Bundesamt
für Sicherheit in der
Informationstechnik

# Archivierungskonzept

## - Beispiel -

**Stand: September 2004**

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn • Postfach 20 03 63, 53133 Bonn
Tel.: + 49 (0) 1888 9582-0 • Fax: + 49 (0) 1888 9582-400 • Internet: www.bsi.bund.de

**INHALTSVERZEICHNIS**

| A. Sensibilisierung | Verweise auf das IT-Grundschutzhandbuch |
|---|---|

**Hinweis:**

Bemerkungen und Hinweise, an welchen Stellen sich eine individuelle Anpassung oder Ergänzung des Musterkonzeptes besonders empfiehlt, sowie Kommentare sind gelb hinterlegt.

Auch Verweise in andere Muster-Richtlinien oder -Konzepte sind gelb hinterlegt, um Redundanzen unter den Hilfsmitteln gering zu halten. Möglich ist aber auch, dieses Konzepts um die entsprechenden Passagen zu ergänzen.

Bei der Archivierung sind viele technische Randbedingung zu berücksichtigen. Es empfiehlt sich daher, die entsprechenden Maßnahmen des IT-Grundschutzhandbuchs nachzulesen, da technische Abhandlungen oder die Diskussion von elektronischen Signaturen im Archivierungskonzept nicht wiederholt werden.

## 1 Gefährdungslage

Neben der Erzeugung, Bearbeitung und Verwaltung von Dokumenten spielt die dauerhafte (beziehungsweise fristgerechte) Aufbewahrung (Archivierung) eine besondere Rolle: Einerseits müssen Daten/Datenträger bis zum Ablauf einer vorgegebenen Aufbewahrungsfrist verfügbar sein. Andererseits muss deren Vertraulichkeit und Integrität gewahrt bleiben.

Eine ungeeignete Archivierung vorhandener Daten kann erhebliche Auswirkungen auf die spätere Verwendung, deren Wiederfinden und Aufbereitung haben. Es existieren gesetzlich verpflichtende Regelungen beispielsweise des Handels- und Steuerrechts, die einzuhalten sind. So schreiben einzelne Gesetze oder Vorgaben die Aufbewahrungszeit und –form explizit vor.

Es kann überlegt werden, an dieser Stelle die entsprechenden Gesetze zur weiteren Sensibilisierung aufzuführen.

Aber auch andere, interne Erfordernisse machen eine systematische Aufbewahrung/Archivierung notwendig. Es handelt sich hierbei zum einen um Daten/Datenträger, die der internen Bearbeitung dienen. Zum anderen sind dies Daten/Datenträger, die zur späteren Recherche wichtiger Sachverhalte unerlässlich sind. So kann beispielsweise der Verlust oder das Nicht- beziehungsweise verspätete Wiederauffinden wichtiger Informationen/Daten in Behörden und Unternehmen Verwaltungs- und Fachaufgaben verzögern, ineffizient oder gar unmöglich machen.

Dabei können die Gründe für den Verlust archivierter Daten vielfältiger Art sein, wie beispielsweise:

- ungeeignete Lagerung von Archivmedien,
- ungeeigneter Datenträger bei der Archivierung,
- unzureichende Erneuerung von digitalen Signaturen,
- unzulängliche Übertragung von Papierdaten in elektronische Archive,
- unklare Zuständigkeiten und Verantwortung für die Archivierung.

## 2 Zielsetzung

Mit diesem Archivierungskonzept soll das Ziel verfolgt werden, eine schnelle und einfache Aufbewahrung sowie Auffindbarkeit von Daten/Datenträgern sicherzustellen. Der Schutz von Vertraulichkeit, Verfügbarkeit und Integrität soll gewährleistet werden.

Mit Hilfe des Konzepts wird den oben genannten Gefährdungslagen begeg-

| A. Sensibilisierung | Verweise auf das IT-Grundschutzhandbuch |
|---|---|

net, indem sowohl gesetzliche als auch interne Aufbewahrungsnotwendigkeiten berücksichtigt werden.

Dabei ist eine zeitlich unbefristete Aufbewahrung zu vermeiden.

Es ist zu empfehlen, ergänzend ein Datensicherungskonzept zu erstellen. M 6.33

## 3 Begriffliche Definitionen

### *3.1 Archivierung*

Die dauerhafte und unveränderbare Speicherung von Daten und Datenträgern auf eine strukturierte Art wird als Archivierung bezeichnet, so dass ein schnelles und einfaches Wiederauffinden ermöglicht ist.

Es ist zweckmäßig, Archivierung gegenüber Datensicherung abzugrenzen. Bei einer Datensicherung werden Kopien der System- und Nutzdaten angelegt, die nach einer zuvor festgelegten Zeit überschrieben werden. Die gesicherten Daten werden hierbei physikalisch vom IT-System getrennt und gefahrengeschützt gelagert; es ist kein Zugriff aus dem Produktivsystem möglich.

### *3.2 Archivmedien*

Hierbei handelt es sich um diejenigen Datenträger, auf denen die zu archivierenden Daten enthalten sind – d. h. Papierdokumente oder elektronische Datenträger wie CD, DVD oder Magnetbänder, aber auch Mikrofilme. M 4.169

### *3.3 Archive*

Archive sind Orte, an denen Daten/Datenträger aufbewahrt werden. Es kann sich sowohl um einen physischen als auch um einen logischen Ort handeln.

