**Inhaltsverzeichnis**



# 0 Dokumenteninformation

## *0.1 Inhalt des Dokuments*

Diese Richtlinie legt Regeln für die Löschung von digitalen Daten sowie die Vernichtung und Entsorgung von Datenträgern jeglicher Art fest.

## *0.2 Verlaufshistorie*

| Version | Datum | Wer | Kapitel | Änderung |
|---|---|---|---|---|
| | 08.04.22 | Dr. Kathrin Stollenwerk | Ersterstellung auf Basis des Dokuments UKT_ISMS_01.035_Entsorgung von Informtionen.docx und in das neue Format überführt | |
| | 06.09.23 | Christian Meier | KVP Anmerkung umgesetzt: Auf Seite 7 und 8 gibt es Verweise auf „Anforderungen aus Kapitel 0“ das es nicht gibt - die Verlaufshistorie passt nicht mit dem Stand überein - Bei Aufzählungen und in Tabellen ist die Schrift größer als im Text, auch bei Referenzen | |

## *0.3 Veröffentlichung*

| Nr. | System | Pfad | Format |
|---|---|---|---|
| | roXtra | Informationssicherheit | Word |

Aus Gründen der leichteren Lesbarkeit wird in den Beschreibungen auf eine geschlechtsspezifische Differenzierung, wie z. B. Teilnehmer/Innen, verzichtet. Es wird durchgängig die männliche Form benutzt. Im Sinne des Gleichbehandlungsgesetzes sind diese Bezeichnungen als nicht geschlechtsspezifisch zu betrachten und gelten gleichermaßen für alle Geschlechter.

# 1 Informationen zu dieser Richtlinie

## *1.1 Ziel und Zweck*

Im Lebenszyklus von Informationen auf Datenträgern stellt das Löschen und Vernichten dieser Informationen einen wesentlichen Bestandteil dar. Werden Datenträger ausgesondert, auf denen sich noch nicht sicher gelöschte Informationen befinden, so kann es zu einer ungewollten Offenlegung von vertraulichen Inhalten kommen.

Ziel der vorliegenden Richtlinie ist daher die Festlegung von angemessenen, dem Stand der Technik entsprechenden Schutzmaßnahmen, die ein informationssicherheitskonformes Löschen von digitalen Daten sowie Vernichten und Entsorgen von Datenträgern im Anwednungsbereich der Richtlinie gewährleisten.
Damit soll verhindert werden, dass:

- Daten unbeabsichtigt verloren gehen oder gelöscht werden,
- Daten auf zu entsorgenden Datenträgern unbeabsichtigt zurückbleiben und dass
- Daten bei der Weiter- oder Wiederverwendung von Datenträgern unbeabsichtigt an Unbefugte weitergegeben werden.

Unter dem Begriff Datenträger werden in dieser Richtlinie sowohl analoge Datenträger als auch digitale Datenträger zusammengefasst. Die folgende Tabelle gibt einen Überblick über Datenträgertypen, wobei sich die verwendeten Bezeichnungen an der DIN 66399 (siehe [3]) orientieren.

| Kürzel | Materialklasse | Datenträgertyp |
|---|---|---|
| P | Papier | Briefe, Akten, Verträge, Formulare, Notizzettel, Ausdrucke, Umschläge, Aufkleber, Etiketten, Faxe, Bilder |
| F | Film | Filme, Mikrofilme, Folien |
| O | Optischer Datenträger | CDs, DVDs, Blu-Ray-Discs, Optische Bänder |
| T | Magnetischer Datenträger | Disketten, Chip-, Magnet-, SD-, ID-Karten, Magnet-, Ton-, Video-Bänder, Audiokassetten |
| H | Magnetischer Datenträger | Festplatten |
| E | Elektronische Datenträger | Speicher-Sticks, Halbleiterspeicher, interne Speicher von Kameras, Mobiltelefonen, Tablets, Druckern, Kopierern und Faxgeräten, elektronische Komponenten, Medizinprodukte und –geräte |

## *1.2 Anwendungsbereich*

Die vorliegende Richtlinie gilt für alle Bereiche des Universitätsklinikums (UKT) und der Medizinischen Fakultät, die vom UKT betreut werden und in denen Personen digitalen Daten löschen sowie Datenträger vernichten und entsorgen.

