sicherheitsanalyse durchzuführen und muss mindestens die hier aufgeführten Aspekte berücksichtigen:

* Es sind die benötigten technischen Verfügbarkeiten (Serviceklassen) des angebotenen Dienstes sowie die Umsetzung dieser Vorgaben am Standort der Leistungserbringung des Cloud-Dienstleister zu erheben und hieraus resultierende potenzielle IT- und Prozessrisiken abzuleiten.
* Es sind die etablierten Sicherheitsanforderungen in Abhängigkeit vom Bereitstellungsmodell einer Multi-Cloud zu erheben und zu bewerten.
* Es sind die vom Cloud-Dienstleister der <Institution> eingeräumten Nutzungsrechte bzgl. den Zutritts-, Zugangs- und Zugriffsrechten auf Informationen und IT-Systeme zu erheben und hieraus resultierende Risiken zu bewerten.
* Es sind die relevanten Europäischen-, Landes- oder Bundesgesetze und Vorschriften als Grundlage für die Sicherheitsbetrachtung insbesondere bei länderübergreifenden oder international agierenden Cloud-Dienstleister heranzuziehen. Da diese Cloud-Dienstleister unter Umständen andersartigen gesetzlichen Anforderungen und Bestimmungen unterliegen. Als Grundlage für die Sicherheitsbetrachtung ist der Anforderungskatalog Cloud Computing (C5) des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) anzuwenden. Sofern ein Cloud-Dienstleister bereits eine C5 Überprüfung erfolgreich durchlaufen ist und die Ergebnisse (Zertifizierung) zur Verfügung stellt, kann auf diese zurückgegriffen werden.

Die Sicherheitsanalyse wird wiederholt, wenn sich technische und organisatorische Rahmenbedingungen wesentlich verändern. Für größere Cloud-Projekte wird eine geeignete Roadmap erarbeitet, die festlegt, wann und wie ein Cloud-Dienst eingeführt wird.

### Service-Definition für Cloud-Dienste durch den Anwender (OPS.2.2.A3)

Für jeden Cloud-Dienst ist eine Service-Definition zu erarbeiten. Alle geplanten und benutzten Cloud-Dienste sind zu dokumentieren.

Im Rahmen der Service-Definition für Cloud-Dienste sind zusätzlich die hier näher beschriebenen Aspekte zu thematisieren:

* Für Cloud-Dienste sind sichere und freigegebene Authentisierungsmethoden auszuwählen und einzusetzen. Wurde im Rahmen der Schutzbedarfserhebung für den Cloud-Dienst ein hohes oder sehr hohes Schutzniveau identifiziert, werden für alle Benutzer starke Authentisierungsmechanismen und eine Zwei-Faktor-Authentisierung (2FA) eingesetzt.
* Neben dem Aspekt Authentisierung sind im Rahmen der Service-Definition für Cloud-Dienste auch Vorgaben zur Verschlüsselung von Informationen auf Basis des ermittelten Schutzbedarfes zu erstellen.
* Es sind konkrete Servicevorgaben an die zu verwendenden Cloud-Dienste unter Berücksichtigung von zu erfüllenden betrieblichen, sicherheitstechnischen, datenschutzrechtlichen und notfalltechnischen Anforderungen auszuarbeiten.

### Festlegung von Verantwortungsbereichen und Schnittstellen (OPS.2.2.A4)

Basierend auf der Service-Definition für Cloud-Dienste identifiziert und dokumentiert die <Institution> alle relevanten Schnittstellen zu externen und internen Diensten und die Verantwortlichkeiten für die Cloud-Nutzung. Hierdurch ist sichergestellt, dass auf die folgenden Fragen eine vollumfängliche Antwort gegeben werden kann:

* Existiert eine definierte Rückfallebene, wenn die PaaS, IaaS oder SaaS ausfällt?
* Sind eventuelle Abhängigkeiten oder Inkompatibilitäten im Zusammenhang mit den vorhandenen Cloud-Anwendungen oder IT-Infrastruktur der <Institution> zu erwarten?
* Kann die Cloud-Software bzw. Cloud-Lösung ohne Weiteres in die bestehenden Prozesse des Änderungsmanagements der <Institution> integriert werden oder sind Anpassungen notwendig?
* Erfüllt die Cloud-Software bzw. Cloud-Lösung die Anforderungen hinsichtlich bestehender Test- und Freigabeprozesse?
* Existiert eine definierte Strategie zur Vermeidung eines Cloud-Anbieter Lock-In-Effektes?
* Wie werden Verantwortungsbereiche zwischen den Cloud-Anbietern und der <Institution> klar erkennbar voneinander abgegrenzt?