Bei einem physischen Archiv handelt es sich um die Räumlichkeiten, in denen Datenträger archiviert oder in denen Archivssysteme – wie Robotsysteme – untergebracht werden. Es ist nicht erforderlich, dass Räumlichkeiten ausschließlich als Archiv genutzt werden. M 1.60

Es können verschiedene Räume in und außerhalb der Institution dazu genutzt werden – beispielsweise für die Trennung zwischen Kurz- und Langzeitarchiven oder für eine dezentrale Archivierung.

Ein Archivierungsort kann aber auch ein logischer Ort innerhalb eines elektronischen Archivsystems (siehe 3.4) sein, an dem die zu archivierenden Daten gespeichert werden.

### *3.4 Elektronische Archivsysteme*

Hierbei handelt es sich um programmgestützte Systeme, die in automatisierter Weise die geeignete Aufbewahrung elektronisch vorliegender Daten unterstützen.

### *3.5 Dokumentenmanagement-System*

Bei einem programmgestützten Dokumentenmanagement-System handelt es sich um die Schnittstelle zwischen Benutzer (-programmen) und elektronischem Archivsystem. Es sorgt für eine konsistente Verwaltung, Versionierung und Zuordnung von elektronischen Dokumenten. M 2.259

Das Dokumentenmanagement-System kann die Pflege der Index-Datenbank übernehmen, in der die zu den elektronischen Dokumenten archivierte Kontextinformation verwaltet werden.

| A. Sensibilisierung | Verweise auf das IT-Grundschutzhandbuch |
|---|---|
| Darüber hinaus ermöglicht ein Dokumentenmanagement-System die Festlegung von Zugriffsberechtigungen zu den archivierten Daten sowie zur Index-Datenbank. | |

| B. Regelungen | Verweise auf das IT-Grundschutzhandbuch |
|---|---|

## 4 Archivierungsverantwortliche

Verantwortlich für die Umsetzung des Archivierungskonzepts innerhalb eines dezentralen Archivs ist der Informationseigentümer. Hierbei sind Vorgaben der Institutionsleitung zu berücksichtigen.

Für das zentrale Archiv (physisches Archiv und programmgestütztes Archivsystem) ist die Institutionsleitung verantwortlich.

Jeder Mitarbeiter ist für die Einhaltung des Archivierungskonzepts und die korrekte Aufbewahrung der Daten/Datenträger verantwortlich. Sie sind auf die Einhaltung des Archivierungskonzepts zu verpflichten.

Für das Archivsystem und jeden Archivierungsort ist eine Person vom Informationseigentümer bzw. Institutionsleitung zu bestimmen, der für die Einhaltung der Rahmenbedingungen einer ordnungsgemäßen Archivierung verantwortlich ist. Des Weiteren ist ein Vertreter zu benennen. — M 3.3

Der Archivierungsverantwortliche hat zu gewährleisten, dass zum einen genügend Raum/Speicherplatz für die zu archivierenden Datenträger und zum anderen dass die für die Archivierung notwendige Ausstattung vorhanden ist, wie beispielsweise Regale oder abschließbare Schränke und hat die notwendigen Sicherheitsmaßnahmen sicherzustellen (siehe Abschnitt C).

Des Weiteren hat er

- die Schulung der betreffenden Mitarbeiter sicherzustellen,
- regelmäßig eine Revision des Archivierungsprozesses durchzuführen (siehe Kapitel 9), — M 2.260
- Marktbeobachtung und kontinuierliche Information, — M 2.261 und M 2.35
- den Betrieb des Archivierungssystems (siehe Kapitel 15) sowie
- eventuelle Einbettung in Dokumentenmanagement-System sicherzustellen. — M 2.259

Die Verantwortlichen sind auf Verschwiegenheit bezüglich der Dateninhalte zu verpflichten und es ist gegebenenfalls eine Verschlüsselung in Betracht zu ziehen. — M 3.2, M 2.164

## 5 Aufbewahrungsfristen

Die minimale und maximale Aufbewahrungszeit (Aufbewahrungsfristen) ist durch den Informationseigentümer festzulegen. Zuvor sind von der Institutionsleitung diejenigen Daten/Datenträger festzulegen, die zu archivieren sind.

Die zu archivierenden Daten/Datenträger und deren Fristen sind innerhalb einer Übersicht zu dokumentieren.

Hierbei sind die gesetzlichen und die organisations-internen Anforderungen zu berücksichtigen. Existieren unterschiedliche Fristen, ist die jeweils längste zu wählen.

Bei der Festlegung ist folgendes zugrunde zu legen:

- Die Daten/Datenträger sind mindestens so lange aufzubewahren, wie es gesetzlich vorgeschrieben ist.
- Sie sind aber maximal so lange aufzubewahren, wie es ein jeweils festzulegendes Institutionsinteresse verlangt.

Den organisations-internen Aufbewahrungsnotwendigkeiten dürfen keine gesetzlichen Aufbewahrungsverboten beziehungsweise Vernichtungsgeboten entgegenstehen.

| B. Regelungen | Verweise auf das IT-Grundschutzhandbuch |
|---|---|

## 6 Auswahl eines elektronischen Archivierungssystems

Es sind Mindestanforderungen an das einzusetzende elektronische Archivsystem vom Archivverantwortlichen zu definieren. M 4.168

Bevor eine Entscheidung getroffen werden kann, welche Verfahren und Produkte für die elektronische Archivierung eingesetzt werden sollen, sind die nachfolgenden Einflussfaktoren zu ermitteln und Anforderungen an das Archivsystem abzuleiten.

