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

Sicherheitsrichtlinie "Archivierung"

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 | ISMS300014 | [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](#_Toc79384279)

[Dokumentenhistorie 3](#_Toc79384280)

[Inhaltsverzeichnis 4](#_Toc79384281)

[Allgemeine Festlegungen 5](#_Toc79384282)

[Ziel / Zweck 5](#_Toc79384283)

[Geltungsbereich 5](#_Toc79384284)

[Zuständigkeiten 6](#_Toc79384285)

[Genehmigungs- und Änderungsverfahren 6](#_Toc79384286)

[Aufbau des Dokuments 6](#_Toc79384287)

[Sicherheitsrichtlinie „Archivierung" 7](#_Toc79384288)

[Basismaßnahmen 7](#_Toc79384289)

[Ermittlung von Einflussfaktoren für die elektronische Archivierung (OPS.1.2.2.A1) 7](#_Toc79384290)

[Entwicklung eines Archivierungskonzepts (OPS.1.2.2.A2) 7](#_Toc79384291)

[Geeignete Aufstellung von Archivsystemen und Lagerung von Archivmedien (OPS.1.2.2.A3) 7](#_Toc79384292)

[Konsistente Indizierung von Daten bei der Archivierung (OPS.1.2.2.A4) 7](#_Toc79384293)

[Regelmäßige Aufbereitung von archivierten Datenbeständen (OPS.1.2.2.A5) 7](#_Toc79384294)

[Schutz der Integrität der Indexdatenbank von Archivsystemen (OPS.1.2.2.A6) 8](#_Toc79384295)

[Regelmäßige Datensicherung der System- und Archivdaten (OPS.1.2.2.A7) 8](#_Toc79384296)

[Protokollierung der Archivzugriffe (OPS.1.2.2.A8) 8](#_Toc79384297)

[Auswahl geeigneter Datenformate für die Archivierung von Dokumenten (OPS.1.2.2.A9) 8](#_Toc79384298)

[Standardmaßnahmen 8](#_Toc79384299)

[Erstellung einer Richtlinie für die Nutzung von Archivsystemen (OPS.1.2.2.A10) 9](#_Toc79384300)

[Einweisung in die Administration und Bedienung des Archivsystems (OPS.1.2.2.A11) 9](#_Toc79384301)

[Überwachung der Speicherressourcen von Archivmedien (OPS.1.2.2.A12) 9](#_Toc79384302)

[Regelmäßige Revision der Archivierungsprozesse (OPS.1.2.2.A13) 10](#_Toc79384303)

[Regelmäßige Beobachtung des Marktes für Archivsysteme (OPS.1.2.2.A14) 10](#_Toc79384304)

[Regelmäßige Aufbereitung von kryptografisch gesicherten Daten bei der Archivierung (OPS.1.2.2.A15) 10](#_Toc79384305)

[Regelmäßige Erneuerung technischer Archivsystem-Komponenten (OPS.1.2.2.A16) 10](#_Toc79384306)

[Auswahl eines geeigneten Archivsystems (OPS.1.2.2.A17) 11](#_Toc79384307)

[Verwendung geeigneter Archivmedien (OPS.1.2.2.A18) 11](#_Toc79384308)

[Regelmäßige Funktions- und Recoverytests bei der Archivierung (OPS.1.2.2.A19) 11](#_Toc79384309)

[Maßnahmen bei erhöhtem Schutzbedarf 11](#_Toc79384310)

[Geeigneter Einsatz kryptografischer Verfahren bei der Archivierung (OPS.1.2.2.A20 - CI) 11](#_Toc79384311)

[Übertragung von Papierdaten in elektronische Archive (OPS.1.2.2.A21 - CI) 12](#_Toc79384312)

# Allgemeine Festlegungen

## Ziel / Zweck

Die Archivierung spielt im Dokumentenmanagementprozess eine besondere Rolle. Denn es wird einerseits erwartet, dass die digitalen Dokumente bis zum Ablauf einer vorgegebenen Aufbewahrungsfrist verfügbar sind. Andererseits soll ihre Vertraulichkeit und Integrität bewahrt bleiben. Zusätzlich muss der Kontext erhalten werden, damit der jeweilige gespeicherte Vorgang bei Bedarf jederzeit rekonstruierbar ist.

Während der gesamten Dauer der Langzeitspeicherung (Archivierung) müssen daher entsprechende Maßnahmen zur Informationserhaltung umgesetzt werden. Falls erforderlich trifft dies auch auf Maßnahmen zur Beweiswerterhaltung zu.

Der in dieser Sicherheitsrichtlinie verwendete Begriff „Dokumente“ beinhaltet Daten und digitale Dokumente, sofern sie nicht ausdrücklich in anderer Bedeutung gebraucht werden.

