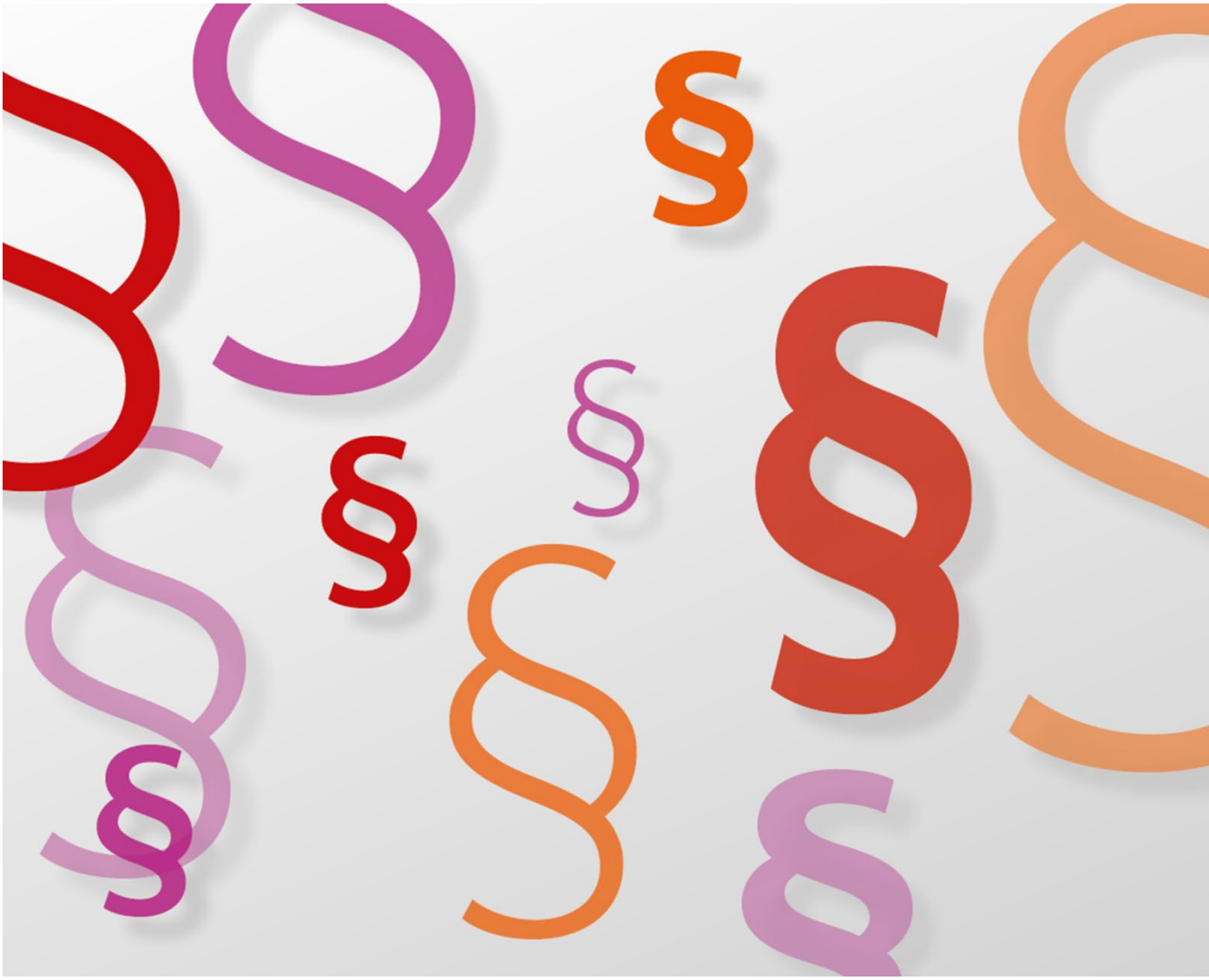

Amtliche Mitteilung Nr. 19/2023

Passwortrichtlinie für die Technischen Hochschule Köln

Vom 21. Juli 2023

Herausgegeben am 6. Oktober 2023

Technology
Arts Sciences
TH Köln

Hinweis:
Es wird darauf hingewiesen, dass gemäß § 12 Abs. 5 des Gesetzes über die Hochschulen des Landes Nordrhein-Westfalen (Hochschulgesetz - HG NRW) eine Verletzung von Verfahrens- oder Formvorschriften des Ordnungs- oder des sonstigen autonomen Rechts der Hochschule nach Ablauf eines Jahres seit dieser Bekanntmachung nicht mehr geltend gemacht werden kann, es sei denn
1) die Ordnung ist nicht ordnungsgemäß bekannt gemacht worden,
2) das Präsidium hat den Beschluss des die Ordnung beschließenden Gremiums vorher beanstandet,
3) der Form- oder Verfahrensmangel ist gegenüber der Hochschule vorher gerügt und dabei die verletzte Rechtsvorschrift und die Tatsache bezeichnet worden, die den Mangel ergibt, oder
4) bei der öffentlichen Bekanntmachung der Ordnung ist auf die Rechtsfolge des Rügeausschlusses nicht hingewiesen worden.

Passwortrichtlinie für die Technische Hochschule Köln

Juli 2023

Campus IT

Inhaltsverzeichnis

1. Geltungsbereich

Diese Passwortrichtlinie gilt für alle Nutzer*innen und Betreiber*innen von IT-Infrastruktur an der Technischen Hochschule Köln.