Zertifizierte Produkte sind nicht-zertifizierten vorzuziehen.

### *6.1 Technische Einflussfaktoren bei der Auswahl*

Es sind die Eigentümer der zu archivierenden Daten (Informationseigentümer) zu befragen, die einen genauen Überblick über den jeweiligen Geschäftsprozess haben.

Die für die elektronische Archivierung maßgeblichen technischen Einflussfaktoren sind unter anderem M 2.244

- das zu erwartendes Datenaufkommen,
- die Dateiformate der zu archivierenden Daten/Datenträger (siehe auch Kapitel 7.3),
- das Änderungsvolumen und die Versionierung,
- die Aufbewahrungsdauer und -form der Daten/Datenträger,
- die Zahl und Art der Zugriffe,
- die Alterungsprozesse und -auswirkungen von Archivmedien,
- die vorhandene IT-Einsatzumgebung sowie
- die zu beachtenden Normen und Standards.

Die von den Einflussfaktoren abgeleiteten Anforderungen sind im Einzelnen festzulegen und zu dokumentieren.

Die festgelegten Anforderungen wirken sich auch auf die Auswahl der Archivmedien und der Speicherlaufwerke aus und beeinflussen die Auswahl und Dimensionierung von Cache-Komponenten.

Bereits bei der Planung ist zu berücksichtigen, dass die eingesetzten Archivsysteme und -medien im Lauf der Zeit technologisch und physikalisch veralten beziehungsweise altern werden.

### *6.2 Rechtliche Einflussfaktoren bei der Auswahl*

Es sind durch den Informationseigentümer die relevanten Gesetze zu erheben und den entsprechenden Daten/Datenträger zuzuordnen.

Die Gesetze regeln neben den Aufbewahrungsfristen auch die Aufbewahrungsformen. Diese haben auch Einfluss bei der Auswahl der Technik wie Archivsystem, Archivmedien etc.

M 2.245

Die rechtlichen Einflussfaktoren betreffen unter anderem

- die Mindestaufbewahrung aus steuerlichen, haushaltsrechtlichen oder sonstigen Gründen (siehe Kapitel 5),
- die Höchstaufbewahrungsdauer aus Datenschutzgründen,
- die Zugriffsrechte für Externe, wie z. B. Steuerbehörden, sowie
- die Qualität von digitalen Signaturen (so wird beispielsweise durch die ZPO geregelt, unter welchen Umständen Dokumente als Urkunde anerkannt werden müssen: Aufgrund einer eigenhändigen Unterschrift oder einer qualifizierten digitalen Signatur).

| B. Regelungen | Verweise auf das IT-Grundschutzhandbuch |
|---|---|

Die gesetzlichen Regelungen sind innerhalb einer Übersicht durch den Informationseigentümer zu führen.

### *6.3 Organisatorische Einflussfaktoren bei der Auswahl*

Des Weiteren sind die organisatorischen Einflussfaktoren zu ermitteln, die bei der Konzeption und der Auswahl des Archivsystems zu berücksichtigen sind. Dazu gehören unter anderem M 2.246

- die Archivierungsfristen (siehe Kapitel 5)
- der Vertraulichkeits-, Verfügbarkeits-, Integritäts-, und Authentizitätsbedarf der Daten,
- die finanziellen Randbedingungen
- der Rekonstruktionsaufwand,
- der Personalaufwand,
- der Zeitraum des Einsatzes des Archivsystems,
- die Festlegung akzeptabler Antwortzeiten,
- die Kenntnisse und die IT-spezifischen Qualifikationen der Benutzer,
- die Ergonomie und Bedienfreundlichkeit des Archivsystems,
- die Einhaltung von Standards und Normen.

Die organisatorischen Einflussfaktoren sind im Einzelnen schriftlich festzulegen.

## 7 Gestaltung der Archivierung

### *7.1 Archivräume und Lagerbedingungen*

Da in Archiven oftmals sensitive Daten konzentriert aufbewahrt werden, sind nur Räume als Archive zu nutzen beziehungsweise auszuwählen, die einen ausreichenden Schutz sicherstellen. Analog gilt dies für das elektronische Archivsystem. M 1.60 M 1.8

Das Schutzniveau der Archive ist abhängig von der Klassifizierung der zu archivierenden Informationen zu wählen (siehe „Sicherheitsrichtlinie zur IT-Nutzung“). M 2.217

Es sind u. a. Brandschutz, elektronische Versorgung, ausreichende Speicherkapazitäten und Klimatisierung zu regeln. M 1.6 M 1.27

Für den Langzeiteinsatz von Archivmedien sind die klimatische Lagerbedingungen zu überwachen. M 1.27 M 2.18

Es sind die verbindlichen Empfehlungen von Herstellern zu den mechanischen Lagerbedingungen einzuholen und zu beachten.

Papier ist idealerweise bei einer Temperatur von ca. 20 °C und bei einer Luftfeuchtigkeit von 40 % aufzubewahren.

