Passwörter

Für die Passwörter eines Benutzerkontos gelten folgende Richtlinen und Empfehlungen:

Einstellung	Richtlinie	Beschreibung / Empfehlung
Mindestzahl an Zeichen	12 Zeichen	Passwort muss mindestens 12 Zeichen lang sein
Mindestzahl eindeutiger Zeichen	4 Zeichen	Passwort muss mindestens 4 Zeichen enthalten, die nur 1 Mal vorkommen
Höchstanzahl an Wiederholungen eines bestimmten Zeichens	4 Zeichen	Passwort kann maximal 4 gleiche aufeinanderfolgende Zeichen enthalten
Mindestanzahl an Großbuchstaben	1 Zeichen	Passwort muss mindestens 1 Großbuchstaben enthalten
Mindestanzahl an Kleinbuchstaben	1 Zeichen	Passwort muss mindestens 1 Kleinbuchstaben enthalten
Mindestanzahl an Zahlen	1 Zahl	Passwort muss mindestens 1 Zahl enthalten
Mindestanzahl an nicht-alphanumerischen Zeichen (! + -)		Passwort sollte mindestens 1 Sonderzeichen enthalten
Gültigkeitsdauer des Passworts		Passwort sollte alle 365 Tage gewechselt werden

- **Nicht-alphabetische Zeichen sind nicht zugelassen (ä ö ü ß Ä Ö Ü)**

Passwortänderung und Rücksetzung

Studierenden empfehlen wir, Ihr Passwort direkt nach dem Erhalt Ihrer Zugangsdaten zu ändern. Desweiteren sollten alle Hochschulmitglieder und -angehörigen Ihr Passwort in regelmäßigen Abständen ändern.

In unserem eIDentity Portal können Sie Ihr Passwort ändern und zusätzlich auch noch weitere Möglichkeiten der Passwortrücksetzung nutzen. Dort können Sie Sicherheitsfragen für den Fall einrichten, dass Sie Ihr Passwort vergessen haben. Ebenfalls können Sie Ihr Smartphone einrichten, um ein vergessenes Passwort zurückzusetzen.

Passwort ändern:

Im eIDentity Portal unter **Anwendung → Passwort ändern** zunächst mit dem aktuellen Passwort anmelden. Anschließend das neue Passwort festlegen, zur Bestätigung wiederholen und auf Passwort ändern klicken.

Bitte beachten Sie, dass sich eine Passwortänderung auf fast alle Dienste auswirkt:

- Collaboration Cloud
- Druckdienste, insbesondere lokal eingebundene Netzwerkdrucker
- E-Mail Konto auf Ihrem iPad, iPhone, PC
- Jade eCampus
- Messaging via Cisco Jabber

- WLAN/Wi-Fi-Zugang eduroam

Hinweis: Unter dem Betriebssystem Microsoft Windows können Sie ihre gespeicherten Passwörter in der Systemsteuerung unter Anmeldeinformationsverwaltung / Windows-Anmeldeinformationen verwalten.

Passwort vergessen

Falls Sie Ihr Passwort vergessen haben, können Sie sich gegen Vorlage eines Lichtbildausweises und eigenhändiger Unterschrift das Zugangsdatenblatt im Hochschulrechenzentrum an einem beliebigen Studienort nochmals ausdrucken lassen. Vergessene Passwörter werden nicht per E-Mail versendet, da wir Ihre Identität nicht überprüfen können.

Alternativ können Sie das eIDentity Portal nutzen, um verschiedene Methoden zur Passwortzurücksetzung zu aktivieren.

Empfehlungen für sichere Passwörter

Bitte verwenden Sie Ihr Passwort ausschließlich für die zentralen IT Systeme der Jade Hochschule. Für die unterschiedlichen Online Angebote sollten Sie jeweils eigene Passwörter nutzen.

Ein guter Einstieg in das Thema sind die Empfehlungen des BSI:

- BSI für Bürger - Passwörter
- BSI für Bürger - Umgang mit Passwörtern

Passwortmanagement

Damit sie Ihre Passwörter sicher speichern und verwalten können, empfehlen wir Ihnen eine Passwortmanagement Software einzusetzen.

KeePass

Beschreibung

KeePass ist grundsätzlich erst einmal ein Programm zur Kennwortverwaltung. KeePass speichert die Benutzernamen / Passwörter und einige andere Daten in einer Datenbank und legt sie verschlüsselt als eine Datei ab. Die wesentlichen Funktionen sind:

- Speichern von Benutzernamen, Passwörtern usw.
- Ablage in einer verschlüsselten Datei
- Öffnen der KeePass Datenbank mit einem (!) Hauptschlüssel (z.B. ein Passwort) oder wahlweise auch mit einem zweiten Faktor (2FA, Passwort und YubiKey)

- Übertragung der Benutzernamen / Passwörter über die Zwischenablage in andere Programme
- Automatische Eingabe von Benutzername und Passwort in die entsprechende Anwendung (z.B. Firefox) über ein globales Tastenkürzel (Auto-Type)
- Automatische Eingabe von Benutzername und Passwort in Firefox über ein PlugIn

Beim ersten Aufruf wird die Datenbank angelegt und der Name für die entsprechende Datei abgefragt. Auch muss jetzt der Hauptschlüssel (z.B. ein starkes Passwort) eingegeben werden.

PC-Software

Eine spezialisierte Variante von KeePass ist KeePassXC. Hierbei handelt es sich um eine Open Source Variante, die für alle drei PC-Betriebssysteme (Apple macOS, Linux, Microsoft Windows) verfügbar ist (Cross-Platform).

KeePassXC kann für alle PC-Betriebssysteme heruntergeladen und installiert werden (für Microsoft Windows eignet sich i.d.R. die „EXE Installer (64-bit)“ Variante).

Apple iOS

Eine spezialisierte Variante von KeePass ist KeePassium. Hierbei handelt es sich um eine Variante, die für Apple iOS optimiert ist.

- Apple App Store: KeePassium

Eine weitere Alternative ist Strongbox:

- Apple App Store: Strongbox

Google Android

Eine spezialisierte Variante von KeePass ist KeePass DX. Hierbei handelt es sich um eine Open Source Variante, die für Android optimiert ist.

- F-Droid: KeePass DX
- Google Play Store: KeePass DX

From:
https://hrz-admin-wiki.jade-hs.de/ - **HRZ-Admin-Wiki**

Permanent link:
https://hrz-admin-wiki.jade-hs.de/de/tp/uadm/passwords

Last update: **2026/08/31 12:37**