

# Passwort ändern

---

## Wichtiger Hinweis für die Mitarbeiter in der Hochschul-Verwaltung

---

Mitarbeiter in der Hochschul-Verwaltung ändern ihr Kennwort nicht auf die unten beschriebene Weise, sondern nach Anmeldung an einem Verwaltungs-Arbeitsplatz-Rechner mittels des dortigen Mechanismusses zum Kennwort-Ändern, spätestens nach Aufforderung durch das System wegen Kennwort-Ablaufs.

## Wo kann ich mein Passwort ändern?

---

Sie finden die Seite, mit der Sie Ihr Passwort ändern können, auf der Homepage des Gauß-IT-Zentrums.

Dazu müssen Sie in der Navigationsleiste auf der linken Seite den Punkt „Self-Service“ auswählen. Anschließend klicken Sie in der Leiste auf „Passwort ändern“.

Alternativ können Sie auch den folgenden Link nutzen, welcher zu der selben Seite führt:

<https://www.tu-braunschweig.de/it/self-service/passwort-aendern>

## Wie kann ich mein Passwort ändern?

---

Um das Passwort zu ändern, müssen Sie bei den Eingabefeldern Ihre Benutzerkennung (z.B. y-Nummer) und ihr altes Passwort eingeben.

Anschließend geben Sie ihr neues Passwort ein und wiederholen dieses.

Wenn Sie das neue Passwort eingegeben haben, müssen sie unten auf der Seite auf **[Abschicken]** klicken.

# Passwort ändern

Benutzerkennung:	<input type="text"/>
bisheriges Passwort:	<input type="password"/>
neues Passwort:	<input type="password"/>
neues Passwort wiederholen:	<input type="password"/>

## Was muss ich beachten wenn ich mein Passwort ändern will? / Richtlinie für Passwörter

Der Umgang mit Passwörtern ist in der [Richtlinie für Passwörter der zentralen Benutzerkennung des Gauß-IT-Zentrums](#) hinterlegt.

Hieraus ergeben sich für die Bildung des Passworts folgende Regeln:

Es muss *Zeichen aus mindestens 3* der folgenden Gruppen enthalten:

- Großbuchstaben **A - Z**
- Kleinbuchstaben **a - z**
- Ziffern **0 - 9**
- folgende Sonderzeichen:

Weiterhin gilt:

- Es darf nicht Teile des Namens oder der Benutzerkennung enthalten, die länger als 2 Zeichen sind
- Es muss 12 bis 30 Zeichen lang sein

- Es darf nicht mit Minuszeichen (-) anfangen
- Es sollte nicht den letzten 10 Passwörtern entsprechen

Wie ein sicheres Passwort gebildet wird, entnehmen Sie bitte der [FAQ#1000795](#) oder den [IT-Sicherheitsinformationen des Gauß-IT-Zentrums](#).

Wir möchten Sie daran erinnern, dass Ihnen die IT-Ressourcen auf Basis universitäts-interner Ordnungen bereitgestellt werden. Durch das Setzen des Häkchens am unteren Seitenrand erkennen Sie an, dass

- die Benutzerkennung und das zugehörige Passwort nicht an Dritte weitergegeben werden darf,
- die Benutzerkennung gemäß der gesetzlichen Bestimmungen (insbes. Urheber-, Datenschutz- und Strafrecht, etc.) und an der TU Braunschweig gültigen Ordnungen und Dienstvereinbarungen zu nutzen ist, das bedeutet insbesondere in wirtschaftlicher und dem Zweck angemessener Weise,
- die Benutzerkennung bei Verstößen gegen die Ordnungen zurückgezogen werden kann.

Die aktuelle Fassung der Ordnungen kann auf [dieser Seite](#) eingesehen werden.

## Zusatzprüfung auf "bekannte" (geleakte) Passwörter

---

Ab dem 03.05.2018 (Weltpassworttag) erweitert das GITZ die Passwortprüfung auf der „Passwort ändern“-Seite.

Zusätzlich zu der bereits bekannten Prüfung auf Einhaltung der Passwort-Regeln (siehe oben) wird ab dem 3.5.2018 auf der „[Passwort ändern](#)“-Seite des [GITZ](#) ebenfalls geprüft, ob das gewünschte Passwort eventuell bereits in einer Liste von bereits schon einmal gehackten und bekannt gewordenen Passwörtern enthalten ist. Wenn dies der Fall ist, gilt das Passwort als unsicher, da solche Passwortlisten auch von Hackern für neue Angriffe oftmals verwendet werden.

Das GITZ verwendet dafür den Service der Webseite „[have I been pwned](#)“ ([HIBP](#)) des unabhängigen Sicherheitsforschers [Troy Hunt](#), bei der es sich um die umfassendste, offen zugängliche Sammlung von unsicheren, „geleakten“ Passwörtern handelt. Die Seite wird auch von mehreren Regierungen als Prüfinstanz verwendet ([Heise Newsticker](#), [Engadget](#)).

Der online verfügbare Service von HIBP verwendet einen ausgeklügelten Mechanismus, der sicherstellt, dass das eingegebene Passwort bzw. der daraus erzeugte sog. „Hash“ in keinem Fall vom GITZ an HIBP weiter gegeben wird .

Falls das Passwort bereits in der Liste vorkommt, wird eine Fehlermeldung ausgegeben und das Passwort wird nicht für die Verwendung an der TU Braunschweig akzeptiert:

**Fehler**

Das von Ihnen gewählte Passwort entspricht zwar den Passwort-Richtlinien, wurde aber als leaked eingestuft. Gemäß aktueller Sicherheitsstandards gelten sog. geleakte (also: einmal oder mehrfach öffentlich bekannt gewordene) Passwörter als Sicherheitsrisiko und sollten daher nicht mehr verwendet werden. Bitte wählen Sie ein anderes Passwort.

[Zurück zum Änderungsformular](#)

In diesem Fall muss man ein anderes Passwort verwenden.

## Allgemeine Hinweise zur Passwortlänge

---

Folgende einfache Merkhilfe kann bei der Wahl des Passwortes sehr hilfreich sein:

Man denkt sich einen Satz aus, in dem auch eine Zahl vorkommt:

**W**ir **h**aben **4** **A**utos **i**n **u**nserer **G**arage **s**tehen.

Nun nimmt man von jedem Wort den Anfangsbuchstaben und schon hat man ein relativ sicheres Passwort:

Wh4AiuGs

Bei der nächsten Passwortänderung kann dann z. B. heruntergezählt werden.

Dadurch erhält man ein (für Computer) völlig neues Passwort und muss sich dabei gar nicht viel merken.

---

Revision #6

Created 22 May 2024 13:24:10 by Dennis Lukas

Updated 23 May 2024 09:17:40 by Dennis Lukas