CDs und DVDs sind idealerweise bei einer Temperatur zwischen 4 °C und 20°C und bei einer Luftfeuchtigkeit von 20 % und 50 % aufzubewahren. Für eine Langzeitlagerung ist 18 °C und 40 °C Luftfeuchtigkeit ideal.

Bei anderen Medien (wie Magnetbändern oder Mikrofilmen) sind die Herstellerangaben zu beachten.

### *7.2 Nutzung geeigneter Archivmedien*

Es sind für den verfolgten Archivierungszweck adäquate Archivmedien auszuwählen und festzulegen. Für die Auswahl sind folgende Aspekte zu berücksichtigen: M 4.169

| B. Regelungen | Verweise auf das IT-Grundschutzhandbuch |
|---|---|

- zu erwartendes Datenvolumen der Archivierung
- notwendige Zugriffszeiten
- Anzahl gleichzeitiger Zugriffe
- durch das Archivmedium abzudeckende Aufbewahrungsfristen
- Notwendigkeit der revisionssicheren Speicherung

### *7.3 Nutzung geeigneter Datenformate*

Für die Archivierung elektronischer Dokumente sind geeignete Datenformate zu wählen. Ziel ist es, auch langfristig eine originalgetreue Reproduktion der Archivdaten sowie ausgewählter Merkmale des ursprünglichen Dokumentmediums zu ermöglichen. Dabei ist der Einsatzzweck der archivierten Daten und ihren Ursprungsmedien der Auswahl zugrunde zu legen. M 4.170

Für die Wahl geeigneter Datenformate sind folgende Kriterien maßgeblich:

- das Datenformat sollte möglichst langfristige Relevanz haben,
- das Dokumentstruktur sollte eindeutig interpretiert werden können,
- der Dokumenteninhalt sollte elektronisch weiterverarbeitet werden können,
- die Beachtung gesetzlicher Vorschriften,
- die Grammatik und die Semantik des Datenformates muss ausführlich dokumentiert sein, so dass eine spätere Migration problemlos möglich ist und
- die Merkmale des Originaldokuments (elektronisch oder in Papierform) sollen später eindeutig nachweisbar sein, auch wenn das Originaldokument nicht mehr vorhanden ist.

Da im Vorfeld meist nicht absehbar ist, welche Merkmale des Originaldokuments bei einer späteren Reproduktion nachgewiesen werden sollen und mit welcher Nachweiskraft dies erfolgen soll, sind die Daten/Dokumente möglichst in mehreren elektronischen Datenformaten gleichzeitig zu archivieren. Dadurch kann eine möglichst hohe Überdeckung der Merkmale des Originaldokuments erreicht werden.

Sofern die elektronische Archivierung von in Papier vorliegender Daten/Datenträger sinnvoll erscheint, sind diese in geeignetes Datenformat zu transformieren (Einscannen, Mikroverfilmung). Für diesen Transformationsprozess sind genaue Organisationsanweisungen festzulegen, die

- das berechtigte Personal,
- den Zeitpunkt der Transformierung und Vernichtung sowie
- den Übereinstimmungsgrad mit dem Original (bildliche oder inhaltliche Wiedergabe) als auch
- die Qualitätskontrolle (Lesbarkeit, Vollständigkeit) regeln.

### *7.4 Aufbewahrungsstruktur*

Grundlage für ein einfaches und schnelles Wiederauffinden wichtiger Daten/Datenträger ist:

- ein Archivierungskatalog, in dem Aufbewahrungsfristen und -formen der einzelnen Daten/Datenträger geführt werden,
- einheitliche Aufbewahrungsstruktur
- sonstige Hilfsmittel, wie beispielsweise Lagepläne oder Indizierung.

Bei einer sogenannten „chaotischer Lagerung“ sollte geprüft werden, inwiefern ein sogenanntes Retrieval-Programm für ein schnelles Wiederauffinden genutzt werden sollte.

Die Datenträger sind eindeutig zu kennzeichnen.

| B. Regelungen | Verweise auf das IT-Grundschutzhandbuch |
|---|---|

Sofern unterschiedliche Fassungen eines Dokuments vorliegen, ist dies mehrfach abzuspeichern (Versionierung).

Die lokale Archivierung von Daten/Datenträgern ist weitestgehend zu vermeiden. Ausnahmen sind zulässig, wenn hierzu ein zwingendes Erfordernis vorliegt.

Bei papierenen Datenträgern gilt darüber hinaus, dass Datenträger, die sich auf einen Sachverhalt beziehen, innerhalb von Ordnern zusammenzufassen sind. Bei umfangreichen Ordnern sind innerhalb der Ordner Unterordner zu bilden, in denen Schriftstücke eines bestimmten Zeitraums abgelegt werden. Innerhalb der Akte beziehungsweise des Bandes sind die Schriftstücke chronologisch nach dem Erstellungsdatum geordnet zu sortieren.

Daten/Datenträger, auf die innerhalb eines Zeitraums von zwei Jahren nicht mehr zugegriffen wurde, sind auszulagern.

