

Informationen zum Umgang mit Passwörtern nach der neuen Richtlinie der Freien und Hansestadt Hamburg zur Authentisierung von Personen und technischen Entitäten (Authentisierungsrichtlinie – RAuPE)

Zum 01.05.2024 tritt die Richtlinie der Freien und Hansestadt Hamburg zur Authentisierung von Personen und technischen Entitäten (Authentisierungsrichtlinie – RAuPE) in Kraft und ersetzt die bisher gültige Richtlinie zur Verwaltung von Passwörtern (Passwortrichtlinie – Passwort-RL) vom 10.10.2007.

Die Authentisierungsrichtlinie wird im [SharePoint bei den IT-Vorschriften](#) bereitgestellt.

Wichtigste Neuerungen der Richtlinie für Sie als Anwendende sind:

- Für die Anmeldung zu IT-Systemen der FHH ist nun ein kurzes, aber komplexes Passwort mit der Mindestlänge von 10 Stellen unter Verwendung von vier verschiedenen Zeichenarten (Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen) zu verwenden.
- Passwörter müssen nicht mehr turnusmäßig nach 90 Tage erneuert werden, sondern gelten im Normalfall dauerhaft.
- Für die gängigen IT-Systeme der FHH bleibt es zunächst bei der Authentisierung mittels eines Passwortes, aber auf Grundlage der Regelungen in der Richtlinie können zukünftig auch Multi-Faktor-Authentisierungen (MFA) realisiert werden.

Weitere Schritte:

- In einer Übergangszeit zwischen dem 01.05.2024 und dem 30.06.2024 können Sie weiterhin Ihr bisheriges Passwort zur Anmeldung verwenden.
- Ab dem 01.07.2024 wird die technische Umsetzung der oben genannten Neuerungen durch Dataport erfolgen. Das bedeutet, sobald Ihr nächster bisher turnusmäßiger Passwortwechsel (nach 90 Tagen) ansteht, gelten die neuen oben genannten Vorgaben für Ihr neues Passwort (mindestens 10 Zeichen unter Verwendung von vier verschiedenen Zeichenarten).

Für Ihr neues dauerhaftes Passwort orientieren Sie sich bitte an den Vorgaben für ein kurzes, aber komplexes Passwort des Faktenblattes für Sichere Passwörter des Bundesamtes für Sicherheit in der Informationstechnik – BSI (siehe Anlage1 und unter [BSI - Faktenblatt PW](#))¹.

¹ Empfehlungen zu MFA können zurzeit systemseitig noch nicht gefolgt werden.

Anlage 1:



BSI-Basischutz: Sichere Passwörter

Passwörter begleiten uns täglich und trotzdem oder gerade deshalb greifen viele Menschen bei der Wahl ihrer Passwörter auf einfache Zahlenabfolgen oder Namen und Orte in Kombination mit Zahlen oder Sonderzeichen zurück. Diese sind zwar leicht zu merken, können aber ebenso leicht von Cyber-Kriminellen geknackt werden.

Bei einem Cyber-Angriff sind nicht nur persönliche Daten und sensible Informationen in Gefahr, Cyber-Kriminelle können die gehackten Accounts auch für kriminelle Machenschaften und illegale Geschäfte nutzen. Um das zu verhindern, sollte ein Passwort bestimmte Anforderungen erfüllen und immer nur für einen Zugang genutzt werden.

Grundsätzlich können Sie zwei Strategien anwenden, um ein sicheres Passwort zu erstellen:



Weitere Informationen:

<https://www.bsi.bund.de/dok/6596574>

Sicheres Passwort



Kurzes, dafür komplexes Passwort

- Ist acht bis zwölf Zeichen lang.
- Besteht aus vier verschiedenen Zeichenarten.
- Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen werden willkürlich aneinander gereiht.

Langes, dafür weniger komplexes Passwort

- Ist mindestens 25 Zeichen lang.
- Besteht aus zwei Zeichenarten.
- Kann zum Beispiel aus sechs aufeinanderfolgenden Wörtern bestehen, die jeweils durch ein Zeichen voneinander getrennt sind.

Um ihre Accounts und Daten zu schützen, sollten Sie außerdem folgende Tipps beherzigen:

Generell gilt



- ✓ Ein individuelles Passwort pro Account!
- ✓ Eine Mehr-Faktor-Authentisierung (ergänzend zum Passwort durch bspw. eine Gesichtserkennung, eine App-Bestätigung, E-Mail oder einer PIN auf einem anderen Gerät) ist empfehlenswert.
- ✓ Alle verfügbaren Zeichen nutzen inklusive Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen (Leerzeichen, ?!%+...).
- ✓ Das vollständige Passwort sollte nicht im Wörterbuch vorkommen.

Zu vermeiden



- ✗ Namen von Familienmitgliedern, Haustieren, Geburtsdaten etc.
- ✗ Einfache oder bekannte Wiederholungs- bzw. Tastaturmuster wie „asdfgh“ oder „1234abcd“
- ✗ Ziffern oder Sonderzeichen an den Anfang oder ans Ende eines ansonsten einfachen Passwortes.
- ✗ Dasselbe Passwort bei mehr als einem Account.

