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

Sicherheitsrichtlinie "Datensicherung"

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 | ISMS300002 | [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](#_Toc78648635)

[Dokumentenhistorie 3](#_Toc78648636)

[Inhaltsverzeichnis 4](#_Toc78648637)

[Allgemeine Festlegungen 5](#_Toc78648638)

[Ziel / Zweck 5](#_Toc78648639)

[Geltungsbereich 5](#_Toc78648640)

[Zuständigkeiten 5](#_Toc78648641)

[Genehmigungs- und Änderungsverfahren 6](#_Toc78648642)

[Aufbau des Dokuments 6](#_Toc78648643)

[Sicherheitsrichtlinie "Datensicherung" 7](#_Toc78648644)

[Basismaßnahmen 7](#_Toc78648645)

[Erhebung der Einflussfaktoren der Datensicherung (CON.3.A1) 7](#_Toc78648646)

[Festlegung der Verfahrensweise für die Datensicherung (CON.3.A2) 7](#_Toc78648647)

[Ermittlung von rechtlichen Einflussfaktoren auf die Datensicherung (CON.3.A3) 7](#_Toc78648648)

[Erstellung eines Minimaldatensicherungskonzeptes (CON.3.A4) 7](#_Toc78648649)

[Regelmäßige Datensicherung (CON.3.A5) 7](#_Toc78648650)

[Standardmaßnahmen 8](#_Toc78648651)

[Entwicklung eines Datensicherungskonzepts (CON.3.A6) 8](#_Toc78648652)

[Beschaffung eines geeigneten Datensicherungssystems (CON.3.A7) 8](#_Toc78648653)

[Funktionstests und Überprüfung der Wiederherstellbarkeit (CON.3.A8) 8](#_Toc78648654)

[Voraussetzungen für die Online-Datensicherung (CON.3.A9) 8](#_Toc78648655)

[Verpflichtung der Mitarbeiter zur Datensicherung (CON.3.A10) 8](#_Toc78648656)

[Sicherungskopie der eingesetzten Software (CON.3.A11) 9](#_Toc78648657)

[Geeignete Aufbewahrung der Backup-Datenträger (CON.3.A12) 9](#_Toc78648658)

[Maßnahmen bei erhöhtem Schutzbedarf 9](#_Toc78648659)

[Einsatz kryptografischer Verfahren bei der Datensicherung (CON.3.A13 - CIA) 9](#_Toc78648660)

# Allgemeine Festlegungen

## Ziel / Zweck

Es werden immer mehr Daten gespeichert und die <Institution> ist gleichzeitig immer stärker auf die digitalen Daten angewiesen. Gehen digitale Daten verloren z. B. durch defekte Hardware, Malware oder versehentliches Löschen, können gravierende Schäden für die <Institution> selbst als auch für eventuelle Kunden der <Institution> entstehen. Durch regelmäßige Datensicherungen lassen sich solche Auswirkungen jedoch minimieren. Eine Datensicherung soll gewährleisten, dass durch einen redundanten Datenbestand der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen.

Das vorliegende Dokument definiert verbindliche Vorgaben zum Prozess „Datensicherung“ für die <Institution>. Bei der Erstellung der Sicherheitsrichtlinie wurden die Vorgaben des BSI Bausteines CON.3 "Datensicherungskonzept" 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 Datensicherung“ 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 "Datensicherung"

## Basismaßnahmen

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

### Erhebung der Einflussfaktoren der Datensicherung (CON.3.A1)

Für jeden Service und dessen IT-System und eventuell für einzelne besonders wichtige IT-Anwendung sind die relevanten Einflussfaktoren zu ermitteln. Mindestens sind die folgenden Einflussfaktoren Änderungsvolumen, Änderungsfrequenz, Verfügbarkeitsanforderungen sowie Integritätsbedarf einzubeziehen. Bei den Verfügbarkeitsanforderungen kann unterschieden werden, zwischen Informationen/Daten unserer Kunden und den Daten der <Institution>. Die Ergebnisse sind nachvollziehbar und auf geeignete Weise zentral festzuhalten. Neue Anforderungen sind zeitnah in einem aktualisierten Datensicherungskonzept zu berücksichtigen.

### Festlegung der Verfahrensweise für die Datensicherung (CON.3.A2)

Für jedes IT-System und für jede Datenart ist ein Verfahren festzulegen, wie die Daten zu sichern sind. Hierzu sind Art, Häufigkeit und Zeitpunkte der Datensicherungen festzulegen. Weiterhin sind die Verantwortlichkeiten für die Datensicherungen zu benennen. Es ist festzulegen, welche Speichermedien eingesetzt werden dürfen und wie die Transport- und Aufbewahrungsmodalitäten entsprechen den gesetzlichen und regulatorischen Anforderungen erfolgen müssen.