### *7.5 Indizierung*

Abgelegte Dokumente und Datensätze sind eindeutig so zu indizieren, dass sie bei späteren Archivanfragen korrekt wiedergefunden werden können. M 2.258

Struktur und Umfang der Indexangaben haben folgende Eigenschaften aufzuweisen:

- *Eindeutigkeit*
  Die Dokumentenbezeichner müssen eindeutig sein.
- *Unterstützung zu erwartender Suchanfragen*
  Da der spätere Suchkontext nicht feststeht, kann im Vorfeld nur eine Abschätzung späterer Suchanfragen vorgenommen und versucht werden, die Kontextangaben so aussagekräftig wie möglich zu gestalten.
- *Geringer Umfang*
  Ein geringer Umfang an Indexdaten beschleunigt spätere Suchanfragen, jedoch kann ein zu geringer Umfang der Indexdaten Suchanfragen behindern beziehungsweise das Auffinden von Dokumenten erschweren.

Diese Parameter sind sorgfältig vor der Inbetriebnahme des Archivs festzulegen, da eine nachträgliche Änderung sehr aufwändig ist: Die Archivdatenbestände müssen neuindiziert werden.

Es ist eine halbautomatische Erzeugung der Indexdaten bei größeren Datenvolumen zu bevorzugen. Dieses Verfahren vergibt die Indexdaten automatisiert, es kann jedoch manuell kontrolliert und korrigiert werden.

Alternative Verfahren sind möglich:

- *manuelle Erstellung:*
  Es werden Indexangaben zu jedem Dokument manuell erzeugt. Hierdurch besteht besonders bei großen Datenmengen die Gefahr, dass inkonsistente Indexangaben erfasst werden.
- *vollautomatische Erzeugung:*
  Hierbei werden Dokumentindizes vollautomatisch ohne manuelle Eingriffsmöglichkeit vergeben. Fehler können dabei nicht erkannt beziehungsweise korrigiert werden.

### *7.6 Entnahme aus Archiven*

Wird ein Dokument oder ein Datenträger aus seinem vorgeschriebenen Archiv temporär entnommen, so ist hierfür ein Vermerk zu hinterlassen.

| B. Regelungen | Verweise auf das IT-Grundschutzhandbuch |
|---|---|

Es ist darauf zu achten, dass aus dem Archiv entnommene Datenträger beim Transport in andere Räumlichkeiten keinen großen Klimaschwankungen (insbesondere Temperatur und Luftfeuchtigkeit) ausgesetzt werden.

Darüber hinaus sind die allgemeinen Regelungen zum Datenträger-Transport beziehungsweise der Datenübermittlung einzuhalten, um einen sicheren Transport/sichere Übermittlung zu gewährleisten (siehe „Sicherheitsrichtlinie für die IT-Nutzung“).

Des Weiteren gelten die Regelungen zu den Zutritts- und Zugangsrechten (Kapitel 12) analog auch für Daten/Datenträger, die aus den Archiven entnommen wurden.

### *7.7 Vernichtung/Löschung*

Es ist zu prüfen, wann Unterlagen ohne Beeinträchtigung gesetzlicher oder interner Interessen vernichtet werden können. Hierbei sind die Maximal-Aufbewahrungsfristen der Entscheidung zugrunde zu legen (siehe Kapitel 5).

Folgende Tatbestände können eine Vernichtung von Daten/Datenträger erforderlich machen:

*(1)* *Es existiert eine gesetzliche Vorschrift, die es zwingend vorschreibt, bestimmte Unterlagen zu vernichten.*
Hierbei sind die relevanten Gesetze (insbesondere Datenschutz) zu beachten. Bei der Bestimmung der vernichtungspflichtigen Daten/Datenträger ist bei personenbezogenen Daten der Datenschutzbeauftragte einzubeziehen und es sind die datenschutzrechtlichen Vorgaben bei der Vernichtung zu beachten.

*(2)* *Die gesetzliche und/oder die betriebliche Aufbewahrungsnotwendigkeit fällt weg.*
Sobald keine Erfordernis zur Aufbewahrung vorliegt, sind die Unterlagen zu vernichten.
Eine Vernichtung ist insbesondere aus folgenden Beweggründen notwendig:
- Entlastung von Unternehmensressourcen durch Archivräume, -schränke und/oder Speicherplatz.
- „Aufgeräumte“ Archive vereinfachen i. d. R. ein Retrieval der Unterlagen.

Werden papierene Dokumente in ein anderes Format transformiert, sind die papierenen Datenträger danach zu vernichten – sofern die Aufbewahrung des Originals beispielsweise aufgrund rechtlicher Anforderungen nicht verlangt wird.

Es ist entsprechend des zu löschenden Datenträgers und seines Schutzbedarfs eine geeignete Löschmethode zu wählen. Der Aufwand, um Restdaten restaurieren zu können, steigt in folgender Reihenfolge: M 2.167
- durch Löschkommandos,
- durch Formatieren,
- durch Überschreiben oder
- durch Zerstörung des Datenträgers.

Für öffentliche Einrichtungen ist die Anbietungspflicht an die Landesarchive vor der Vernichtung zu prüfen.

| B. Regelungen | Verweise auf das IT-Grundschutzhandbuch |
|---|---|

## 8 Einbettung in Dokumentenmanagement-System

Sofern große Datenbestände zu verwalten sind, ist der Einsatz eines übergeordneten Dokumentenmanagement-Systems (DMS) zu prüfen. M 2.259

Dokumentenmanagement-Systeme müssen in geeigneter Weise eingesetzt und in die Organisation eingebettet werden. Hierzu sind entsprechende Organisationsprozesse zu definieren. Regelungsbedarf besteht unter anderem hinsichtlich folgender Punkte:

- Einstellen von Dokumenten ins DMS,
- Nutzung des DMS beim Umgang mit Dokumenten,
- Verantwortlichkeiten für Nutzung und Betrieb des DMS,
- Rechtevergabe und Zuständigkeit hierfür,
- Anforderungen an den Betrieb des DMS.

