AMTLICHES MITTEILUNGSBLATT

Herausgeber: Der Präsident der Technischen Universität Berlin
Straße des 17. Juni 135, 10623 Berlin
ISSN 0172-4924

Redaktion: Ref. K 3, Telefon: 314-22532

Nr. 13/2021
(74. Jahrgang)

Berlin, den
8. Juli 2021

I N H A L T

II. Bekanntmachungen

Seite

Zentraleinrichtungen

II. Bekanntmachungen

Zentraleinrichtungen

Passwortrichtlinie der Technischen Universität Berlin

vom 23. Juni 2021

Der Direktor der Zentraleinrichtung Campusmanagement hat gem. § 6 der Ordnung für die Organisation und Benutzung des zentralen Dienstleistungszentrums Campusmanagement der Technischen Universität Berlin (ZECM) vom 12. September 2018 (AMBl. Nr. 33/2018 10. Dezember 2018) am 23. Juni 2021 folgende Passwortrichtlinie erlassen.

1. Kurzbeschreibung

Der Zugang zu allen IT-Diensten wird durch Authentifizierungsverfahren abgesichert. Im Regelfall werden dazu passwortbasierte Verfahren eingesetzt. Die vorliegende Sicherheitsrichtlinie regelt den Einsatz, die Verwendung und den Aufbau von Passwörtern für den Einsatz an IT-Systemen der TU Berlin, sowie die Rechte und Pflichten aller Nutzer*innen der IT-Systeme bei der Verwendung von passwortbasierten Authentifizierungsverfahren.

2. Geltungsbereich

Diese Richtlinie gilt für alle Benutzer*innen der TU Berlin, deren Nutzer*innenkonten über das zentrale Provisioning durch die ZECM erzeugt und verwaltet wurden. Grundsätzlich stellt diese Regelung nur den Mindestschutz dar und kann von jeder*m Betreiber*in von IT-Systemen im Bedarfsfall durch strengere Regelungen ergänzt werden.

Für administrative Passwörter innerhalb zentraler Dienste und der ZECM gelten separate, strengere Vorschriften.

3. Vorgaben für Passwörter

Grundsätzlich müssen für jedes Konto verschiedene Passwörter verwendet werden. Eine doppelte Verwendung des gleichen Passworts ist unzulässig.

Für Passwörter gelten die folgenden Regeln:

- Das Passwort hat eine **Länge von mindestens 10 Zeichen**.
- Das Passwort besteht aus jeweils **mindestens einem Zeichen dieser vier Zeichengruppen**:
  - o Großbuchstaben, A-Z,
  - o Kleinbuchstaben a-z,
  - o Ziffern 0-9 und
  - o Sonderzeichen ! # $ % \ ( ) * + , - . / : ; = > ? oder Leerzeichen.

    Nicht erlaubt sind aus technischen Gründen:
    o „ (double quote) , (single quote) § < &

Ab einer Länge von 25 Zeichen muss das Passwort **nur aus zwei dieser vier Zeichengruppen** bestehen.

Zusätzlich gilt:

- Gruppen von mehr als zwei Zeichen, die auch in Vornamen, Nachnamen oder Benutzer*innennamen vorkommen, sind unzulässig.
- Es dürfen nicht mehr als zwei gleiche Zeichen in Folge auftreten.
- Gruppen von mehr als drei Zeichen, die der Anordnung des Alphabets oder der Tastatur entsprechen, sind zu vermeiden. Höchstens eine solche Gruppe ist zulässig.

4. Ablauf und Änderung von Passwörtern

Passwörter müssen nach einer dem Schutzbedarf angemessenen Frist gewechselt werden. Die*Der Benutzer*in ist für das Wechseln des Passwortes selbst verantwortlich. Es wird empfohlen das Passwort halbjährlich zu wechseln.

Passwörter müssen außerdem anlassbezogen geändert werden, z.B. nach einem IT-Sicherheitsvorfall oder falls eine weitere Person Kenntnis von dem Passwort erlangt haben könnte.

5. Regeln bei der Verwendung von Passwörtern

Passwörter sind geheim zu halten. Sie dürfen nicht an andere Personen weitergegeben oder diesen zugänglich gemacht werden.

Mitarbeiter*innen der ZECM werden nie telefonisch, per E-Mail oder persönlich nach Passwörtern fragen.

Passwörter sind von Fremden unbeobachtet einzugeben.

Passwörter dürfen nicht unverschlüsselt auf Rechnern gespeichert werden.

Initiale Passwörter oder Passwörter die Nutzer*innen nach der Rücksetzung durch den Helpdesk erhalten sind unmittelbar durch die*den Nutzer*in zu ändern.

6. Inkrafttreten

Diese Richtlinie tritt mit Beschluss des CIO am 23. Juni 2021 in Kraft.