## *1.3 Gültigkeit*

Die fachliche Freigabe der Dienstanweisung erfolgt durch das ISecBoard. Die disziplinarische Freigabe erfolgt durch den Vorstand des Klinikums und das Dekanat.
Sie wird unmittelbar nach der Beschlussfassung gültig und bleibt es bis zur Freigabe der nachfolgenden Version.

## *1.4 Referenzen*

Im Folgenden werden die Referenzen für die normativen Anforderungen gelistet.

[1] Bundesamt für Sicherheit in der Informationstechnik, „Cloud Computing Compliance Criteria Catalogue – C5:2020“, 2020

[2] Bundesamt für Sicherheit in der Informationstechnik, „Konkretisierung der Anforderungen an die gemäß §8a Absatz 1 BSIG umzusetzenden Maßnahmen“, Version 1.0, 2020

[3] DIN e.V., „DIN 66399 Büro- und Datentechnik – Vernichten von Datenträgern“, 2012

[4] DIN e.V., „DIN ISO/IEC 27001 - Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen“, 2015

[5] Uniklinikum Tübingen, „Prüfgrundlage §8a BSIG, Sektor ‚Gesundheit‘ für das Uniklinikum Tübingen“, 2021

[6] Uniklinikum Tübingen, „Richtlinie Lieferantenbeziehungen“, in Planung

# 2 Anforderungen an die Entsorgung von Informationen

Die in diesem Kapitel formulierten Anforderungen sind normative Anforderungen im Sinne eines ISMS nach ISO 27001 (siehe [4]). Abweichungen von diesen Anforderungen sind zu begründen und in das Risikomanagement aufzunehmen.
Bei der Formulierung der Anforderungen wird auf die folgenden Modalverben, deren Interpretation dem BSI IT-Grundschutz-Kompendium[1] entnommen ist, zurückgegriffen.

| **Modalverb** | **Interpretation** |
|---|---|
| MUSS / DARF NUR | Dieser Ausdruck bedeutet, dass es sich um eine Anforderung handelt, die unbedingt erfüllt werden muss. |
| DARF NICHT / DARF KEIN | Dieser Ausdruck bedeutet, dass etwas in keinem Fall getan werden darf. |
| SOLLTE | Dieser Ausdruck bedeutet, dass eine Anforderung normalerweise erfüllt werden muss, es aber Gründe geben kann, dies doch nicht zu tun. Dies muss sorgfältig abgewogen und stichhaltig begründet werden. |
| SOLLTE NICHT / SOLLTE KEIN | Dieser Ausdruck bedeutet, dass etwas normalerweise nicht getan werden sollte, es aber Gründe gibt, dies doch zu tun. Dies muss aber sorgfältig abgewogen und stichhaltig begründet werden. |
| KANN | Hier handelt es sich um eine Empfehlung, deren Umsetzung nicht verpflichtend ist. |

Die nachfolgenden Anforderungen werden in den Umsetzungshinweisen in Kapitel 3 detailliert beschrieben und sind von den technischen Fachabteilungen nachvollziehbar zu berücksichtigen.

| | | |
|---|---|---|
| **EVI.1.1 Gesetzliche Anforderungen** | | |
| EVI.1.2 | Berücksichtigung gesetzlicher Aufbewahrungsfristen | *Anforderung*<br>Die gesetzlichen Aufbewahrungspflichten und --fristen **MÜSSEN** eingehalten und vor der Datenlöschung und/oder Datenträgervernichtung geprüft werden. |
| ***EVI.1.3*** **Anforderungen an die Entsorgung von Informationen bei Wiederverwendung des Datenträgers** | | |
| EVI.1.4 | Weiterverwendung von Datenträgern | *Anforderung*<br>Vor der Weiterverwendung eines Datenträgers **MUSS** sichergestellt sein, dass die dort gespeicherten Daten gesichert sind. Der Asseteigner des Datenträgers **MUSS** vor der Weiterverwendung des Datenträgers festlegen, ob und mit welchem Verfahren die Daten gelöscht werden. |
| EVI.1.5 | Löschen von Informationen ohne Vernichtung des Datenträgers | *Anforderung*<br>Die Löschung von Informationen **MUSS** sich an der Vertraulichkeitsklasse der Informationen orientieren. Informationen der Vertraulichkeitsklasse TLP_Green **SOLLTEN** über die Bordmittel des eingesetzten Systems / der eingesetzten Anwendung gelöscht werden. Digitale |