Aus rechtlicher Sicht ist der Begriff „Archivierung“ in Deutschland durch die Archivgesetze des Bundes und der Bundesländer konkretisiert und belegt. „Archivierung“ im juristisch korrekten Sinne betrifft allein Unterlagen der öffentlichen Verwaltung. Sie bezieht sich darauf, dass Unterlagen einer Behörde, sobald sie für deren Zwecke nicht mehr benötigt werden, ausgesondert und durch eine zuständige staatliche Einrichtung (Bundesarchiv) auf unbegrenzte Zeit verwahrt werden sollen (vgl. §§ 1 und 2 BarchG). Diese Art der Archivierung ist von der in dieser Sicherheitsrichtlinie betrachteten zeitlich beschränkten Aufbewahrung zu unterscheiden.

Diese Sicherheitsrichtlinie beschreibt, wie digitale Dokumente langfristig, sicher, unveränderbar und wieder reproduzierbar archiviert werden können. Dazu werden Anforderungen definiert, mit denen sich ein Archivsystem sicher planen, umsetzen und betreiben lässt. Die Aufbewahrung von Papierdokumenten wird in dieser Sicherheitsrichtlinie nicht betrachtet, es werden aber Anforderungen gestellt, wie diese digitalisiert und archiviert werden können.

Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben des BSI Bausteines OPS.1.2.2 "Archivierung" zurückgegriffen.

## 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 Archivierung“ 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 „Archivierung"

## Basismaßnahmen

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

### Ermittlung von Einflussfaktoren für die elektronische Archivierung (OPS.1.2.2.A1)

Bevor entschieden wird, welche Verfahren und Produkte für die elektronische Archivierung eingesetzt werden, sind die technischen, rechtlichen und organisatorischen Einflussfaktoren zu ermitteln und zu dokumentieren. Die Ergebnisse sind in das Archivierungskonzept zu übertragen.

### Entwicklung eines Archivierungskonzepts (OPS.1.2.2.A2)

Es wird definiert, welche Ziele mit der Archivierung erreicht werden sollen. Hierbei werden zu beachtende interne und gesetzliche Regularien, verantwortliche Mitarbeitende sowie der Funktions- und Leistungsumfang berücksichtigt.

Die Ergebnisse werden in einem Archivierungskonzept erfasst. Das Archivierungskonzept wird regelmäßig an den Stand der Technik, die Vorgaben der <Institution> und den gesetzlichen und regulatorischen Anforderungen angepasst. Die Geschäftsführung wird in die Entwicklung des Archivierungskonzepts eingebunden.

### Geeignete Aufstellung von Archivsystemen und Lagerung von Archivmedien (OPS.1.2.2.A3)

Die schützenswerten Archivsysteme und deren IT-Komponenten werden in gesicherten Räumen aufgestellt. Es ist sichergestellt, dass nur berechtigte Mitarbeitende die Räume betreten dürfen. Die Archivspeichermedien müssen für die langfristige Aufbewahrung geeignet gelagert werden.

### Konsistente Indizierung von Daten bei der Archivierung (OPS.1.2.2.A4)

Alle in einem Archiv abgelegten Daten, Dokumente und Datensätze werden eindeutig gekennzeichnet, um sie bei späteren Suchanfragen schnell wiederfinden zu können. Während der Konzeption wurden bereits die Strukturen und Umfänge der Indexangaben für das Archiv festgelegt.

### Regelmäßige Aufbereitung von archivierten Datenbeständen (OPS.1.2.2.A5)

Über den gesamten Archivierungszeitraum hinweg wird sichergestellt, dass:

* Das verwendete Datenformat von den benutzten Anwendungen verarbeitet werden kann,
* Die gespeicherten Daten auch zukünftig lesbar und so reproduzierbar sind, sodass Semantik und Beweiskraft beibehalten werden können,
* Das benutzte Dateisystem auf dem Speichermedium von allen beteiligten Komponenten verarbeitet werden kann,
* Die Speichermedien jederzeit technisch einwandfrei gelesen werden können und
* Die verwendeten kryptografischen Verfahren zur Verschlüsselung und zum Beweiswerterhalt mittels digitaler Signatur, Siegel, Zeitstempel oder technischen Beweisdaten (Evidence Records) dem Stand der Technik entsprechen.

### Schutz der Integrität der Indexdatenbank von Archivsystemen (OPS.1.2.2.A6)

Die Integrität der Indexdatenbank ist sicherzustellen und überprüfbar. Zusätzlich ist die Indexdatenbank regelmäßig zu sichern. Die Datensicherungen ist auf Wiederherstellbarkeit zu prüfen. Mittlere und große Archive müssen über redundante Indexdatenbanken verfügen.