Es ist auf eine Kompatibilität von Dokumentenmanagement- und Archivsystemen zu achten.

## 9 Revision

Der Prozess der Archivierung ist regelmäßig einer Revision zu unterziehen. Dabei ist die Korrektheit und Ordnungsmäßigkeit zu prüfen und daraus die korrekte und authentische Ablage der Daten im Archivsystem abzuleiten. M 2.260

Alle Maßnahmen am Archivsystem sind revisionssicher zu dokumentieren. Administratortätigkeiten sind zu protokollieren. M 4.172

Es ist eine regelmäßige Kontrolle der Funktionalität des Systems, der IT-Sicherheit und der Einhaltung der Richtlinien durchzuführen. Hierzu sind neben der technischen Beurteilung des Archivsystems (siehe Kapitel 15.4 und 15.5) Fragen zu folgenden Aspekten zu klären: M 2.263 und M 4.173 M 2.260

- Verantwortlichkeiten, wie z. B.
  - Benennung der verantwortlichen Personen
  - Einweisung in ihre Aufgaben
  - Schriftliche Dokumentation
  - Vertretungsregelungen
- Organisationsprozess, wie z. B.
  - Organisationsweite Regelungen zum Einsatz elektronischer Archivsysteme
  - Dokumentation der zu archivierenden Daten/Datenträger
  - Regelung und Dokumentation der Sicherheitsanforderungen an die Daten/Datenträger
  - Anpassung der Regelungen an aktuelle Entwicklungen
- Einsatz der Archivierung, wie z. B.
  - Eindeutige Regelungen hinsichtlich zu archivierenden Daten/Datenträger
  - Dokumentierte Regelungen hinsichtlich der Kontextangaben für archivierte Daten/Datenträger
  - Einhaltung der Anforderungen an die Vertraulichkeit, Authentizität und Integrität der zu archivierenden Dokumente
- Redundanz der Archivdaten, wie z. B.
  - Ausreichende Redundanz der Archivdaten
  - Regelmäßige Datensicherung der Archivsysteme (siehe 14)
- Administration, wie z. B.
  - Ordnungsgemäße Vernichtung beziehungsweise Entsorgung nicht mehr benötigte, beschriebene Archivmedien

| B. Regelungen | Verweise auf das IT-Grundschutzhandbuch |
|---|---|
| - Im geforderten Maße vorzuhaltende Lesegeräte und Speichermedien | |
| Es sind die sicherheitsrelevanten Ereignisse und Zugriffe auf sensitive Bereiche möglichst automatisch zu protokollieren und durch den Administrator regelmäßig zu überprüfen. | M 4.106<br>M 2.64 |
| Bei der Protokollierung sind Datenschutzaspekte zu beachten. Ermöglicht die Auswertung der Daten eine Verhaltens- und Leistungskontrolle, ist sie mitbestimmungspflichtig. | |
| Die Revision sollte auch eine technische Neubewertung der Archivsystem-Komponenten und der verwendeten Datenformate beinhalten. Hierdurch soll gewährleistet werden, dass technische Weiterentwicklungen frühzeitig erkannt werden und technische Änderungen am Archivsystem selbst durch den Hersteller im Vorfeld bekannt sind (siehe Kapitel 15.5). | |
| Die Prüfergebnisse der Revisionen sind ebenfalls gemäß den Anforderungen an den Archivierungsprozess selbst zu archivieren. | |
| **10 Schulungen** | |
| Die Mitarbeiter sind hinsichtlich der Bedeutung der Archivierung zu schulen und zu sensibilisieren. | M 3.34 und M 3.35 |
| Die betreffenden Mitarbeiter sind in der Durchführung der notwendigen Maßnahmen zu schulen. Dies umfasst unter anderem<br>▪ die korrekte Archivierung inkl. Aufbewahrungsfristen,<br>▪ die Wahl und Nutzung der Archivmedien,<br>▪ die Zugriffsberechtigungen auf das Archivsystem,<br>▪ die Nutzung des Archivsystems,<br>▪ die Indizierung der Daten/Datenträger,<br>▪ die Aufbewahrung und Dokumentation der Archivmedien. | |
| Die Schulungen sind in das gesamte Schulungskonzept der Institution einzubinden. | M 3.26 |
| **11 Regelmäßige Aktualisierung des Archivierungskonzepts** | |
| Das Archivierungskonzept ist regelmäßig zu überprüfen und bei Bedarf an die aktuellen Gegebenheiten anzupassen. Dies kann durch veränderte interne oder gesetzliche Anforderungen, durch eine gestiegener Gefährdungslage oder durch geänderte technische Rahmenbedingungen verursacht werden. | |