[1] BSI IT-Grundschutz-Kompendium, aktuelle Version abrufbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

| | | |
|---|---|---|
| | | Daten der Vertraulichkeitsstufe TLP_Red **MÜSSEN** so gelöscht werden, dass eine Rekonstruktion der Daten nicht oder nur unter unverhältnismäßig großem Aufwand möglich ist. |
| ***EVI.1.6* Anforderungen an die Entsorgung / Vernichtung von Datenträgern** | | |
| EVI.1.7 | Lagerung / Zwischenlagerung von Datenträgern | *Anforderung*<br>Für die Entsorgung vorgesehene Datenträger **MÜSSEN** in verschließbaren und diebstahlgeschützten Sammelcontainer gelagert werden. Diese Sammelcontainer **MÜSSEN** an vereinbarten Orten bereitgestellt werden. Datenträger **DÜRFEN NUR** über die Sammelcontainer entsorgt werden. |
| EVI.1.8 | Transport der Datenträger | *Anforderung*<br>Die Sammelcontainer (siehe *EVI.1.7*) **MÜSSEN** verschlossen zum Entsorgungszentrum transportiert werden. Das Öffnen und Entleeren der Sammelcontainer **DARF NUR** durch befugtes Personal geschehen. Während des Transports **DÜRFEN KEINE** Datenträger entnommen werden. |
| EVI.1.9 | Löschen von Informationen durch Vernichtung der Datenträger | *Anforderung*<br>Die Vernichtung von Datenträgern **MUSS** nach dem aktuellen Stand der Technik erfolgen. Dabei **MÜSSEN** bei Informationen der Vertraulichkeitsklasse TLP_Green mindestens Verfahren der Sicherheitsstufe 3 der DIN 66399 (siehe *[3]*) zum Einsatz kommen. Sind Informationen der Vertraulichkeitsstufe TLP_Amber oder TLP_Red beteiligt, **MÜSSEN** Verfahren der Sicherheitsstufe 4 der DIN 66399 (siehe *[3]*) eingesetzt werden. |
| EVI.1.10 | Vernichtung von Datenträgern durch externe Dienstleister | *Anforderung*<br>Werden externe Dienstleister zur Entsorgung von Datenträgern beauftragt, **MUSS** der Prozess zum Vernichten ausreichend sicher und nachvollziehbar sein. Der Dienstleister **MUSS** mindestens die im Anwendungsbereich geltenden Anforderungen an die Vernichtung von Datenträgern erfüllen. Es **SOLLTE** regelmäßig überprüft werden, ob der Vernichtungsvorgang korrekt erfolgt. |
| EVI.1.11 | Vernichtung defekter digitaler Datenträger | *Anforderung*<br>Können digitale Datenträger aufgrund eines Defekts nicht entsprechend EVI.1.5 gelöscht werden, **SOLLTEN** sie mindestens nach Sicherheitsstufe 3 der DIN 66399 (siehe [3]) entsorgt werden. Wird der defekte Datenträger durch einen Dienstleister ausgetauscht oder repariert, **SOLLTE** der Datenträger durch den Dienstleister entsorgt oder gelöscht werden. Die vom Dienstleister zur Löschung / Vernichtung eingesetzten Verfahren **SOLLTEN** mindestens die im Anwendungsbereich geltenden Anforderungen erfüllen. |
| EVI.1.12 | Dokumentation und Nachweis | *Anforderung*<br>Der Asseteigner eines Datenträgers **MUSS** die ordnungsgemäße Vernichtung eines Datenträgers protokollieren und nachweisen. |

# 3 Umsetzungshinweise zu den Anforderungen

Dieses Kapitel enthält Informationen und Hinweise zur Umsetzung der normativen Anforderungen aus Kapitel 2.