### Regelmäßige Datensicherung der System- und Archivdaten (OPS.1.2.2.A7)

Alle Archivdaten, die zugehörigen Indexdatenbanken sowie die Systemdaten sind regelmäßig zu sichern.

### Protokollierung der Archivzugriffe (OPS.1.2.2.A8)

Alle Zugriffe auf elektronische Archive werden gemäß den Vorgaben des Dokuments ISMS-E3-00039-DE protokolliert. Zu diesem Zweck werden Datum, Uhrzeit, Benutzer, Clientsystem und die ausgeführten Aktionen sowie Fehlermeldungen aufgezeichnet. Die Aufbewahrungsdauer der Protokolldaten wird im Archivierungskonzept festgelegt.

Die Protokolldaten der Archivzugriffe werden regelmäßig ausgewertet. Dabei sind die Vorgaben der <Institution> zu beachten.

Es ist definiert, welche Ereignisse (zum Beispiel Systemfehler, Timeouts oder Datensätze kopieren) welchen Mitarbeitenden angezeigt und signalisiert werden. Kritische Ereignisse werden sofort nach der Signalisierung geprüft und, falls nötig, weiter an den Fachvorgesetzten und den Informationssicherheitsbeauftragten eskaliert.

### Auswahl geeigneter Datenformate für die Archivierung von Dokumenten (OPS.1.2.2.A9)

Für die Archivierung ist ein geeignetes Datenformat auszuwählen. Dieses Dateiformat gewährleistet, dass sich Archivdaten sowie ausgewählte Merkmale des ursprünglichen Dokumentmediums langfristig und originalgetreu reproduzieren lassen.

Die Dokumentstruktur des ausgewählten Datenformats ist eindeutig interpretierbar und elektronisch verarbeitbar. Die Syntax und Semantik der verwendeten Datenformate werden dokumentiert und veröffentlicht. Es ist für eine beweis- und revisionssichere Archivierung ein verlustfreies Bildkompressionsverfahren zu benutzen.

## Standardmaßnahmen

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

### Erstellung einer Richtlinie für die Nutzung von Archivsystemen (OPS.1.2.2.A10)

Es ist sicherzustellen, dass Mitarbeitende das Archivsystem so benutzen, wie es im Archivierungskonzept vorgesehenen ist. Allgemeine Vorgaben sind in den Dokumenten ISMS-E2-00001-DE und ISMS-E2-00003-DE benannt. Zusätzlich sollten folgende Punkte beachtet werden:

* Festlegung der Verantwortung für Betrieb und Administration der Archivsysteme
* Vereinbarungen über Leistungsparameter beim Betrieb (Service Level Agreements)
* Modalitäten der Vergabe von Zutritts- und Zugriffsrechten
* Modalitäten der Vergabe von Zugangsrechten zu den vom Archiv bereitgestellten Diensten
* Regelungen zum Umgang mit archivierten Daten und Archivmedien
* Überwachung des Archivsystems und der Umgebungsbedingungen
* Regelung zur Datensicherung
* Regelungen zur Protokollierung
* Regelungen im Open Archival Information System (OAIS-Modell - ISO 14721)

### Einweisung in die Administration und Bedienung des Archivsystems (OPS.1.2.2.A11)

Die verantwortlichen Administratoren und Benutzer sind für ihren Aufgabenbereich geeignet und regelmäßig entsprechend dem Dokument ISMS-E2-00007-DE zu schulen.

Die Schulung für die Administratoren umfasst folgende Themen:

* Systemarchitektur und Sicherheitsmechanismen des verwendeten Archivsystems und des darunterliegenden Betriebssystems
* Installation und Bedienung des Archivsystems
* Umgang mit Archivmedien
* Dokumentation der Administrationstätigkeiten
* Eskalationsprozeduren

Die Schulung der Benutzer umfasst folgende Themen:

* Umgang mit dem Archivsystem
* Bedienung des Archivsystems
* Rechtliche Rahmenbedingungen der Archivierung

Die Durchführung und Teilnahme an den Schulungen werden dokumentiert.

### Überwachung der Speicherressourcen von Archivmedien (OPS.1.2.2.A12)

Die auf den Archivmedien vorhandene freie Speicherkapazität sind kontinuierlich zu überwachen. Sobald ein definierter Grenzwert unterschritten wird, erfolgt ein automatisierter Alarm an die verantwortlichen Mitarbeitenden. Es wird darauf geachtet, dass die Alarmierung rollenbezogen erfolgt.

Es sind immer ausreichend leere Archivmedien verfügbar, um Speicherengpässen schnell vorbeugen zu können.

