Passwortrichtlinien

1. Allgemeine Anforderungen an Passwörter

Alle Benutzerinnen und Benutzer, die auf IT-Systeme und Netzwerke der GBW zugreifen, müssen sichere Passwörter verwenden, um unbefugten Zugriff zu verhindern. Die Passwortrichtlinien basieren auf aktuellen Best Practices zur Informationssicherheit und erfüllen die Anforderungen des revidierten Datenschutzgesetzes (nDSG).

1.1 Mindestanforderungen an ein sicheres Passwort

Ein Passwort muss:

- Mindestens 8 Zeichen lang sein
- Gross- und Kleinbuchstaben enthalten (z. B. "aA")
- Mindestens eine Zahl (0-9) enthalten (z. B. "7")
- Mindestens ein Sonderzeichen enthalten (z. B. "!@#$%^&*()_+")
- Nicht den eigenen Vor- oder Nachnamen enthalten
- Nicht häufig verwendete oder leicht erratbare Wörter oder Kombinationen enthalten (z. B. "Passwort123")

1.2 Passworthistorie und Wiederverwendung

- Ein neues Passwort darf nicht identisch mit den letzten 5 Passwörtern sein.
- Die Passwörter müssen alle 12 Monate erneuert werden.

2. Verwaltung und Änderung von Passwörtern

2.1 Passworterstellung und -änderung

- Das Passwort wird bei der ersten Anmeldung gesetzt und kann über das Schulintranet (**https://intranet.gbwetzikon.ch**) geändert werden.
- Falls ein Passwort vergessen wurde, kann über das Intranet ein temporäres Passwort per SMS angefordert werden.
- Nach dem Erhalt des temporären Passworts muss sofort ein neues, sicheres Passwort gesetzt werden.

2.2 Passwort-Sperrmechanismen

- Nach 5 fehlgeschlagenen Anmeldeversuchen unter MS365 wird das Benutzerkonto für 30 Min. gesperrt.

3. Verhaltensregeln für den sicheren Umgang mit Passwörtern

- Passwörter **dürfen nicht weitergegeben** oder gemeinsam genutzt werden.
- Passwörter dürfen **nicht schriftlich** (z. B. auf Papier oder Post-its) notiert werden.
- Die Speicherung von Passwörtern in **unsicheren digitalen Dokumenten (z. B. Word, Excel, Notepad)** ist untersagt.
- Falls ein Passwort kompromittiert wurde, muss es **sofort geändert** und der **IT-Support benachrichtigt** werden.

- Passwörter können auch mit **Passwortmanagern** wie «Keeper», «Bitwarden», «1Password», «Dashlane» oder anderen Softwareanbietern abgespeichert werden. Dafür muss sich der Benutzer nur noch 1 Passwort merken und alle anderen Passwörter werden im Datensafe gespeichert.

4. Sonderregelungen für Administratoren und IT-Systeme

Für IT-Administratoren und Systemkonten gelten strengere Anforderungen:

- Passwörter müssen mindestens **10-12 Zeichen** enthalten.
- Ein **zweiter Faktor (2FA)** muss für administrative Zugänge immer aktiviert sein.
- **Systempasswörter müssen mind. alle 6 Monate geändert werden.**