Sie ist im Rahmen der technischen Möglichkeiten auf alle IT-Systeme und Telekommunikationssysteme anzuwenden, deren Ressourcen und Daten durch Passwörter vor unberechtigtem Zugriff und missbräuchlicher Verwendung oder Veränderung geschützt werden sollen.

Alle technischen Systeme wie Netzwerkswitche, USV, etc., die in einem gekapselten, vom Internet isolierten VLAN's betrieben werden, sind von dieser Regelung ausgenommen. Diese sind durch organisationsbezogene Richtlinien abzusichern.

2. Anforderungen an Passwörter

Allgemeine Anforderungen

- Das Passwort muss mindestens 12 Zeichen lang sein.
- Das Passwort muss jeweils mindestens 1 Zeichen aus den folgenden Zeichenarten enthalten:
  - Großbuchstaben: A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z
  - Kleinbuchstaben: a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z
  - Ziffern: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
  - Sonderzeichen: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ]
- Das erste Zeichen darf kein Sonderzeichen (nicht-alphanumerisches Zeichen) sein.
- Darf kein mehr als 4 Mal hintereinander wiederholtes Zeichen enthalten.
- Es dürfen keine persönlichen Daten, Namen oder die Kennung von Nutzenden enthalten sein.
- Es dürfen keine bekannten Wörter aus einem Wörterbuch verwendet werden

Zusätzliche Anforderungen an Passwörter für administrative Accounts

- Das Passwort muss mindestens 20 Zeichen lang sein.
- Das Passwort stammt aus einem Passwortgenerator.
- Erlaubte Zeichenarten siehe oben.

3. Pflichten der Nutzer beim Umgang mit Passwörtern

Initiale Wahl von Passwörtern

- Für jeden Dienst ist ein eigenes Passwort zu verwenden. Ausgenommen sind Single Sign-on Dienste der CampusIT.

- Durch Administrator*innen oder systemseitig gesetzte Passwörter sind beim darauffolgenden Erstzugriff zu ändern.
- Passwörter sollten möglichst zufällig erzeugt werden. Die Verwendung eines Passwortgenerators in Verbindung mit einem Passwortmanager(*) wird empfohlen.
- Alternativ können Passwort-Sätze verwendet werden, um gut merkbare Passwörter zu erhalten.

Nutzung von Passwörtern

- Bei der Eingabe von Passwörtern ist darauf zu achten, dass die Eingabe nicht beobachtet wird.
- Persönliche Passwörter dürfen nicht an Dritte weitergegeben werden.
- System-Administratorpasswörter dürfen nur den Personen bekannt sein, die sie zur Erledigung der ihnen übertragenen Aufgaben benötigen. Verlässt eine Person den Kreis der berechtigten Personen (beispielsweise durch Verlassen der TH Köln), so sind die betroffenen Passwörter umgehend zu ändern.
- Ein Passwort muss umgehend gewechselt werden, wenn es unautorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht. Eine weitere Verwendung des bisher benutzten ist nicht zulässig.

Aufbewahrung von Passwörtern

- Eine unverschlüsselte Speicherung von Passwörtern auf IT-Systemen ist unzulässig.
- Eine verschlüsselte Speicherung in einem Passwortmanager ist zulässig. Ein geeignetes Tool wird über die TH Köln Apps bereitgestellt.
- Das Notieren von Passwörtern ist zu vermeiden. Ist ein Notieren auf Papier unumgänglich, sind die Unterlagen an einem sicheren, zugangsgeschützten Ort aufzubewahren.
- Die Notfallhinterlegung von Passwörtern in einem Tresor ist zulässig.

Nutzen der Zwei-Faktor-Authentifizierung (2FA)

- Zur Absicherung des Zugriffs auf die IT-Infrastrukturen der TH Köln wird die Aktivierung und Nutzung der Zwei-Faktor-Authentifizierung empfohlen.

4. Technische Maßnahmen

Speicherung und Zugriffsschutz

- Der Zugriff auf den Passwortspeicher ist kryptografisch gemäß dem Stand der Technik gegen unerlaubten Zugriff zu schützen.
- Passwörter dürfen über unsichere Netze nur verschlüsselt übertragen werden.

Intrudersperre und Angriffsschutz

- Es ist ein Verfahren zum Zurücksetzen von Passwörtern zu definieren.
- Eine automatische Accountsperre muss nach 7 Fehleingaben des Passwortes in Kraft treten.
- Sperrfrist des Accounts bei einer automatischen Sperrung beträgt mindestens 15 Minuten.
- Die automatisch erteilte Accountsperre darf (ggf. automatisiert) frühestens nach der Sperrfrist wieder aufgehoben werden.

Qualitätssicherung der Passwörter

- Die/der Betreiber*in von IT-Infrastrukturen kann direkt beim Setzen eines Passwortes technische Maßnahmen zum Überprüfen der geltenden Richtlinie einsetzen.

5. Organisatorische Maßnahmen

- Soweit der Schutzbedarf der Daten und Ressourcen es erfordert, ist von den verantwortlichen Stellen für die Passwörter eine angemessene Länge von mindestens 12 Stellen und eine kürzere Gültigkeitsdauer als 180 Tage dokumentiert festzulegen.
- Alle Nutzer*innen und Betreiber*innen von IT-Infrastruktur sind über den Inhalt dieser Richtlinie zu informieren und entsprechend zu schulen.

6. Inkrafttreten

- Diese Richtlinie tritt am 01.08.2023 in Kraft.
- Es gilt eine Übergangsfrist bis zum 30.09.2023.

(*) Empfehlungen zu einem geeigneten Passwortmanager finden Sie auf den Web-Seiten der Campus IT