**Passwortrichtlinie****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** | Passwortrichtlinie |
| **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 | 01.01.2022 | LSI |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Inhalt**

[1. Einleitung 3](#_Toc95468423)

[2. Geltungsbereich 4](#_Toc95468424)

[3. Zweck 4](#_Toc95468425)

[4. Regelungen 4](#_Toc95468426)

[4.1. Vorgaben zu Passwörtern 4](#_Toc95468427)

[4.1.1. Allgemeine Passwörter 4](#_Toc95468428)

[4.1.2. Administrative Passwörter 4](#_Toc95468429)

[4.1.3. Passwörter mobiler Geräte (Smartphones, Tablets) 4](#_Toc95468430)

[4.2. Richtiger Umgang mit Passwörtern 5](#_Toc95468431)

[4.2.1. Allgemeiner Umgang mit Passwörtern 5](#_Toc95468432)

[4.2.2. Initialpasswörter 5](#_Toc95468433)

[4.2.3. Verwendung von Passwörtern 5](#_Toc95468434)

[4.2.4. Sicheres Aufbewahren von Passwörtern 5](#_Toc95468435)

[4.2.5. Verhalten bei Verdacht auf Kompromittierung des Passworts 5](#_Toc95468436)

[4.2.6. Zurücksetzen von Passwörtern 5](#_Toc95468437)

[4.3. Schulung der Mitarbeiter 6](#_Toc95468438)

[4.4. Genehmigung von Ausnahmen 6](#_Toc95468439)

[4.5. Pflichten von Systembetreibern 6](#_Toc95468440)

[4.5.1. Allgemeiner Umgang mit Passwörtern 6](#_Toc95468441)

[4.5.2. Accountsperre 6](#_Toc95468442)

[4.5.3. Zweifaktorauthentifizierung (2FA) 6](#_Toc95468443)

# Einleitung

Das Ziel dieser Passwortrichtlinie ist die Sicherstellung der Qualität von verwendeten Passwörtern und die Festlegung der Regeln, welche im sicheren Umgang mit Passwörtern und Benutzerkonten in der <Name der Organisation> einzuhalten sind. Dieses Dokument muss jedem Mitarbeiter und Dienstleister bekannt sein sowie für jeden zugänglich an einem zentralen Ort abgelegt sein.

# Geltungsbereich

Dieses Dokument gilt für alle Nutzer sowie interne und externe Dienstleister der <Name der Organisation>.

# Zweck

Um Zugänge zu Systemen angemessen zu schützen und ein hohes Sicherheitsniveau von Passwörtern sicherzustellen, muss es feste Passwort- Regelungen geben. Die Mindestanforderungen sind in der folgenden Richtlinie festgelegt und Benutzer und Betreiber von IT-Systemen sind bezüglich Ihrer Verpflichtung zur Einhaltung zu unterweisen. Ausnahmen von dieser Regelung müssen beim zuständigen Informationssicherheitsbeauftragten beantragt werden.

# Regelungen

## Mindestanforderungen an die Komplexität der Passwörter

Um die Mindestanforderung an Passwörter zu erfüllen, sind die nachfolgenden Anforderungen umzusetzen und falls möglich auch technisch zu implementieren.

Alle Passwörter dürfen nicht im Wörterbuch vorkommen, sollten keine persönlichen Daten enthalten (z.B. Geburtsdatum, Name des Haustiers) und dürfen kein Tastaturmuster (z.B. „qwertz“) sein.

Es kann aus einem Merksatz abgeleitet werden und muss alle vier Zeichensätze (Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen) nutzen (z.B. Unser Zweckverband besteht aus 13 Gemeinden und wir arbeiten alle wirklich sehr gerne dort! => UZba13Guwaawsgd!). Hinweis: unbedingt einen eigenen Merksatz ausdenken!

Das Passwort muss mindestens 10 Zeichen lang sein oder mindestens die technisch maximal möglichen Stellen umfassen (z.B. bei PIN und PUKs).

Um die Komplexitätsanforderungen zu erfüllen müssen alle der folgenden Zeichensätze genutzt werden:

* Großbuchstaben (A bis Z)
* Kleinbuchstaben (a bis z)
* Ziffern (0 bis 9)
* Sonderzeichen (z.B. !, $, -, %)

Sollte dies nicht möglich sein, so sind zumindest die technisch möglichen Zeichensätze zu verwenden.

Passwörter für den Zugang zu sensiblen Bereichen z.B. die Passwörter für Systemadministratoren müssen mindestens 16 Zeichen lang sein.

## Richtiger Umgang mit Passwörtern

Passwörter dürfen nicht geteilt, weitergegeben oder anderen zugänglich gemacht werden.

Passwörter dürfen nicht notiert und für Dritte einsehbar sein (z.B. im Notizbuch auf dem Schreibtisch). Ist das Notieren eines Passwortes unvermeidlich, so ist dieses jedoch zugangsgeschützt aufzubewahren (z.B. versiegelt in einem Tresor für Notfälle).