### EVI.1.1 Gesetzliche Anforderungen

### EVI.1.2 Berücksichtigung gesetzlicher Aufbewahrungsfristen

Viele im Anwendungsbereich gespeicherte Informationen unterliegen gesetzlichen Aufbewahrungspflichten und -fristen, die eingehalten werden müssen. Vor dem Löschen von Informationen bzw. dem Vernichten eines Datenträgers muss also geprüft werden, ob die entsprechenden Informationen überhaupt gelöscht werden dürfen.

### EVI.1.3 Anforderungen an die Entsorgung von Informationen bei Wiederverwendung des Datenträgers

### EVI.1.4 Weiterverwendung von Datenträgern

Vor der Weiterverwendung eines Datenträgers ist sicherzustellen, dass die dort gespeicherten Daten gesichert sind. Der Asseteigner des Datenträgers muss vor der Weiterverwendung des Datenträgers festlegen, ob und mit welchem Verfahren die vorhandenen Daten gelöscht werden. Unter Weiterverwendung wird in diesem Kontext folgendes verstanden:

- Weiter- und Rückgabe
- Lagerung und Aufbewahrung
- Reparatur
- Vernichtung und Entsorgung

### EVI.1.5 Löschen von Informationen ohne Vernichtung des Datenträgers

Wie Daten von einem Datenträger gelöscht werden müssen, bestimmt die Vertraulichkeitsstufe der Information. Informationen der Vertraulichkeitsklasse TLP_Green dürfen über die Bordmittel der verwendeten Anwendung / des verwendeten Systems gelöscht werden.
Informationen der Vertraulichkeitsklasse TLP_Amber und TLP_Red sind so zu löschen, dass eine Rekonstruktion gar nicht oder mit nur unverhältnismäßig großem Aufwand möglich ist.

### EVI.1.6 Anforderungen an die Entsorgung / Vernichtung von Datenträgern

### EVI.1.7 Lagerung / Zwischenlagerung von Datenträgern

Zum Schutz vor unbefugter Entwendung erfolgt die Lagerung von für die Entsorgung vorgesehenen Datenträgern bis zum Abtransport ausschließlich in verschließbaren und diebstahlgeschützten Sammelcontainern. Die Sammelbehälter sind in Gebäuden/Etagen/Räumen an vereinbarten Orten bereitzustellen. Es gibt dedizierte Sammel-Container sind für die Materialklasse

- Papier,
- Filme und
- optische, magnetische und elektronische Datenträger.

Die Benutzer sind verpflichtet, die Sammel-Container zu nutzen.

### EVI.1.8 Transport der Datenträger

Die Sammelcontainer (siehe EVI.3.2) werden verschlossen zum Entsorgungszentrum trans-portiert. Das Öffnen und Entleeren der Sammelcontainer darf nur durch befugtes Personal erfolgen. Während des Transports dürfen keine Datenträger entnommen werden.

### EVI.1.9 Löschen von Informationen durch Vernichtung der Datenträger

Die Vernichtung von Datenträgern hat nach dem aktuellen Stand der Technik zu erfolgen. Dabei müssen bei Informationen der Vertraulichkeitsklasse TLP_Green mindestens Verfahren der Sicherheitsstufe 3 der DIN 66399 (siehe *[3]*) zum Einsatz kommen. Sind Informationen der Vertraulichkeitsstufe TLP_Amber oder TLP_Red beteiligt, müssen Verfahren der Sicherheitsstufe 4 der DIN 66399 (siehe *[3]*) eingesetzt werden.

### EVI.1.10 Vernichtung von Datenträgern durch externe Dienstleister

Die Vernichtung von Datenträgern kann auch durch externe Dienstleister erfolgen. In diesem Fall muss der Vernichtungsprozess bei dem Dienstleister ausreichend sicher und nachvollziehbar sein. Der Dienstleister muss mindestens die im Anwendungsbereich geltenden Anforderungen an die Vernichtung von Datenträgern erfüllen. Es sollte regelmäßig überprüft werden, ob der Vernichtungsvorgang noch korrekt erfolgt.
Ein externer Dienstleister zur Datenvernichtung muss die entsprechenden Anforderungen der Richtlinie zu Lieferantenbeziehungen (siehe [6]) erfüllen.