### Ermittlung von rechtlichen Einflussfaktoren auf die Datensicherung (CON.3.A3)

Die rechtlichen Anforderungen an die Datensicherung sind zu ermitteln und fließen in das Minimaldatensicherungskonzept ein.

### Erstellung eines Minimaldatensicherungskonzeptes (CON.3.A4)

Im Minimaldatensicherungskonzept ist festgelegt, welche Anforderungen für die Datensicherung mindestens einzuhalten sind. Dazu zählen kurze Beschreibungen, wie die Datensicherung erstellt und wiederhergestellt werden kann, welche Parameter gewählt wurden und welche Hard- und Software eingesetzt wird.

### Regelmäßige Datensicherung (CON.3.A5)

Es sind regelmäßige Datensicherungen unter Einhaltung der internen Vorgaben durchzuführen. Es werden mindestens die Daten regelmäßig gesichert, die nicht aus anderen Informationen ableitbar sind. Die erstellten Datensicherungen sind in geeigneter Weise vor dem Zugriff Dritter geschützt. Die gewünschte Funktionsfähigkeit der Datensicherung wird regelmäßig getestet. Das Wiedereinspielen von Datensicherungen läuft koordiniert und problemlos ab.

## Standardmaßnahmen

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

### Entwicklung eines Datensicherungskonzepts (CON.3.A6)

Das Datensicherungskonzept ist mit allen Verantwortlichen abzustimmen. Im Datensicherungskonzept sind sämtliche zu berücksichtigende IT-Systeme aufzuführen. Die Mitarbeiter werden über den sie betreffenden Teil des Datensicherungskonzepts unterrichtet. Durch regelmäßige Kontrollen wird gewährleistet, dass die Datensicherungskonzepte korrekt umgesetzt sind.

### Beschaffung eines geeigneten Datensicherungssystems (CON.3.A7)

Bevor ein Datensicherungssystem beschafft wird, sollte eine Anforderungsliste erstellt werden, nach der die am Markt erhältlichen Produkte oder vom Cloud-Dienstleister integrierten Produkte bewertet werden. Die angeschafften Datensicherungssysteme müssen die Anforderungen des Sicherheits- und des Datensicherungskonzepts erfüllen.

### Funktionstests und Überprüfung der Wiederherstellbarkeit (CON.3.A8)

Die gewünschte Funktionsfähigkeit der Datensicherungen und die Überprüfungen der problemlosen Wiederherstellbarkeit der Datensicherungen sind regelmäßig zu testen. Die Ergebnisse des Tests sind geeignet zu dokumentieren.

### Voraussetzungen für die Online-Datensicherung (CON.3.A9)

Wenn für die Datensicherung ein Cloud-Service verwendet wird, sind mindestens folgende Aspekte zu berücksichtigen:

* Gestaltung des Vertrages
* Ort der Datenspeicherung
* Vereinbarungen zu den Serviceklassen:
	+ Service-Level Agreement (SLA)
	+ Operational-Level Agreement (OLA)
	+ Recovery Time Objective (RTO)
	+ Recovery Point Objective (RPO)
* Geeignete Authentisierungsmethoden
* Verschlüsselung der Daten
* Verschlüsselung auf dem Transportweg

### Verpflichtung der Mitarbeiter zur Datensicherung (CON.3.A10)

Alle für die Datensicherung verantwortlichen Mitarbeiter werden über die Regelungen zur Datensicherung sensibilisiert und bei Bedarf geschult. Sie werden in diesem Kontext über die Aufgaben bei der Erstellung von Datensicherung und den Datensicherungspflichten (zum Beispiel regelmäßige Durchführung der Datensicherung) informiert.

### Sicherungskopie der eingesetzten Software (CON.3.A11)

Von eingesetzten Softwareprogrammen werden Sicherungskopien angefertigt, sofern das rechtlich erlaubt und technisch möglich ist. Dabei werden alle notwendigen Pakete und Informationen vorgehalten, um die Software im Notfall wieder installieren zu können. Die originalen Installationsquellen sowie die Lizenznummern werden an einem geeigneten Ort sicher aufbewahrt.

### Geeignete Aufbewahrung der Backup-Datenträger (CON.3.A12)

Die Backup-Datenträger werden vor unbefugtem Zugriff geschützt und räumlich von den Quellsystemen getrennt. Der Aufbewahrungsort ist so klimatisiert, dass die Datenträger längerfristig aufbewahrt werden können.

## 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).

### Einsatz kryptografischer Verfahren bei der Datensicherung (CON.3.A13 - CIA)

Zur Gewährleistung der Vertraulichkeit und Integrität der gesicherten Daten sollten alle Daten bei einem erhöhten Schutzbedarf verschlüsselt werden. Prozessual ist sicherzustellen, dass die verschlüsselten Daten auch nach längerer Zeit wieder eingespielt werden können. Verwendete kryptografische Schlüssel sind mit einer getrennten Datensicherung zu schützen.