FH;P Fachhochschule Potsdam
University of
Applied Sciences

Passwort-Richtlinie

Fachhochschule Potsdam

Dokumentenname:	passwortrichtlinie-fachhochschule-potsdam-c-it-sicherheit-fhpotsdam-2022-09-01
Version/Änderungsdatum:	Version 1.0 / 01.08.2022
Geltungsbereich:	alle Einrichtungen der FH Potsdam
Verantwortlich:	Informationssicherheitsbeauftragter
Revision:	jährlich
Klassifizierung:	intern

Inhaltsverzeichnis

1. Präambel

Das Informationssicherheitsmanagement der Hochschule ist verantwortlich für die Planung und Implementierung von Richtlinien zum Schutz von Daten insbesondere vor deren Verlust, Schäden oder Diebstahl. Die Vergabe von sicheren Passwörtern spielt dabei im Bereich IT-Sicherheit und Datenschutz eine essenzielle Rolle. Bei der Umsetzung hilft eine sinnvolle Passwortrichtlinie. Festgelegte aktuelle Vorgaben zur Passwortvergabe werden darin festgehalten. Mithilfe einer festgeschriebenen Passwortrichtlinie können sich Mitarbeitende, Studierende und Externe über geltende Passwort-Vorgaben informieren, diese entsprechend umsetzen und sind so davor geschützt, z. B. in Folge schwacher Passwörter oder Passwortverlust Ziel eines Cyber-Angriffs zu werden.

1.1 Zielsetzung

Um die Sicherheit der IT-Infrastrukturen sowie der IT-gestützten Hochschulprozesse zu gewährleisten und somit Schaden von der Hochschule möglichst abzuwenden, ist ein sicheres Passwort-Management sowie der sichere Gebrauch von Passwörtern notwendig. Dieses Dokument beschreibt die Passwort - Regeln für alle IT-Systeme und Nutzer innerhalb der Hochschule.

1.2 Geltungsbereich

1.2.1 Persönlicher Geltungsbereich

Der persönliche Geltungsbereich erstreckt sich auf alle Nutzerinnen und Nutzer der IT-Infrastruktur der Fachhochschule Potsdam.

1.3 Definitionen

Begriff	Definition
Passwörter	Passwörter sind geheime Authentisierungsinformationen und dienen zur Verifikation der Identität eines Benutzers.
Anwender	Anwender dieser Passwortrichtlinie sind Nutzer von IT-Infrastrukturen, Systemen oder Anwendungen der Hochschule.

2. Passwortverwaltung

Die Verfahren zur Bereitstellung und Verwaltung von Benutzer-Passwörtern müssen gewährleisten, dass zugewiesene Zugangsberechtigungen und -beschränkungen wirksam geschützt sind. Ausnahmen von den hier definierten Grundsätzen bzw. Verfahren müssen schriftlich beantragt werden und bedürfen der Freigabe durch den Informationssicherheitsbeauftragten (ISB) z.B. bei der Verwendung von Gruppenkonten oder unbegrenzter Gültigkeit. Diese Ausnahmen werden im ISMS dokumentiert.

2.1 Anforderungen an die Passwortverwaltung

Nachfolgende Grundsätze sind bei der Verwaltung von Passwörtern anzuwenden:

