**Backup-Richtlinie** **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.

Dokumenteneigenschaften

|  |  |
| --- | --- |
| **Titel** | Backup-Richtlinie |
| **Art** | Richtlinie |
| **Hauptverantwortlicher** | <Name der Organisationsleitung> |
| **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> |
| **In Kraft gesetzt durch** | <Name der Organisationsleitung / des Verantwortlichen> |
| **Überarbeitungsintervall** | <12> Monate |
| **Nächste Überarbeitung** | <yy.yy.2023> |

Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Änderung** | **Datum** | **Autor** |
| v.1.0 | Initialerstellung | 01.06.2022 | LSI |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Inhalt**

[1 Einleitung 4](#_Toc94864385)

[2 Geltungsbereich 4](#_Toc94864386)

[3 Zweck 4](#_Toc94864387)

[4 Regelungen 4](#_Toc94864388)

[4.1 Umfang der Datensicherung 4](#_Toc94864389)

[4.2 Durchführung der Datensicherung 5](#_Toc94864390)

[4.2.1 Eingesetzte Speichermedien 5](#_Toc94864391)

[4.2.2 Backup-Typen, Softwarelösungen und -Zeiträume 5](#_Toc94864392)

[4.2.3 Verschlüsselung des Backups 6](#_Toc94864393)

[4.3 Aufbewahrung und Dokumentation der Datensicherung 6](#_Toc94864394)

[4.3.1 Anzahl der Generationen 6](#_Toc94864395)

[4.3.2 Vorherige Löschung der Datenträger vor Wiederverwendung 6](#_Toc94864396)

[4.3.3 Dokumentation 6](#_Toc94864397)

[4.4 Aufbewahrungsort 6](#_Toc94864398)

[4.4.1 Datensicherungsarchiv 6](#_Toc94864399)

[4.5 Funktionstests und Überprüfung der Wiederherstellbarkeit 6](#_Toc94864400)

[4.6 Gesetzlichen Aufbewahrungs- und Löschfristen 6](#_Toc94864401)

# Einleitung

Daten sind für Unternehmen von enormem Wert, da sie den meisten Geschäftsprozessen zugrunde liegen, dazu kommen noch gesetzliche Aufbewahrungsfristen und gegebenenfalls spezielle Kundenanforderungen. Dies betrifft im industriellen Umfeld zum Beispiel auch Konfigurationseinstellungen und Steuerungsdaten. Da die meisten Daten heutzutage nur noch digital verwaltet werden, müssen diese vor allem vor defekter Hardware, menschlichen Fehlern und vor Malware geschützt werden. Hierfür empfiehlt sich der Einsatz von Backups, da ein kompletter Ausschluss der genannten Risiken nahezu unmöglich ist.

# Geltungsbereich

Die in dieser Richtlinie festgelegten Regelungen gelten für die gesamte <Name der Organisation> und umfassen alle Bereiche, in welchen Daten erhoben, gespeichert oder verarbeitet werden.

# Zweck

Ziel der Backuprichtlinie ist es, mithilfe von Datensicherungen die Auswirkungen auf die Geschäftsprozesse nach einem möglichen Datenverlust auf ein Minimum zu reduzieren bzw. eine zügige Wiederherstellung zu ermöglichen. Die folgenden Regelungen definieren Umfang, Zuständigkeiten, Durchführung, Häufigkeit, Aufbewahrung, Test, Wiederherstellung und gesetzliche Fristen von Datensicherungen.

# Regelungen

##  Umfang der Datensicherung

Sämtliche zu sichernde Daten müssen in einer zentralen Liste oder in einer anderen geeigneten Form (z.B. Softwarelösung) dokumentiert werden.

Hierzu wird der Reiter <Datenliste> in der Tabelle <Backup\_Dokumentation.xlsx> genutzt. Zu sämtlichen zu sichernden Daten ist folgendes festzulegen:

* der Name der Daten
* das einzusetzende Speichermedium
* Art der Sicherung (z.B. Vollsicherung, inkrementelle Datensicherung)
* der Zeitpunkt (für die Vollsicherungen bzw. der Startpunkt für die regelmäßigen Intervallsicherungen z.B. freitags, 18:00 Uhr)
* das Sicherungsintervall (z.B. wöchentlich, täglich)
* besondere Aufbewahrungs- und Löschfristen
* der Aufbewahrungsort

Im Wasserwerk muss es für folgende Aufgaben einen Verantwortlichen sowie eine Vertretung geben:

* Verantwortlichkeit für die Backups
* Zuständigkeit für die Durchführung der Backups
* Zuständigkeit für die Dokumentation der korrekten Ausführung
* Berechtigung für die Wiederherstellung

Die Verantwortung und damit die regelmäßige Kontrolle der korrekten Durchführung liegt hiermit bei <Max Kontrollmann> bzw. in Vertretung bei <Erika Kontrollfrau>.

## Durchführung der Datensicherung

### Eingesetzte Speichermedien

Grundlage für die Wahl des Speichermediums ist das zu sichernde Datenvolumen, die Wiederherstellungszeiten und die Lebensdauer des Mediums.