Bei der Eingabe von Passwörtern ist darauf zu achten, dass man von niemandem beobachtet wird.

Passwörter dürfen nicht als Teil eines automatisierten Anmeldeprozesses verwendet werden (z.B. Passwortspeicherung des Browsers).

Passwörter dürfen nicht in Online-Passwortchecks eingegeben werden, da diese so abgefangen und missbraucht werden können.

Die Passwörter dürfen nicht im Webbrowser gespeichert werden, da die Verschlüsselung schwach ist und umgangen werden kann.

### Initialpasswörter

Voreingestellte Initialpasswörter (Default-Passwörter) bzw. zurückgesetzte Passwörter sind unverzüglich, konform zu den Kriterien in 4.1, durch ein neues Passwort zu ersetzen.

### Verwendung von Passwörtern

Passwörter, welche Sie bereits im privaten Bereich verwenden, dürfen geschäftlich nicht verwendet werden. Dies gilt auch im umgekehrten Fall.

Bei der Anmeldung an verschiedenen Systemen sind jeweils eigene unterschiedliche Passwörter einzurichten bzw. zu verwenden, soweit technisch umsetzbar.

### Sicheres Aufbewahren von Passwörtern

Die unverschlüsselte Speicherung von Passwörtern auf IT-Systemen ist nicht gestattet (z.B. ein Word Dokument abgelegt auf dem Desktop).

Für die sichere Aufbewahrung und Speicherung von Passwörtern wird ein Passwort-Manager-Programm empfohlen.

### Verhalten bei Verdacht auf Kompromittierung des Passworts

Auffälligkeiten sind umgehend an die IT-Abteilung und den Informationssicherheits-beauftragten zu melden. Sollte der Verdacht aufkommen, dass ein Passwort fremden Personen bekannt oder zugänglich geworden ist, so muss dieses sofort geändert werden.

Ansonsten genügt ein jährlicher Passwortwechsel.

### Zurücksetzen von Passwörtern

[*Hinweis: Für eine ordnungsgemäße Umsetzung der Richtlinie muss nicht speziell die folgende Option abgebildet werden. Dies ist ein Vorschlag und kann selbstverständlich an die eigene Organisation angepasst werden.*]

Muss ein Passwort zurückgesetzt werden, so erfolgt dies nach einer geeigneten Identitätsprüfung bei einer berechtigten Person, welche dazu befugt ist die Neuvergabe von Passwörtern zu genehmigen oder selbst durchzuführen. Hierbei wird das neue Passwort ausgehändigt. In solchen Fällen sollte auf ein Einmal-Passwort zurückgesetzt werden, welches nach der ersten Anmeldung geändert werden muss.

## Schulung der Mitarbeiter

Alle Benutzer der IT-Systeme der <Name der Organisation> müssen über die korrekten Vorgehensweisen zum richtigen Umgang mit Passwörtern geschult sein.

Die Schulung sollte den sicheren Umgang mit Passwörtern, mögliche Angriffsszenarien, dazugehörige Präventionsmaßnahmen und die Behandlung von Sicherheitsvorfällen umfassen.

## Genehmigung von Ausnahmen

Sollten die Mindestanforderungen dieser Richtlinie nicht erfüllt werden können, so kann unter Einbeziehung des Informationssicherheitsbeauftragen eine Ausnahmegenehmigung erteilt werden. Diese muss dokumentiert werden.

## Pflichten von Systembetreibern

Eine Passwortübertragung darf nur über verschlüsselte Netze erfolgen.

Beim Zurücksetzen von Passwörtern sollen (falls möglich) nur Einmal-Passwörter verwendet werden.

Gemäß Stand der Technik muss der Passwortspeicher kryptographisch gegen unerlaubten Zugriff schützen.

### Accountsperre

Nach einer vorgegebenen Anzahl ausschließlich fehlerhafter Authentisierungsversuche (max. drei), hat eine Sperrung des Systems für eine definierte oder sich automatisch verlängernde Zeitspanne zu erfolgen. Alternativ kann der Zugang dauerhaft gesperrt werden. Dieser darf nur durch eine berechtigte Person wieder freigeschaltet werden.

### Zweifaktorauthentifizierung (2FA)

Systeme mit erhöhtem Schutzbedarf sind mit der Zweifaktorauthentifizierung abzusichern (z.B. VPN Zugang mit Passwort und Smartcard). Hier werden üblicherweise sowohl die Eingabe eines Passworts, als auch ein zweiter Faktor benötigt (z.B. eine Smartcard; ein zusätzlicher Code auf dem Handy oder ein biometrischer Fingerabdruck). Alle Faktoren müssen vor dem Missbrauch durch Dritte geschützt werden. Zu beachten ist, dass die Faktoren sowohl aus unterschiedlichen Kategorien stammen als auch zwei der drei Kategorien erfüllen müssen: Wissen (Code), Besitz (Smartcard) und Biometrie (Gesichtserkennung).