**Richtlinie** **zur sicheren Löschung und Vernichtung von Daten und Datenträgern**

**der** **<Name der Organisation>**

**Anwendungshinweis (Bitte vor Benutzung entfernen):**

Wir bitten Sie in Kenntnis zu nehmen, dass die vorliegende Richtlinie mit größter Sorgfalt erstellt und geprüft wurde, jedoch keinen Anspruch auf Vollständigkeit erhebt. Sie muss auf Ihre Organisation und auf deren Gegebenheiten individuell angepasst sowie zugeschnitten werden und dient hierfür als Hilfestellung und mögliches Beispiel.

Disclaimer: Die Inhalte dieses Leitfadens wurden von LSI erarbeitet und sind sorgfältig recherchiert. Trotz

Größtmöglicher Sorgfalt erhebt die vorliegende Publikation keinen Anspruch auf Vollständigkeit. Sie spiegelt des LSI wider. Das LSI übernimmt keine Haftung für den Inhalt.

Dokumenteneigenschaften

|  |  |
| --- | --- |
| **Titel** |  |
| **Art** | Richtlinie |
| **Hauptverantwortlicher** | <Name der Geschäftsführung> |
| **E-Mail, Telefon** | <E-Mail-Adresse, Telefonnummer> |
| **Ansprechpartner** | <Name des Ansprechpartners der Richtlinie / ISB> |
| **E-Mail, Telefon** | <E-Mail-Adresse, Telefonnummer> |
| **Version** | <x.x> |
| **In Kraft seit** | <xx.xx.2022> |
| **Überarbeitungsintervall** | 12 Monate |
| **Nächste Überarbeitung** | <yy.yy.2023> |

Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Änderung** | **Datum** | **Autor** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhalt

[1. Einleitung 3](#_Toc122521664)

[2. Geltungsbereich 3](#_Toc122521665)

[3. Allgemeine Bestimmungen 4](#_Toc122521666)

[4. Vorgehensweise bei der Löschung und Vernichtung 4](#_Toc122521667)

[5. Löschen und Vernichten durch Dritte 5](#_Toc122521668)

# Einleitung

Alle sensiblen Informationen müssen vor unbefugter Kenntnisnahme geschützt werden, das gilt auch wenn Geräte, die diese Informationen verarbeiten, aus der Organisation entfernt werden oder die Daten einfach nicht mehr benötigt werden. Daher ist es wichtig sämtliche Daten sicher, d.h. vollständig und unwiderruflich, zu löschen bzw. zu vernichten. Das einfache Löschen von Datenträgern oder Zerreißen von Papierdokumenten reicht dafür nicht aus.

Eine einheitliche Regelung für die gesamte Organisation hilft dabei den Missbrauch von Daten zu verhindern, Mitarbeiter zu sensibilisieren und sie bei der Auswahl der richtigen Werkzeuge und Verfahren zu unterstützen.

Geeignete Vorgehensweisen der Datenvernichtung sind sowohl vom Schutzbedarf der Informationen, als auch von der Art des Datenträgers und der Speichertechnologie abhängig.

Der Zweck dieses Dokumentes ist die Gewährleistung der sicheren Löschung und Vernichtung von Daten.

# Geltungsbereich

Diese Richtlinie gilt für die gesamte <Name der Organisation> und berücksichtigt alle zurzeit gebräuchlichen und in der <Name der Organisation> eingesetzten Datenträger.

Ein Datenträger stellt jedes Medium dar, auf dem Daten analog oder digital gespeichert werden. Zu analogen Medien zählen z.B.: Daten in Papierformat, Videobänder, Magnetbänder. Im Gegensatz dazu lassen sich die digitalen Datenträger in elektromagnetische (z.B. HDD-Festplatten, Disketten), optische (z.B. CD-ROM, DVD) und Flash-Speicher (z.B. SSD-Festplatten, USB-Sticks) untergliedern.

Die Richtlinie gilt für alle Beschäftigten der <Name der Organisation>.