### Regelmäßige Revision der Archivierungsprozesse (OPS.1.2.2.A13)

In der regelmäßigen Revision der Archivierungsprozesse wird überprüft, ob die Archivierungsprozesse noch korrekt und ordnungsgemäß funktionieren. Die Überprüfung enthält folgende Aspekte:

* Fragen zu Verantwortlichkeiten
* Fragen zu Organisationsprozessen
* Fragen zum Einsatz der Archivierung
* Fragen zur Redundanz der Archivdaten
* Fragen zur Administration und der technischen Beurteilung des Archivsystems

Die Auditergebnisse sind nachvollziehbar zu dokumentieren und mit dem Soll-Zustand abzugleichen. Abweichungen werden zeitnah angemessen behandelt.

### Regelmäßige Beobachtung des Marktes für Archivsysteme (OPS.1.2.2.A14)

Der Markt für Archivsysteme wird regelmäßig und systematisch beobachtet.

Bei der Marktbeobachtung werden folgende Kriterien berücksichtigt:

* Veränderungen bei Standards
* Technologiewechsel bei Herstellern von Hard- und Software
* Veröffentlichte Sicherheitslücken oder Schwachstellen
* Verlust der Sicherheitseignung bei kryptografischen Algorithmen

### Regelmäßige Aufbereitung von kryptografisch gesicherten Daten bei der Archivierung (OPS.1.2.2.A15)

Im Rahmen des Betriebes der Archivierung sind die internen Vorgaben zur Kryptographie umzusetzen (siehe Dokument ISMS-E3-00024-DE).

Alle Archivdaten, die mit veralteten oder zukünftig verbotenen kryptografischen Verfahren gesichert werden und über eine geringe Sicherheitseignung verfügen werden rechtzeitig mit sicheren Verfahren neu abgesichert (zum Beispiel Verschlüsselung/Signatur).

### Regelmäßige Erneuerung technischer Archivsystem-Komponenten (OPS.1.2.2.A16)

Die Archivsysteme werden während der gesamten Betriebsphase auf dem aktuellen technischen Stand gehalten. Neue Hard- und Software wird vor der Installation in ein laufendes Archivsystem ausführlich getestet, bevor ein Release im Produktivsystem erfolgt. Wenn neue Komponenten in Betrieb genommen oder neue Dateiformate eingeführt werden, wird ein angemessenes Migrationskonzept erstellt. Darin sind alle Änderungen, Tests und erwartete Testergebnisse zu beschreiben. Die Konvertierung der einzelnen Daten ist zu dokumentieren (Transfervermerk).

Wenn Archivdaten in neue Formate konvertiert werden, ist zu prüfen, ob aufgrund rechtlicher Anforderungen die Daten zusätzlich in ihren ursprünglichen Formaten zu archivieren sind.

### Auswahl eines geeigneten Archivsystems (OPS.1.2.2.A17)

Ein neues Archivsystem wird immer aufgrund der im Archivierungskonzept beschriebenen Vorgaben ausgewählt. Die dort formulierten Anforderungen sind zu erfüllen.

### Verwendung geeigneter Archivmedien (OPS.1.2.2.A18)

Für die Archivierung werden geeignete Medien ausgewählt und benutzt. Dabei sind die Aspekte zu archivierendes Datenvolumen, mittlere Zugriffszeiten und mittlere gleichzeitige Zugriffe auf das Archivsystem zu beachten. Die Archivmedien erfüllen die Anforderungen an eine Langzeitarchivierung hinsichtlich Revisionssicherheit und Lebensdauer.

### Regelmäßige Funktions- und Recoverytests bei der Archivierung (OPS.1.2.2.A19)

Für die Archivierung werden regelmäßige Funktions- und Recoverytests durchgeführt. Die Archivierungsdatenträger werden mindestens einmal jährlich auf Lesbarkeit und Integrität überprüft. Für die Fehlerbehebung werden geeignete Maßnahmen realisiert.

Die Hardwarekomponenten des Archivsystems und die Archivierungsprozesse werden regelmäßig auf ihre einwandfreie Funktion hin geprüft.

## 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).

### Geeigneter Einsatz kryptografischer Verfahren bei der Archivierung (OPS.1.2.2.A20 - CI)

Um lange Aufbewahrungsfristen abdecken zu können, sind Archivdaten nur mit kryptografischen Verfahren auf Basis aktueller Standards und Normen (siehe Dokumente ISMS-E3-00024-DE und ISMS-E4-00001-DE) zu sichern.

### Übertragung von Papierdaten in elektronische Archive (OPS.1.2.2.A21 - CI)

Bei der Überführung von Papierdokumenten und digitalisierten Gegenstände in das elektronische Archiv, wird sichergestellt, dass die digitale Kopie mit dem Originaldokument bildlich und inhaltlich übereinstimmt.