| C. Sicherheitsmaßnahmen | Verweise auf das IT-Grundschutzhandbuch |
|---|---|
| **12 Zutritts- und Zugriffsrechte** | |
| Unbefugten ist der Zutritt zu den Archiven zu verwehren. | M 2.6 und M 2.17 |
| Weiterhin ist zu verhindern, dass Unberechtigte Daten/Datenträger lesen, kopieren, verändern und/oder entfernen. | |
| Für jeden einzelnen Mitarbeiter sind Berechtigungen für den Zugriff auf die archivierten Daten festzulegen. Alle Rechte sind restriktiv zu vergeben und zu dokumentieren. Hierbei sind die zwingenden dienstlichen Erfordernisse zugrunde zu legen. | M 2.8<br>M 2.31 |
| Die Zugriffe auf elektronische Archive sind zu protokollieren. Dies macht Aktivitäten nachvollziehbar und ermöglichen eventuelle Fehlerkorrekturen. | M 4.172 |
| Es sind darüber hinaus die Regelungen der „Sicherheitsrichtlinie zur IT-Nutzung“ zu beachten. | |
| **13 Digitale Signatur und Kryptographie** | |
| Kryptographische Verfahren und digitale Signaturen sind für die elektronische Archivierung einzusetzen, wenn dies erforderlich ist. | M 2.161 und 4.34 |
| Technisch bedingt haben digitale Signaturen eine begrenzte Lebensdauer, die vorher nicht immer bekannt ist. | M 2.265 |
| Um beurteilen zu können, ob ein Algorithmus weiterhin zuverlässig und ausreichend sicher ist, sind die Entwicklungen auf dem Gebiet der Kryptographie durch den Archivverantwortlichen kontinuierlich zu beobachten. Darüber hinaus sind einschlägige Informationsquellen laufend dahingehend auszuwerten, ob Möglichkeiten bekannt werden, bestehende Verfahren zu kompromittieren. | M 2.35 und M 2.261 |
| Bei Aufbewahrungsfristen von 10 Jahren und länger ist davon auszugehen, dass verschlüsselte oder signierte Daten wiederholt mit neuen Schlüsseln und gegebenenfalls auf Basis neuer Algorithmen umgeschlüsselt werden müssen. | |
| Wenn die verwendeten Kryptoverfahren nicht mehr zeitgemäß sind und daher die Vertraulichkeit oder Integrität der verschlüsselten Daten nicht mehr sichergestellt werden kann, müssen die Daten neu verschlüsselt beziehungsweise signiert werden. Zu diesem Zweck ist Kapitel 15.5 zu beachten. | M 2.264 und M 2.266 |
| Nach der Neuverschlüsselung und erneuten Archivierung sind die alten Datenbestände zuverlässig zu vernichten (siehe Kapitel 7.7) | M 2.13 |
| **14 Datensicherung** | |
| Elektronische Archivsysteme unterliegen denselben Risiken hinsichtlich eines Datenverlustes wie andere IT-Systeme auch. Eine redundante Speicherung der Archivdaten, der zugehörigen Index-Datenbank und der Systemdaten ist daher unerlässlich. | M 4.171 |
| Ergänzend zu einer Datensicherung der Archivdaten kann auch eine redundante Speicherung auf physikalisch getrennten und in unterschiedlichen Brandabschnitten aufgestellten Archivsystemen erfolgen (Spiegelung). | M 6.84 |
| Das Datensicherungskonzept ist zu beachten. | M 6.33 |

| C. Sicherheitsmaßnahmen | Verweise auf das IT-Grundschutzhandbuch |
|---|---|

## 15 Sicherstellung des Betriebs des Archivsystems

### *15.1 Grundsätze der elektronischen Archivierung*

Für eine ordnungsgemäße Archivierung muss über den gesamten Archivierungszeitraum hinweg sichergestellt werden, dass

- das benutzte Datenformat dem Stand der Technik entspricht und von den verwendeten Anwendungen derzeit und zukünftig verarbeitet werden kann,
- die gespeicherten Daten auch zukünftig lesbar sind und unter Beibehaltung der Semantik und der Nachweiskraft reproduziert werden können,
- das benutzte Dateisystem auf dem Speichermedium von allen beteiligten Komponenten verarbeitet werden kann,
- die Archivmedien jederzeit physikalisch einwandfrei gelesen werden können,
- die verwendeten kryptographischen Verfahren zur Verschlüsselung und zur digitalen Signatur dem Stand der Technik entsprechen und
- für alle Komponenten der Speichereinheit (Archivmedien, Laufwerke, Jukeboxen sowie die Steuersoftware) Ersatz- und Wartungsmöglichkeiten bestehen.

### *15.2 Überwachung der Speicherressourcen*

Die auf dynamisch angelegten Archivmedien vorhandene, freie Speicherkapazität ist kontinuierlich zu überwachen. Wenn die freie Speicherkapazität unter den festzulegenden Schwellenwert sinkt, hat eine Benachrichtigung des Administrators zu erfolgen. Sinkt die freie Speicherkapazität weiter unter einen kritischen Grenzwert, sollte eine Alarmierung ausgelöst werden. M 2.257

Der Schwellenwert ist bei einer Restkapazität von 15 % der Gesamtkapazität des Speichermediums und für den kritischen Grenzwert eine Restkapazität von 10 % zugrunde zu legen.

Die Alarmierung hat rollenbezogen zu erfolgen, so dass sie unabhängig von konkreten Personen ist und auch im Krankheitsfall oder bei Urlaub Alarmierungen wahrgenommen werden. M 3.3

Wenn der kritische Alarm ausgelöst wird, muss gewährleistet sein, dass für eine hinreichende Zeit weiterhin das durchschnittliche Datenaufkommen archiviert werden kann.