# Allgemeine Bestimmungen

Daten sind unter Berücksichtigung der gesetzlichen Aufbewahrungspflichten zu löschen. Dies muss für jeden Datensatz individuell festgelegt werden. Dafür muss ein Verantwortlicher benannt sein, der je nach Datenart, -form, Schutzklasse und -bedarf etc. den richtigen Umgang, sowie die Einhaltung gesetzlicher Pflichten bis hin zur Löschung und Vernichtung der Daten überwacht.

Wann sind Daten zu löschen:

* Wenn die Daten nicht mehr zur Erfüllung der in der Zuständigkeit liegenden Aufgaben für die verantwortliche Stelle erforderlich sind.
* Wenn die Speicherung unzulässig ist.
* Falls ein Gerät, auf welchem sensible Daten gespeichert sind, den Geltungsbereich der <Name der Organisation> verlässt durch Weiterverkauf, Reparatur und Entsorgung etc. *[Hinweis: Werden die Daten noch benötigt, müssen sie in der Organisation anderweitig gesichert werden.]*

Wann sind Datenträger zu vernichten:

* Wenn sie dauerhaft außer Betrieb genommen werden.
* Wenn sie defekt sind.

Die Löschung schützenswerter Informationen und die Vernichtung von Datenträgern muss in einer geeigneten Form schriftlich dokumentiert werden.

# Vorgehensweise bei der Löschung und Vernichtung

Das „normale“ Löschen von Dateien bietet keinen ausreichenden Schutz. Die Daten sind auf den Datenträger weiterhin vorhanden und können wiederhergestellt und ausgelesen werden. Daten werden, je nach Speichermedium folgendermaßen gelöscht oder gemäß DIN 66399 vernichtet:

*[Hinweis (bitte löschen): Für die in der Organisation genutzten Speichermedien müssen individuelle passende Lösch- und Vernichtungsmechanismen ausgewählt werden.*

*Für die endgültige Löschung von Daten auf fast alle Speichermedien können software- oder hardwaretechnische Methoden genutzt werden. Durch den Einsatz von speziellen Löschprogrammen, die den Speicher mehrfach mit Zufallsdaten überschreiben, können Daten mit einer hohen Sicherheit gelöscht werden. Entmagnetisierung ist eine weitere Möglichkeit zur nachhaltigen zuverlässigen Löschung, dies kann mittels eines elektrisches Gerätes „Degausser“ durchgeführt werden.*

*Eine zuverlässige Methode zur endgültigen Datenlöschung ist die hardwarebasierte, physikalische Zerstörung von Datenträgern, ihre Weiterverwendung ist daher ausgeschlossen. Eine gängige Methode ist das sogenannte Schreddern, wodurch der Datenträger in kleine Teile zerlegt und somit zerstört wird. Auch durch die thermische Zerstörung können Datenträger ihre magnetische Eigenschaft verlieren oder sogar komplett vernichtet werden.]*

* Analoge Medien wie Papier und CD/DVD´s müssen geschreddert werden.
* Video- und Magnetbänder werden entmagnetisiert oder sind physikalisch zu vernichten.
* HDD-Festplatten, USB-Sticks und Speicherkarten werden mit Spezialsoftware durch mehrfaches Überschreiben gelöscht. Für SSD-Festplatten muss eine spezielle Software zur sicheren endgültigen Löschung vom Hersteller genutzt werden.
* Mobile Devices und IoT-Geräte müssen auf Werkseinstellung zurückgesetzt und die Zugangsdaten abgeändert werden. Zum Abschluss des Löschvorgangs sollte die Einrichtung des Gerätes erneut durchgeführt werden.

Können digitale Datenträger mit schützenswerten Informationen aufgrund eines Defekts nicht sicher gelöscht werden, müssen diese vernichtet werden.

Sind für die Löschung und Vernichtung keine technischen Möglichkeiten in der eigenen Organisation vorhanden, muss dafür ein Dienstleister beauftragt werden.

# Löschen und Vernichten durch Dritte

Wenn ein Dienstleister den Auftrag zur Vernichtung bzw. Löschung der Daten übernimmt, verbleibt die Verantwortung für den Schutz der Daten weiterhin im Verantwortungsbereich der <Name der Organisation>. Die ordnungsgemäße Löschung/Vernichtung der technischen und organisatorischen Maßnahmen muss dokumentiert und regelmäßig überprüft werden.

Ort, den Datum

Name, Position, Unterschrift