Passwort-Richtlinie des Sehbehinderten- und Blindenzentrums Südbayern (SBZ)

Stand: 5.12.2023

1. Zweck

Diese Passwortrichtlinie dient dazu, klare Regeln für die Erstellung von Passwörtern und den sicheren Umgang mit denselben festzulegen.

2. Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeiter*innen, Auftragnehmer*innen und sonstige Dritte, die auf die Systeme, Netzwerke und Daten des Sehbehinderten- und Blindenzentrum Südbayern e.V. (im Folgenden SBZ) zugreifen.

3. Verantwortlichkeiten

Der Vorstand ist für die Implementierung, Überwachung und Fortschreibung dieser Richtlinie verantwortlich.
Alle Mitarbeiter*innen, Auftragnehmer*innen und sonstige Dritte sind verpflichtet, diese Richtlinie zu befolgen und jegliche Verstöße dem Vorstand zu melden. Sie sollen zudem Anpassungsbedarfe der Richtline anregen.

4. Zielsetzung

Beim SBZ werden viele unterschiedliche digitale Endgeräte genutzt. Auf diesen Geräten werden üblicherweise viele personenbezogene Daten verarbeitet. Zugang und Zugriff zu diesen personenbezogenen Daten dürfen nur berechtigte Personen haben.
Um dies zu gewährleisten, werden Passwörter – hierzu zählen auch Persönliche Identifikationsnummern (PIN) eingesetzt.
Erst nachdem eine angemessene Identifikation und Authentisierung des zugreifenden Benutzers erfolgt ist, kann ein Zugriff zu den jeweiligen IT-Systemen und Diensten erfolgen.
Ein sicheres Passwort ist unabdingbar, um einen unbefugten Zugang zu Daten zu verhindern. Da das Passwort personenbezogen und geheim ist, liegt es in der Pflicht des Nutzers, ein sicheres Passwort zu erstellen, das soweit wie möglich sicher davor ist, erraten oder ermittelt zu werden.
Dies ist ein wichtiger Beitrag um damit die Informationssicherheit in der Organisation aufrecht zu erhalten.

5. Risiken bei Nichtbeachtung

Bei einer Nichtbeachtung der nachfolgenden Hinweise kann es dazu kommen, dass Daten von unberechtigten Personen eingesehen, bearbeitet und/oder verbreitet werden können.
Dies stellt eine schwere Verletzung des Datenschutzes dar und führt zu einer Verletzung der Rechte der betroffenen Personen.
Zudem können Daten für einen legitimen Zugriff – beispielsweise durch Verschlüsselung – gesperrt werden und damit eine notwendige betrieblichen Nutzung verhindert werden. (Cyber-Angriff)

6. Regelungen für Passwort-verarbeitende Anwendungen

Um eine angemessene Passwortsicherheit zu gewährleisten, werden durch die passwortverarbeitenden Anwendungen und IT-Systeme in der Regel folgende Rahmenbedingungen sichergestellt:

- Erstanmeldung:
  - Jeder Benutzer erhält ein individuelles Passwort für die Erstanmeldung.
  - Nach der Erstanmeldung ist ein Passwortwechsel erforderlich.
- Jeder Nutzer hat immer die Möglichkeit, sein eigenes Passwort zu ändern.
- Hat ein Passwort-Wechsel stattgefunden, kann das Passwort für die Dauer eines Tages nicht erneut geändert werden.
- Passwörter dürfen nicht mehrmals genutzt werden; dies wird mittels einer Passwort-Historie sichergestellt.
- Bei der Erstellung des Passwortes wird der Nutzer unterstützt, indem er Hinweise zur Passworterstellung und –qualität erhält.
- Bei erfolglosen Anmeldeversuchen ist nicht erkennbar, ob die falsche Eingabe das Passwort oder die Nutzerkennung betrifft:
- Nach mehreren erfolglosen Anmeldeversuchen erfolgt eine Sperrung für eine bestimmte Zeitspanne.
- Ein Passwort-Wechsel wird nach einer festgelegten Frist erzwungen.
- Zusätzlich zur Authentifizierung durch Benutzername und Passwort ist eventuell ein weiterer individuell generierten Authentifizierungsfaktor (Multi-Faktor-Authentifizierung – MFA) notwendig

