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

Sicherheitsrichtlinie "Löschen und vernichten von Informationen"

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 Dokumentenvertraulichkeit  offen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300003 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung (vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "Datensicherung" | [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

Damit Informationen der <Institution> nicht in falsche bzw. unberechtigte Hände geraten, ist eine geregelte Vorgehensweise erforderlich, um Daten und Datenträger vollständig und zuverlässig zu löschen oder zu vernichten. Dabei müssen schutzbedürftige Informationen, die auf analogen und digitalen Datenträgern gespeichert sind, berücksichtigt werden.

Wenn nicht oder nur unzureichend gelöschte Datenträger bspw. in Druckern, Notebooks, Firewalls, Switches, SANs weitergegeben, verkauft oder ausgesondert werden, können dadurch unbeabsichtigt schützenswerte Informationen in falsche Hände gelangen. Dadurch können erhebliche Reputationsschäden, Vertragsstrafen sowie weitere kurzfristige finanzielle Belastungen im Rahmen der Beseitigung des Security Incidents entstehen. Deshalb muss eine Vorgehensweise zum sicheren Löschen und Vernichten von Informationen etabliert werden. Der Vernichtungsvorgang muss dabei die Daten auf dem Datenträger dahingehend löschen/vernichten, dass ihre Reproduktion oder Rekonstruktion unmöglich ist oder weitestgehend erschwert wird.

In dieser Sicherheitsrichtlinie wird beschrieben, wie Informationen sicher gelöscht und vernichtet werden können und wie ein entsprechendes Konzept dazu erstellt wird. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben des BSI Bausteines CON.6 "Löschen und Vernichten" 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 löschen und vernichten von Informationen“ 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 "Löschen und vernichten von Informationen"

## Basismaßnahmen

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

### Regelung der Vorgehensweise für die Löschung und Vernichtung von Informationen (CON.6.A1)

Das Löschen und Vernichten von Informationen ist innerhalb der Architrave GmbH geregelt. Dabei ist festgelegt, welche Informationen und Betriebsmittel unter welchen Voraussetzungen gelöscht und entsorgt werden dürfen. Zusätzlich ist festgelegt, in welchen räumlichen Bereichen Entsorgungs- und Vernichtungseinrichtungen aufgebaut sind.

Innerhalb der Planungsphase ist festzulegen, wer für das Löschen und Vernichten von Informationen und Betriebsmitteln zuständig ist und welche Schnittstellen es zwischen den Organisationseinheiten der Architrave GmbH gibt. Außerdem wurde der interne Informationsfluss und zwischen den Zuständigen der Institution mit möglichen Outsourcing-Dienstleistern geregelt.

### Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln und Informationen (CON.6.A2)

Um alle schutzbedürftigen Informationen und Betriebsmittel sicher zu entsorgen, müssen in den Gebäuden der Architrave oder ihren Töchtern bzw. den externen Dienstleistern geeignete Entsorgungseinrichtungen existieren. Es muss ebenfalls eine zentrale Sammelstelle für Informationen und Betriebsmittel, die erst gesammelt und später entsorgt werden, vorhanden sein. Bis zur Abholung müssen die Datenträger vor unbefugtem Zugriff gesichert und auf der gesamten Transportstrecke geschützt sein. Das Entsorgungsprotokoll des Dienstleisters ist dem Löschprotokoll beizufügen.

Die Entsorgung erfolgt konform der DIN 66399 mit folgenden Sicherheitsstufen:

* Für Schutzklasse 1 – normaler Schutzbedarf für interne Daten
  + Entsprechend den Sicherheitsstufen 1 und 2
* Für Schutzklasse 2 – hoher Schutzbedarf für vertrauliche Daten
  + Entsprechend den Sicherheitsstufen 3 und 4
* Für Schutzklasse 3 – sehr hoher Schutzbedarf für streng vertrauliche Daten
  + Entsprechend den Sicherheitsstufen 4 und 5

Trotz der Entsorgung nach den entsprechenden Sicherheitsstufen, müssen die Datenträger zuvor soweit wie möglich gelöscht werden.

Werden externe Dienstleister beauftragt, ist der Entsorgungsvorgang ausreichend sicher und nachvollziehbar zu etablieren. Die mit der Entsorgung beauftragten Unternehmen werden regelmäßig daraufhin überprüft, ob der Entsorgungsvorgang noch dem Soll-Zustand entspricht.

## Standardmaßnahmen

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

### Löschen der Datenträger vor und nach dem Austausch (CON.6.A3)

Vor Weitergabe oder erneutem Einsatz bereits benutzter Datenträger, sind alle darauf befindlichen Daten sicher zu löschen. Allen Mitarbeitenden der Architrave GmbH sind hierfür geeignete Werkezeuge zur Verfügung zu stellen.

### Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern (CON6.A4)

Innerhalb der Architrave GmbH sind geeignete Verfahren zum Löschen und Vernichten von Datenträgern zu benennen. Je nach Datenträgerart existieren geeignete Geräte und Werkzeuge, mit denen die verantwortlichen Mitarbeitenden die gespeicherten Informationen löschen oder vernichten kann. Die ausgewählten Verfahren sind allen Mitarbeitenden bekannt und werden regelmäßig auf ihre Aktualität und Sicherheit überprüft.

### Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern (CON6.A5)

Die Außerbetriebnahme von IT-Systemen und Datenträgern ist geregelt und zu dokumentieren. Dabei ist sicherzustellen, dass vor der Aussonderung alle auf einem IT-System oder Datenträger gespeicherten Daten sicher gelöscht sind. Neben "klassischen" IT-Systemen werden auch alle IT-Systeme mit dauerhaften Speicherelementen berücksichtigt.

### Einweisung aller Mitarbeitenden in die Methoden zur Löschung oder Vernichtung von Informationen (CON.6.A6)

Alle Mitarbeitende sind in die Methoden und Verfahrensweisen zum Löschen und Vernichten von Informationen einzuweisen.

### Beseitigung von Restinformationen (CON6.A7)

Innerhalb der Architrave GmbH muss ein Prozess zur Beseitigung von Restinformationen eingeführt und dokumentiert werden. Dieser stellt sicher, dass alle Restinformationen vor Weitergabe von Datenträgern und Dateien beseitigt sind. Alle Mitarbeitende sind über potenzielle Gefahren von Rest- und Zusatzinformationen zu informieren. Es erfolgen stichprobenartige Kontrollen, ob die Restinformationen auch wirklich gelöscht wurden.

## 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).

### Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern bei erhöhtem Schutzbedarf (CON.6.A9 - CIA)

Es werden Verfahren zur Löschung und Vernichtung eingesetzt, die dem erhöhten Schutzbedarf der Informationen und Betriebsmittel gerecht werden.

### Beschaffung geeigneter Geräte zur Löschung oder Vernichtung von Daten (CON.6.A10 - CIA)

Für die Beschaffung geeigneter Geräte zur Löschung und Vernichtung von Daten ist eine Anforderungsdokumentation zu erstellen. Anhand dieser Dokumentation sind die auf dem Markt verfügbaren Werkzeuge zu verglichen.

### Vernichtung von Datenträgern durch externe Dienstleister (CON6.A11 - CIA)

Alle zu vernichtenden Datenträger werden bis zur Abholung durch den externen Dienstleister sicher vor unbefugtem Zugriff aufbewahrt. Der Abtransport ist zusätzlich dem Schutzbedarf entsprechend abgesichert. Der Entsorgungsprozess ist regelmäßig durch eingewiesene Personen überprüft.