Um etwaige Lieferengpässe bei Archivmedien zu überbrücken, sollte eine ausreichende Zahl leerer Archivmedien an einem bekannten Ort gelagert werden. Es ist Kapitel 7.1 zu beachten. M 1.60

Für den Fall der Alarmierung ist zu dokumentieren, in welcher Weise und in welchem Zeitraum eine Reaktion auf die Alarme erfolgen soll. Falls der Betrieb des Archivsystems durch Dritte erfolgt, ist dies vertraglich zu regeln (Service Level Agreements (SLAs)). Hierbei ist die „Sicherheitsrichtlinie für das Outsourcing von IT-Leistungen“ zu beachten. M 2.253

Neben dem Speicherplatz müssen auch betriebssystem- oder anwendungsspezifische Restriktionen überwacht werden. Die entsprechenden Programmdokumentationen müssen daraufhin geprüft werden. Beispielsweise können die Anzahl der maximal zugelassenen Dateien pro Verzeichnis oder die maximal erlaubten Datenbankeinträge überschritten werden, so dass keine weiteren Daten auf dem Speichermedium angelegt werden können. M 2.257

| C. Sicherheitsmaßnahmen | Verweise auf das IT-Grundschutzhandbuch |
|---|---|

### *15.3 Wartung*

Durch regelmäßige Wartungsarbeiten ist das Archivsystem vor Störungen zu bewahren. Bei elektronischen Archiven sollten diese Arbeiten in die übrigen Wartungsarbeiten der IT eingebunden werden. Im Anschluss an die Wartungs- oder Reparaturarbeiten ist die ordnungsgemäße Funktion der gewarteten Anlage zu überprüfen. M 2.4 M 2.62

Arbeiten am System sind gegenüber den betroffenen Mitarbeitern rechtzeitig anzukündigen.

Die Wartung des Archivsystems hat sich an den allgemeinen Regelungen zur Wartung innerhalb der Institution zu orientieren (siehe „Sicherheitsrichtlinie zur IT-Nutzung“).

### *15.4 Regelmäßige Tests*

Unabhängig von der Art des gewählten Archivmediums sollte grundsätzlich nach der Speicherung eine Verifikation durchgeführt werden. Zum einen sollte diese durch das System erfolgen, um zu überprüfen, ob ein genaues Abbild der zu speichernden Daten angelegt wurde. Zum anderen sollte stichprobenartig immer wieder durch den Archivverantwortlichen geprüft werden, ob auch alle für die Archivierung vorgesehen Daten archiviert und nicht durch Fehlkonfigurationen übersehen wurden. M 1.60 und M 2.263f

Durch regelmäßig Funktions- und Recovery-Tests ist einem Datenverlust auf den Datenträgern entgegen zu wirken. Bei dieser Prüfung kann sich herausstellen, dass technische Komponenten des Archivsystems geändert werden müssen (siehe hierzu 15.5). M 4.173

Der Archivierungsvorgang selbst kann fehlerhaft verlaufen. Einmal pro Tag ist daher zu überprüfen, ob alle Archivierungsprozesse fehlerfrei abgelaufen sind. Dies kann durch Auswertung von Log-Dateien sowie stichprobenartige Ansicht der erstellten Archivmedien durch den Administrator geschehen. Mögliche Ursachen können sein:

- Konfigurationsfehler,
- Softwarefehlfunktionen (z. B. beim Einsatz neuer Programme),
- Probleme mit den Archivmedien oder
- Änderungen und Fehler in der Ablaufsteuerung.

Die Index-Datenbank ist zudem regelmäßig (mindestens wöchentlich) zu prüfen, ob sie konsistent und integer ist. M 4.171

In regelmäßigen Abständen (mindestens monatlich) ist darüber hinaus zu prüfen, ob die Datensicherungen der Index-Datenbank lesbar und wiederverwendbar sind. Alle Ergebnisse der regelmäßigen Integritätsprüfung sollten ebenfalls archiviert werden, damit Datenänderungen später nachvollzogen werden können.

### *15.5 Regelmäßige Erneuerung des Archivsystems*

Ist abzusehen, dass eine der geforderten Eigenschaften in naher Zukunft nicht mehr gegeben ist, müssen die betroffenen Systeme ausgetauscht werden. Dabei ist zu berücksichtigen, dass unter Umständen eine erhebliche Menge an archivierten Daten auf neue Datenträger kopiert werden muss. M 2.266

Es ist sicherzustellen, dass Hard- und Software auch für veraltete Formate zur Rekonstruktion zur Verfügung stehen.

Neue Hard- und Software ist vor der Installation in ein laufendes Archiv-

| C. Sicherheitsmaßnahmen | Verweise auf das IT-Grundschutzhandbuch |
|---|---|
| system grundsätzlich ausführlich zu testen. Es muss sichergestellt werden, dass ausgetauschte Komponenten, z. B. Laufwerke, Archivmedien, Betriebssoftware, einwandfrei mit allen anderen Komponenten unter Beibehaltung der für den Betrieb notwendigen Funktionalität zusammenarbeiten. | M 2.266 |
| Vor der Inbetriebnahme neuer Komponenten oder der Einführung neuer Datenformate ist ein Migrationskonzept zu erstellen, in dem alle Änderungen und Tests beschrieben werden. | M 2.243 |