7. Umgang mit Passwörtern

Soweit nicht durch die jeweiligen Anwendungen und Systeme bestimmte Vorgehensweisen erzwungen werden (s. 6.) sind bei der Nutzung von Passwörtern von den Benutzern folgende Regelungen zu beachten, um eine sichere Verwendung zu gewährleisten:

- Voreingestellte Passwörter und Kennungen sind schnellstmöglich durch individuelle Passwörter und Kennungen zu ersetzen.
- Die Passwörter sind geheim zu halten, d.h.
    - Die Weitergabe von Passwörtern ist untersagt.
    - Die Speicherung von Passwörtern auf programmierbaren Funktionstasten von Tastaturen oder Mäusen ist nicht gestattet.
    - Die Speicherung in Browsern, auf lokalen Geräten und in Cloud-Speichern ist grundsätzlich unzulässig. Dies ist ausschließlich in einem Passwortmanager (s. 10.) erlaubt.
    - Passwörter dürfen nicht auf Notizzetteln o.ä. hinterlegt werden.
    - Bei der Eingabe des Passwortes ist darauf zu achten, dass die Eingabe unbeobachtet erfolgt.
    - Ein Passwort-Wechsel ist zwingend notwendig, wenn das Passwort einer unautorisierten Person bekannt geworden ist oder ein solcher Verdacht besteht.
- Jedes Passwort darf nur einmal genutzt werden.
- Bei Verdacht, dass das Passwort Unbefugten bekannt geworden ist und ein Account zu einer unzulässigen unberechtigten Nutzung genützt werden könnte, d.h. „kompromittiert“ ist, ist dies umgehend zu melden.

8. Erstellung von Passwörtern

Der Nutzer hat bei der Erstellung von Passwörtern auf Folgendes zu achten:

- Ein Passwort sollte keine Informationen aus dem beruflichen oder persönlichen Umfeld enthalten wie z. B. Namen oder Geburtsdaten.
- Für jede Anwendung sowie jedes System ist ein eigenes Passwort zu verwenden (z. B. unterschiedliche Passwörter für den Zugriff auf das Benutzerkonto und auf Schulverwaltungs-Software).
- Passwörter dürfen nicht geteilt werden. Die bewusste Verwendung desselben Passworts durch mehrere Personen („Gruppenpasswörter“) ist nicht erlaubt.
- Bereits genutzte Passwörter dürfen nicht wiederholt genutzt werden.
- Eine Verwendung von Trivialpasswörtern und üblichen Zeichenketten ist nicht erlaubt.

9. Stärke von Passwörtern, Passwortwechsel

Die Stärke hängt von der Länge des Passworts und den verwendeten unterschiedlichen Zeichenarten ab. Eine Mischung von Groß-/Kleinbuchstaben, Sonderzeichen, Buchstaben und Ziffern ist sinnvoll.
Ein starkes Passwort kann man bedenkenlos über Jahre hinweg nutzen. Passwörter, die nicht mindestens 12 Zeichen lang sind, sind einmal pro Jahr zu ändern.
Je nachdem wo ein Passwort eingesetzt wird, ist eine unterschiedliche Passwortstärke notwendig. So können Passwörter, die im Rahmen von Mehr-Faktor-Authentifizierungen eingesetzt werden, eine geringere Stärke haben als solche, die alleiniger Sicherheitsfaktor sind.
Falls keine zusätzlichen Authentifizierungsfaktoren vorgesehen sind, muss das Passwort mindestens 12 Zeichen lang sein.

10. Passwort-Manager

Passwort-Manager gestatten es dem Anwender, sichere Passwörter zu generieren, zu speichern und zu verwalten, diese vor unberechtigtem Zugriff zu schützen und trotzdem bequem nutzen zu können.
Beim SBZ wird folgender Passwort-Manger zentral bereitgestellt: *KeePass.*
Dieser Passwort-Manager bietet folgende Eigenschaften:

- Die Länge und die Zeichenzusammensetzung der hinterlegten Passwörter ist nicht eingeschränkt.
- Ein Zugriff auf die Passwörter ist nur möglich, wenn vorher ein Master-Passwort eingegeben worden ist.
- Der Passwort-Manager speichert die Passwörter verschlüsselt ab.

Hilfestellungen und Anleitungen finden Sie unter: **https://keepass.info**

Beschlossen durch den Vorstand am 5.12.2023