- Es sind vorrangig personalisierte Nutzerkonten anzuwenden. Zugehörigkeiten zu Funktionalaccounts sind in geeigneter Weise zu dokumentieren.
- Alle intern genutzten Passwörter sind vollständig und ausschließlich in geeigneter Weise, vor Fremdzugriffen geschützt, zu speichern. Vorzugsweise kann dies in einem Passwortmanager wie „KeePass Password Safe“ (einem Programm zur Sicheren Speicherung von Passwörtern) erfolgen. Bei den Passwort-Tresoren müssen Master-Passwörter aktiviert sein.
- Erstmalig übergebene Passwörter werden als einzigartige, temporäre Initial-Passwörter erstellt und müssen bei der ersten Anmeldung vom Nutzer selbstständig geändert werden.
- Temporäre Passwörter müssen dem Nutzer auf eine sichere Weise, kommuniziert werden. Die Identität der Nutzer muss überprüft werden, bevor die Übergabe von Anmeldedaten und Passwörtern erfolgt.
- Passwörter dürfen nicht unverschlüsselt (im Klartext) gespeichert oder unverschlüsselt über das Netzwerk übertragen werden.
- Es ist sicherzustellen, dass nur Passwörter verwendet werden können, die den in diesem Dokument genannten Qualitätsanforderungen entsprechen.
- Eine erneute Verwendung der mindestens 5 zuletzt verwendeten Passwörter sollte verhindert werden.
- Fehlerhafte Anmeldeversuche werden protokolliert und werden nach maximal 30 Versuchen temporär für mindestens 15 Minuten gesperrt werden.
- Bekannte unsichere Passwörter können nicht genutzt werden. z.B. welche die auf https://haveibeenpwned.com/ veröffentlicht wurden. Für Zentrale Accounts erfolgt diese Prüfung automatisiert im Hintergrund.

2.2 Anforderungen an Passwörter

Um Daten zu stehlen und auf verschiedene passwortgeschützte Dienste Zugriff zu erhalten, nutzen cyberkriminelle Werkzeuge, die vollautomatisch alle möglichen Zeichenkombinationen ausprobieren, ganze Wörterbücher einschließlich gängiger Kombinationen aus Worten und angefügten Zahlen testen oder einmal im Internet veröffentlichte Zugangsdaten bei allen möglichen Diensten durchprobieren. Um das zu verhindern, sollte ein Passwort bestimmte Qualitätsanforderungen erfüllen und immer nur für einen Zugang genutzt werden. Sichere Passwörter dürfen daher keine Zeichenwiederholungen (z.B. aaa, 111), Zahlen und Daten aus dem Lebensbereich des Nutzers wie Namen von Haustieren, Verwandten, Geburtsdaten etc., Zeichenkombinationen, die nur unwesentlich von den vorherigen Passwörtern abweichen, einfache Ziffern- und Buchstabenkombinationen (ABC123), Zeichen, die durch nebeneinanderliegende Tasten eingegeben werden (Qwertz) und Zeichenkombinationen, die Suchbegriffen in Wörterbüchern und Lexika entsprechen (Trivialpasswörter) enthalten.

Sichere Passwörter müssen sich außerdem wie folgt zusammensetzen:

- Mindestens **8-12 Zeichen und 4 Zeichenarten**

  Beispiel %st3g><T2
  oder H0nd+Kuch3n

oder

- Mindestens **13 Zeichen und 3 Zeichenarten**

  Beispiel 9JGTCBYNmc3Ts
  oder Hund+Kuchen+Apfel

oder

- Mindestens **20 Zeichen und 2 Zeichenarten**

  Beispiel cawCyvBekVjpxrfmfATv
  oder hund-kuchen-apfel-birne

  Zeichenarten sind:
  1. Kleinbuchstaben (a-z)
  2. Großbuchstaben (A-Z)
  3. Ziffern (0-9)
  4. Sonderzeichen () [] {} ? ! = * + , . : < > - _

Passwörter sind prinzipiell mit einer unbegrenzten Gültigkeitsdauer zu erstellen. Der Wechsel sollte nur in begründeten Fällen erzwungen werden (z. B. Verlust des Passwortes). Werksseitige Standard - Passwörter (z. B. von Firewalls, Access Points, Managed Switches) von Software- oder Hardware Herstellern müssen bei der erstmaligen Einrichtung oder Übergabe nach Auftrags- oder Projektabschluss geändert werden.