## Standardmaßnahmen

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

### Planung der sicheren Migration zu einem Cloud-Dienst (OPS.2.2.A5)

Die Basis für die Migrationen zu Cloud-Diensten in der <Institution> sind die einzelnen zu erstellenden Migrationskonzepte. In den Migrationskonzepten sind organisatorische Regelungen und angemessene Aufgabenverteilungen für jede Migration festzulegen. Zudem werden bestehende Betriebsprozesse hinsichtlich der Cloud-Nutzung identifiziert und angepasst. In allen Migrationsprozessen sind die eigenen IT-Systeme und -Infrastrukturen zu berücksichtigen. Die Migrationsverantwortlichen ermitteln und bestimmen, ob beteiligte Mitarbeiter von der <Institution> zusätzlich geschult oder sensibilisiert werden sollten.

### Planung der sicheren Einbindung von Cloud-Diensten (OPS.2.2.A6)

Nachdem die Planung der sicheren Migration von Cloud-Diensten abgeschlossen ist, muss geplant werden, wie Cloud-Dienste sicher in die IT-Infrastruktur der <Institution> einzubinden sind. Hierbei sind über die Migrationsplanung hinausgehen die hier aufgeführten Aspekte zu betrachten.

1. Betrachtung des Anpassungsbedarfs der Schnittstellensysteme (Loadbalancer, Proxys, Router, Sicherheitsgateways und Federation-Systeme).
   1. Besteht ein Bedarf an der Bereitstellung neuer Schnittstellensysteme?
   2. Sind alle benötigten Schnittstellensysteme mit dem betrachteten Cloud-Diensten interoperabel?
   3. Können die vorhandenen Schnittstellensysteme auf allen Ebenen mit dem jeweiligen Cloud-Dienst umgehen?
   4. Welche Performance beziehungsweise welchen Datendurchsatz müssen geeignete Schnittstellensysteme zur Verfügung stellen können?
   5. Müssen Schnittstellensysteme redundant ausgelegt sein und wenn ja, wie wird dies umgesetzt?
2. Betrachtung des Anpassungsbedarfs der Netzanbindung.
   1. Ist die bestehende Bandbreite der Netzanbindung ausreichend oder muss sie für die Cloud-Nutzung angepasst werden?
   2. Stellen die zu nutzenden Cloud-Dienste spezielle Anforderungen an die Latenz der Netzanbindung?
   3. Sollen Cloud-Dienste redundant angebunden werden?
   4. Welche Vorkehrungen wurden hinsichtlich der Ausfallsicherheit der Netzanbindung getroffen?
3. Betrachtung des Anpassungsbedarfs des Administrationsmodells.
   1. Wurde die Administration von Cloud-Diensten sorgfältig geplant?
   2. Existiert ein Rollen- und Berechtigungskonzept, das eine Trennung von Administratoren und Benutzern für die Cloud-Nutzung vorsieht?
4. Betrachtung des Anpassungsbedarfs des Datenmanagementmodells.
   1. Welche Daten der <Institution> befinden sich gegebenenfalls nicht mehr ausschließlich in der administrativen Hoheit der <Institution>?
   2. Welche Auswirkungen auf die bisherigen die Datensicherungs- und Datenaufbewahrungsstrategien ändern sich durch die Nutzung von Cloud-Diensten?

Die Ergebnisse der Prüfungen werden dokumentiert und in regelmäßigen Abständen aktualisiert.

### Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung (OPS.2.2.A7)

Auf Grundlage der identifizierten Sicherheitsanforderungen ist ein Sicherheitskonzept für die Nutzung von Cloud-Diensten zu erstellen. Eine der wenigen Besonderheiten bei Cloud-Diensten ist, dass mehrere Parteien beteiligt sind. Dieses ist bei der Erstellung des Sicherheitskonzepts zu berücksichtigen.