Auflistung der genutzten Medien:

* <Festplatten>
* <Magnetbänder>
* <...>

### Backup-Typen, Softwarelösungen und -Zeiträume

*[Hinweise (bitte löschen): Es empfiehlt sich die 3-2-1-Backup\* Regel (drei Datenkopien auf mindestens zwei unterschiedlichen Medien, wovon mindestens ein Backup nach Erstellung, vom Netz getrennt, sicher gelagert werden sollte) umzusetzen. Zusätzlich zu den regelmäßigen Backups sollte sowohl bei der Einrichtung als auch bei Änderungen am System (dabei ist auf jeweilige Vollständigkeit zu achten z.B. SPS-Programm, Konfiguration und Prozessvariablen) eine Vollsicherung erstellt werden.*

*Die Häufigkeit der Datensicherung ist von der Kritikalität der Systeme abhängig zu machen. Es sollte stets auf eine Kompatibilität des aktuellen Systems mit den älteren, vorgehaltenen Backups geachtet werden, damit diese bei Bedarf problemlos eingesetzt werden können.*

*Die Backups sollten physisch sicher gelagert werden (z.B. separate Brandabschnitte). Der Zugriff auf Backups darf nur nach dem Minimalprinzip und nur durch berechtigte Mitarbeiter möglich sein.]*

Die Organisation setzt zum Backup ein:

Vollsicherung: Bei der monatlichen Sicherung mit <Software> werden 3 Kopien (auf 2 Festplatten und 1 Magnetband) der kritischen Systeme (außerhalb der Hauptgeschäftszeit) erstellt. Das Magnetband ist nach der Erstellung gesichert an <Ort> aufzubewahren.

Differentielles Backup: Eine tägliche Sicherung erfolgt mit <Software>. Erstellt werden 2 Kopien der kritischen Systeme auf 2 Festplatten und eine wöchentliche Sicherung erfolgt auf Magnetband (basierend auf der zugehörigen, monatlichen Vollsicherung).

Details werden in der Tabelle <Backup\_Dokumentation.xlsx> im Reiter <Datenliste> definiert.

*[Hinweise (bitte löschen): Bei der Wahl des Backup-Typs müssen vor allem die Wichtigkeit und die Menge der zu sichernden Daten sowie die zur Sicherung benötigte Zeit und die Speicherkapazitäten berücksichtigt werden.*

*Backup-Typen: Vollsicherung, differentielles Backup (sichert alle Änderungen seit der letzten Vollsicherung) und inkrementelle Datensicherung (sichert nur die Änderungen seit der letzten Sicherung).*

*Es empfiehlt sich eine Kombination der drei Sicherungstypen zu wählen, um die jeweiligen Vorteile miteinander zu verbinden.]*

### Verschlüsselung des Backups

Vertrauliche Daten müssen verschlüsselt auf dem Backupmedium gespeichert werden. Der verwendete Schlüssel ist für Notfälle hinterlegt unter: <Ort und Zugangsmöglichkeit sowie Zugangsberechtigte>.

## Aufbewahrung und Dokumentation der Datensicherung

### Anzahl der Generationen

Es ist festzulegen, wie viele verschiedene Backup-Stände vorgehalten werden sollen, bis die älteste Version mit einem neuen Backup-Stand überschrieben wird.

### Vorherige Löschung der Datenträger vor Wiederverwendung

Bevor ein Datenträger erneut für ein Backup verwendet wird sollte dieser zuerst bereinigt werden.

### Dokumentation

Folgende Parameter müssen beim Erstellen von Datensicherungen hinterlegt werden:

* das Datum und die Uhrzeit
* die Beschriftung des Backups
* das System
* die Art der Durchführung
* das Speichermedium
* Die Aufbewahrungszeit
* der Lagerort
* der Name des durchführenden Mitarbeiters

Die Dokumentation hat fortan in <Backup\_Dokumentation.xlsx> zu erfolgen. Die Tabelle liegt im Intranet unter <Link>.

##  Aufbewahrungsort

### Datensicherungsarchiv

Um den physischen Zugriff durch Unbefugte zu verhindern ist es nötig die Sicherheitskopien an einem abgesicherten Ort aufzubewahren. Die Backups sollten an verschiedenen Orten (redundant) gelagert werden.

Wir verwenden dafür <Datensicherungsarchiv>.

Folgende Personen haben Zugriff auf das Archiv:

* <Max Mustermann>

##  Funktionstests und Überprüfung der Wiederherstellbarkeit

Um einen reibungslosen Wiederherstellungsprozess gewährleisten zu können, müssen in regelmäßigen Abständen Funktionstests durchgeführt werden.

<Intervall und Ablauf der Tests>

##  Gesetzlichen Aufbewahrungs- und Löschfristen

Folgende organisationsspezifische gesetzliche Aufbewahrungs- und Löschfristen sind einzuhalten:

<Die für Sie relevanten gesetzliche Vorgaben auflisten>