2.3 Passwörter für privilegierte Zugriffsberechtigung

Mit der Nutzung von privilegierten Zugangsberechtigungen (z. B. Kennungen zur Administration von IT-Systemen, Software oder IT-Infratrukturen) sind höhere Risiken bezüglich des Verlustes vertraulicher Informationen, der Verfälschung von Daten oder des Datenverlustes verbunden. Aufgrund dieser höheren Kritikalität gelten für solche Passwörter neben den Anforderungen aus Abschnitt 2.2 weitergehende Anforderungen an die Komplexität und den Zugangsschutz. So ist hier eine Passwort-Länge von mindestens 12 Zeichen und 4 Zeichenklassen vorgeschrieben ebenso wie die Hinterlegung eines Super-Admin-Accounts an einem gesicherten Ort und Benennung der Zugangsberechtigten für den Notfall. Die Zugangsdaten zu diesem Notfallaccount sollten ausgedruckt und in geeigneter Weise licht-, wasser-, und feuergeschützt gelagert werden. Nach Möglichkeit sind

diese Zugänge in einer Passwortdatenbank offline abzulegen, um im Bedarfsfall für Vertretung oder Notfallkontakt einen einfachen Zugang zu ermöglichen.

3. Verwaltung von anderen Authentifizierungsinformationen

In Fällen, in denen die Verwendung von Benutzername und Passwort aus technischen Gründen nicht möglich ist, sind alternative Verfahren zulässig. Hier sind alphanummerische Passwörter, PINs: (mindestens vierstellig, Begrenzung der Falscheingaben auf max. 5 Versuche, keine einfach einzugebenden PINs, wie 1234, 0000, 2580, 0852, 1212, oder Geburtsdaten/Jahreszahlen) sowie biometrische Merkmale, wie Fingerabdruck oder Gesichtserkennung zu nennen.

Nicht zulässig sind unabhängig vom Anwendungsfall (Wisch-)Muster.

4. Pflichten der Anwender

Für den sicheren Umgang mit Zugangsdaten und Passwörtern sind alle Nutzer selbst verantwortlich. Passwörter sind unbedingt geheim zu halten. Sie dürfen gegenüber anderen Personen nicht offengelegt werden; auch nicht für Abwesenheiten oder zeitweilige Vertretungen. Die Doppelnutzung für Passwörter zu verschiedenen Zwecken ist zu unterlassen. Passwörter, die für dienstliche Zwecke genutzt werden, sollten nicht zusammen mit Passwörtern für private Zwecke gespeichert werden. Beispielsweise sollten diese nicht zusammen in einem digitalen Passwort-Tresor gespeichert werden.

Bei Vergessen des Passworts steht den Studierenden eine durch das Rechenzentrum bereitgestellte Passwort-Vergessen-Funktion zur Verfügung, Mitarbeitende können sich an die dezentralen Fachadministratoren oder die Zentrale IT wenden, welche die Vergabe eines neuen Passwortes ermöglicht. Grundsätzlich sollte der Nutzende sein neues Passwort selbst nach den entsprechenden Qualitätsanforderungen eingeben. Ist dies nicht möglich, wird durch den IT-Mitarbeiter ein temporäres Passwort vergeben, mit dem Hinweis, dass der Nutzer anschließend unverzüglich das Passwort selbst ändern soll.

Falls es Anzeichen dafür gibt, dass Zugangsdaten, Passwörter oder IT-Systeme kompromittiert sein könnten, muss dies als Sicherheitsvorfall an das Informationssicherheitsmanagement der Hochschule gemeldet werden. Die betreffenden Passwörter sind umgehend zu ändern.

5. Inkrafttreten und Veröffentlichung

Diese Richtlinie tritt am Tag nach ihrer Veröffentlichung in Kraft. Sie wird allen Hochschulangehörigen dauerhaft und in aktualisierter Form zur Verfügung gestellt.

Potsdam, 01.08.2022

elektronisch gezeichnet

Maximilian Budwill (Informationssicherheitsbeauftragter ISB)
(informationssicherheit@fh-potsdam.de)