Im Sicherheitskonzept für die Cloud-Nutzung ist zusätzlich die besondere Gefährdungslage durch Cloud-Dienste zu beschrieben. Hierbei sollten insbesondere folgende Punkte betrachtet werden:

* Vorzeitige oder zwangsweise Vertragsbeendigung,
* Fehlende Portabilität von Daten bei Software as a Service (SaaS) oder Function as a Service (FaaS), Anwendungen bei Platform as a Service (PaaS) und IT-Systemen bei Infrastructure as a Service (IaaS) für den Fall, dass der gewählte Cloud-Dienst von etablierten Standards der <Institution> abweicht,
* Abhängigkeit von einem Cloud-Dienstleister durch fehlende Möglichkeit, den Anbieter zu wechseln (Vendor-Lock-in),
* Nutzung proprietärer Datenformate, die die Integrität der Informationen gefährden und den Wechsel des Cloud-Anbieters erschweren,
* Gemeinsame Nutzung der Cloud-Infrastruktur durch die <Institution> und Kunden (Multi-Tenancy),
* Fehlende Kenntnis über den tatsächlichen Speicherort von Informationen,
* Hohe Mobilität der Informationen sowie
* Unbefugter Zugriff auf Informationen durch Administratoren des Cloud-Dienstleisters, zuständige Landesbehörden des Cloud-Anbieters oder Dritte.

### Sorgfältige Auswahl eines Cloud-Diensteanbieters (OPS.2.2.A8)

Basierend auf der Service-Definition für den Cloud-Dienst wird ein detailliertes Anforderungsprofil für einen Cloud-Dienstleister erstellt. Zusätzlich sind Leistungsbeschreibungen und Lastenhefte zu erstellen. Für die Bewertung eines Cloud-Dienstleisters werden auch ergänzende Informationsquellen herangezogen. Ebenso werden verfügbare Service-Beschreibungen des Cloud-Dienstleisters sorgfältig geprüft und hinterfragt.

### Vertragsgestaltung mit dem Cloud-Diensteanbieter (OPS.2.2.A9)

Die vertraglichen Regelungen zwischen der <Institution> und dem Cloud-Dienstleister werden in Art, Umfang und Detaillierungsgrad dem Schutzbedarf der Informationen angepasst, die im Zusammenhang mit der Cloud-Nutzung stehen.

Bestandteil des Vertrages sind.

* Der Ort der Leistungserbringung durch den Cloud-Dienstleister.
* Welche Subunternehmer oder andere Dritte an der Erbringung des Dienstes beteiligt sind.
* Die Absicherung der Infrastruktur durch den Cloud-Anbieter.
* Ob besondere Anforderungen an Fähigkeiten, Qualifikationen und Zertifizierungen hinsichtlich des Personals beim Cloud-Dienstleister erforderlich sind.
* Welche Kommunikationswege genutzt und welche Ansprechpartner für die <Institution> verantwortlich sind.
* Spezielle Regelungen zu Prozessen, Arbeitsabläufen und Zuständigkeiten.
* Regelungen zur Beendigung des Vertragsverhältnisses.
* Sicherstellung der sicheren Datenlöschung beim Cloud-Dienstleister.
* Regelungen zu Zutritts- und Zugriffsberechtigungen.
* Regelungen zur Notfallvorsorge.
* Regelungen zu rechtlichen Rahmenbedingungen.
* Festlegungen zum Änderungsmanagement und zu Testverfahren.
* Regelungen zur Durchführung von Kontrollen,
  + Vorgaben zur Aufbewahrungsfrist für Log-Daten,
  + Wirksame Kontrollen zum Schutz von Logs vor nicht autorisiertem Zugriff,
  + Methoden zur Überprüfung und Sicherung der Integrität von Audit-Logs,
  + Durchführung von Audit-Log-Reviews sowie
  + Vorgaben zur Zeitquelle, die genutzt wird, um Systeme zu synchronisieren und einen exakten Zeitstempel für Audit-Logs anzubieten.
* Berücksichtigung besonderer Anforderungen der <Institution>
  + Nutzung von ausschließlich vorab definierten Rechenzentren
  + Regelungen zum Import bzw. Export von Daten sowie zu benötigten Schnittstellen zu anderen Services und Systemen,
  + Festlegung der konkreten Konfigurationsparameter bezüglich definierter Interoperabilitätsanforderungen sowie
  + Einräumen des Rechts eigene Datensicherungen durchzuführen und notwendige Schnittstellen und Parameter zu erfassen.

### Sichere Migration zu einem Cloud-Dienst (OPS.2.2.A10)

Alle Migrationen zu den vertraglichen Cloud-Diensten erfolgen auf Basis der erstellten Migrationskonzepte.

Während den Migrationen ist zu prüfen, ob die Sicherheitskonzepte für die Cloud-Nutzung an etwaige neue Anforderungen angepasst werden müssen. Alle Notfallvorsorgemaßnahmen im Rahmen der Migrationen sind vollständig und aktuell vorzuhalten.