### EVI.1.11 Vernichtung defekter digitaler Datenträger

Ist ein Datenträger defekt, können unter Umständen auf ihm gespeicherte Informationen nicht mehr ordnungsgemäß gelöscht werden. In diesem Fall sollte der Datenträger mindestens nach Sicherheitsstufe 3 der DIN 66399 (siehe [3]) entsorgt werden.
Falls der defekte Datenträger durch einen Dienstleister ausgetauscht oder repariert wird, sollte der Datenträger durch den Dienstleister entsorgt oder gelöscht werden. Die vom Dienstleister zur Löschung / Vernichtung eingesetzten Verfahren haben dabei mindestens die im Anwendungsbereich geltenden Anforderungen zu erfüllen.

### EVI.1.12 Dokumentation und Nachweis

Der Eigner eines Datenträgers (im Sinne des Asseteigners) hat die ordnungsgemäße Vernichtung des Datenträgers zu protokollieren und nachzuweisen.

# 4 Anhang

## *4.1 Zuordnung der Anforderungen zu den Maßnahmenzielen der ISO 27001*

Die folgende Tabelle enthält eine Zuordnung der in Kapitel 2 formulierten Anforderungen zu den Maßnahmenzielen aus dem Anhang A der Norm ISO 27001 (siehe [4]).
Maßnahmenziele, die in der vorliegenden Richtlinie nicht adressiert werden, werden in der folgenden Tabelle nicht aufgeführt.

| **Maßnahmenziele gemäß ISO 27001** | **Anforderungen aus Kapitel 2** |
|---|---|
| A.8.3.1 Handhabung von Wechseldatenträgern | EVI.1.4 Weiterverwendung von Datenträgern |
| A.8.3.2 Entsorgung von Datenträgern | EVI.1.6 Anforderungen an die Entsorgung / Vernichtung von Datenträgern |
| A.8.3.3 Transport von Datenträgern | EVI.1.8 Transport der Datenträger |
| A.11.2.5 Entfernen von Werten | EVI.1.2 Berücksichtigung gesetzlicher Aufbewahrungsfristen |
| A.11.2.7 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln | Gesamtes Dokument |

## *4.2 Zuordnung der Anforderungen zur Prüfgrundlage §8a BSIG*

Die folgende Tabelle enthält eine Zuordnung der in Kapitel 2 formulierten Anforderungen zu den Anforderungen an die Prüfgrundlage §8a BSIG (siehe [5]).
Anforderungen aus [5], die in der vorliegenden Richtlinie nicht adressiert werden, werden in der folgenden Tabelle nicht aufgeführt.

| **Anforderungen gemäß [5]** | **Anforderungen aus Kapitel 2** |
|---|---|
| Anf.01.035.RL<br>Entsorgung von Informationen | Gesamtes Dokument |
| Anf.02.006.Orga<br>Entsorgung von Informationen | Gesamtes Dokument |

## *4.3 Zuordnung der Anforderungen zu den Anforderungen der Konkretisierung des BSIG §8a des BSI*

Die folgende Tabelle enthält eine Zuordnung der in Kapitel 2 formulierten Anforderungen zu den Anforderungen der Konkretisierung des BSIG §8a des BSI (siehe [2]). Die in [2] formulierten Anforderungen basieren auf einer älteren Version des Anforderungskatalogs für das Cloud-Computing des BSI (siehe [1]). In der folgenden Tabelle werden die entsprechenden Kriterien aus der aktuellen Version des Anforderungskatalogs für das Cloud Computing des BSI (siehe [1]) mit aufgeführt.
Anforderungen aus [2], die in der vorliegenden Richtlinie nicht adressiert werden, werden in der folgenden Tabelle nicht aufgeführt.

| **Anforderungen gemäß [2]** | **Basiskriterien gemäß [1]** | **Anforderungen aus Kapitel 2** |
|---|---|---|
| 11. Verwaltung von Datenträgern | AM-07 | Gesamtes Dokument |