Alle Migrationen zu Cloud-Diensten sind sorgfältig und gemäß Anforderungsliste vor der Überführung in die Produktivumgebung in einer Testumgebung zu testen. Sofern der Cloud-Dienst in den produktiven Betrieb übergeht, wird abgeglichen, ob der Cloud-Dienstleister die definierten Anforderungen der <Institution> erfüllt.

### Erstellung eines Notfallkonzeptes zu einem Cloud-Dienst (OPS.2.2.A11)

Im Rahmen des Notfallkonzeptes sind sowohl organisatorische als auch technische Aspekte zu betrachten. Um bei einem Notfall schnell reagieren zu können, muss das Notfallkonzept alle notwendigen Angaben zu internen und externen Zuständigkeiten und deren Ansprechpartnern benennen. Alle im Notfallkonzept vorgesehenen Abläufe müssen klar geregelt und vollständig dokumentiert sein. Von besonderer Wichtigkeit sind Detailregelungen für die Datensicherung, da diese in den meisten Notfallszenarien besonders wichtig sind. Darüber hinaus sind um alle betrieblichen, sicherheitstechnischen Vorgaben im Rahmen des Notfallmanagements mit zu beachten durch die betrieblichen Verantwortliche für Cloud-Dienste, den Notfallbeauftragten, den Informationssicherheitsbeauftragten sowie dem Technical Security Officer ein Konzept für regelmäßig durchzuführende Notfallübungen zu erarbeiten. Es ist zu entscheiden und festzuhalten, inwieweit gemeinsame Notfallübungen mit dem Cloud-Dienstleistervorgesehen sind.

Bei der Erstellung des Notfallkonzepts für die Cloud-Nutzung ist zu beachten, dass der Schutzbedarf für die Anbindung und die Schnittstellensysteme verglichen mit den bisherigen Anforderungen höher sein könnte. Ursache hierfür ist die Nutzung von Cloud-Diensten für kritische Geschäftsprozesse.

### Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb (OPS.2.2.A12)

Die Vorgaben und Dokumentationen für die eingesetzten Cloud-Dienste sind zur Aufrechterhaltung der Informationssicherheit regelmäßig zu aktualisieren. Im Rahmen der periodischen Kontrolle, ob die Cloud-Dienstleister die vertraglich zugesicherten Services erbringen, sind folgende Themenblöcke zu prüfen.

* Kontrolle der Dienst-Erbringung z. B. Verfügbarkeit, maximale Anzahl gleichzeitiger Benutzer, maximale Anzahl aktiver Systeme, Schnelligkeit der Einrichtung neuer Benutzer oder neuer Ressourcen sowie die Performance der Netzanbindung und -verbindungen.
* Service-Reviews z. B. Gegenüberstellung der vereinbarten und die tatsächlich erreichten Service-Level, Behandlung von Ausnahmesituationen und Sicherstellung der Interoperabilität von Cloud-Diensten bei Nutzung mehrerer Cloud-Dienste. Bei hohen Schutzbedarf sollten die Service-Reviews zwischen Cloud-Dienstleister und der <Institution> erfolgen.
* Es sind durch den Cloud-Dienstleister Sicherheitsnachweise zu erbringen.
* Es ist die ordnungsgemäße Durchführung von Datensicherungen zu verifizieren.
* Es ist die Einhaltung vorgesehener und vereinbarter Prozesse sicherzustellen.
* Es sind die technischen Maßnahmen zur Verhinderung der Nutzung nicht erlaubter Services zu kontrollieren.
* Es sind betriebliche und sicherheitstechnische Audits sowie Penetrationstests regelmäßig durchzuführen.

Es sind regelmäßige Reviews der vergebenen Berechtigungen zur Wahrung der ordnungsgemäßen Administration von Cloud-Diensten durchzuführen.

### Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung (OPS.2.2.A13)

Die <Institution> lässt sich von den Cloud-Anbietern regelmäßig nachweisen, dass die vereinbarten Sicherheitsanforderungen erfüllt werden. Es werden nur Nachweis akzeptiert, die auf einem international anerkannten Standard (z. B. Anforderungskatalog Cloud Computing (C5), Cloud Controls Matrix der Cloud Security Alliance) basieren. Die <Institution> prüft, ob der Geltungsbereich und Schutzbedarf die genutzten Cloud-Dienste erfasst.

Nutzt ein Cloud-Dienstleister Subunternehmer, um die Cloud-Dienste zu erbringen, sind der <Institution> regelmäßige Nachweise über die Durchführung der notwendigen Audits durch die Subunternehmer zu übermitteln.

Um die Wirksamkeit vorhandener technischer Sicherheitsmaßnahmen seitens des Cloud-Dienstleisters zu überprüfen, sind regelmäßige Penetrationstests als ein erprobtes und geeignetes Vorgehen zu etablieren.

### Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses (OPS.2.2.A14)

Bei Beendigung eines Dienstleistungsverhältnisses mit einem Cloud-Dienstleister wird sichergestellt, dass dadurch die Geschäftstätigkeit nicht beeinträchtigt wird. Die Verträge mit dem Cloud-Dienstleister regeln die geordneten Auflösungen der Dienstleistungsverhältnisse. Folgende Aspekte sind mindestens zu beachten:

* Eigentumsrechte an Hard- und Software (Schnittstellenprogramme, Tools, Batch-Abläufe, Makros, Lizenzen, Backups) sind zu regeln.
* Die Weiterverwendung der vom bisherigen Cloud-Dienstleister eingesetzten Tools, Prozeduren, Skripte, Batch-Programme ist für den Fall der Beendigung des Dienstleistungsverhältnisses zu regeln.
* IT-Systeme, Anwendungen und Arbeitsabläufe sind ausreichend zu dokumentieren.
* Alle notwendigen Daten sind vom Cloud-Dienstleister an die <Institution> zu übertragen beziehungsweise zu übergeben.
* Alle bisher angefallenen Datenbestände beim Cloud-Dienstleister sind sicher zu löschen.
* Mitarbeiter, welche Aufgaben des Cloud-Dienstleisters übernehmen, sind einzuweisen und zu schulen.
* Es sind Übergangsfristen vertraglich zu vereinbaren, in der der bisherige Cloud-Dienstleister noch für Rückfragen und Hilfestellungen seitens der <Institution> zur Verfügung steht.
* Es ist eine Definition abgestimmt, wie mit Daten aus älteren Datensicherungen umzugehen ist.

## 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).

### Portabilität von Cloud-Diensten (OPS.2.2.A15 - A)

Im Rahmen der Portabilität von Cloud-Diensten bei erhöhtem Schutzbedarf werden alle Anforderungen definiert, die es ermöglichen, einen Cloud-Dienstleister zeitnah zu wechseln oder den Cloud-Dienst bzw. die Daten in die eigene IT-Infrastruktur zurückzuholen. Zudem sind regelmäßig Portabilitätstests durchzuführen.

In den Verträgen mit den Cloud-Anbietern werden Vorgaben festgehalten, mit denen sich die notwendige Portabilität gewährleisten lässt.

### Durchführung eigener Datensicherungen (OPS.2.2.A16 - IA)

Bei erhöhtem Schutzbedarf wird geprüft, ob neben den vertraglich festgelegten Datensicherungen der Cloud-Dienstleister auch eigene Datensicherungen erstellt werden sollen. Zudem werden in diesem Zusammenhang detaillierte Anforderungen an einen Datensicherungsservice im Rahmen der Cloud-Nutzung erstellt.

### Einsatz von Verschlüsselung bei Cloud-Nutzung (OPS.2.2.A17 - IA)

Sofern Daten bei erhöhtem Schutzbedarf durch einen Cloud-Dienstleister verschlüsselt werden, ist vertraglich zu regeln, welche Verschlüsselungsmechanismen und welche Schlüssellängen eingesetzt werden dürfen. Zudem ist die Herkunft der Schlüssel abzustimmen.

Bei der Verwendung von eigenen Verschlüsselungsmechanismen ist ein geeignetes Schlüsselmanagement sicherzustellen. Bei der Verschlüsselung werden die eventuellen Besonderheiten des gewählten Cloud-Service-Modells berücksichtigt.

### Einsatz von Verbunddiensten (OPS.2.2.A18 - CIA)

Bei erhöhtem Schutzbedarf ist zu prüfen, ob beim jeweiligen Cloud-Nutzungs-Vorhaben Federation Services eingesetzt werden und dass die <Institution> als Identity-Provider agiert.

In den SAML-Tickets (Security Assertion Markup Language) sind an den Cloud-Anbieter ausschließlich die erforderlichen Informationen zu übertragen. Die Berechtigungen werden regelmäßig überprüft, sodass nur berechtigten Benutzern ein SAML-Ticket ausgestellt wird.

### Sicherheitsüberprüfung von Mitarbeitern (OPS.2.2.A19 - CIA)

Bei erhöhtem Schutzbedarf werden mit den externen Cloud-Anbietern Vereinbarungen über die geeigneten Prüfungen der Qualifikationen und Vertrauenswürdigkeiten des eingesetzten Personals festgelegt. Dazu werden gemeinsam mit dem Cloud-Anbieter Kriterien definiert.