Passwortrichtlinie der Technischen Universität Darmstadt

Informationssicherheit TU Darmstadt
Veröffentlichung: 06. Mai 2026

TECHNISCHE UNIVERSITÄT DARMSTADT

!nfoSec
TU Darmstadt

Kennzeichnung

Titel (Dokumentenkürzel):	Passwortrichtlinie der Technischen Universität Darmstadt (PW-RL)
Erstellende:	Johannes Braun / Review: Jochen Becker
Funktion der Erstellenden:	CISO TUDa / Leiter TUDa-CERT
Überarbeitende:	Gerrit Kollegger / Review: Jochen Becker
Funktion der Überarbeitenden:	CISO TUDa / Leiter TUDa-CERT
Versionsnummer:	v04
Letzte Überarbeitung:	06. Mai 2026
Nächstes geplantes Review:	Q2/2029
Erste Freigegabe am / durch:	26. November 2021 (Erstfassung) / Herbert De Gersem, Vizepräsident für Wissenschaftliche Infrastruktur und Digitalisierung
Inkrafttreten:	mit der jeweiligen Veröffentlichung
Klassifizierung:	intern
erechtigte Rollen (Verteilerkreis):	alle Angehörige der TU Darmstadt

Änderungsübersicht

v01	Dezember 2021	Erstveröffentlichung
v02	Dezember 2021	Erweiterung der erlaubten Sonderzeichen
v03	Januar 2026	Entfernung der Obergrenze von Passwortlängen, Erlaubnis von Passphrases, Ergänzung von Regelungen zu 2FA
v04	Mai 2026	Erweiterung der erlaubten Sonderzeichen

Zusammenfassung

Das Ziel dieser Richtlinie (Policy) ist die Sicherstellung eines ausreichenden Sicherheitsniveaus für den Einsatz von Benutzername/Passwort-Verfahren. Die dazu notwendigen grundlegenden Regelungen und Handlungsanweisungen sind im Folgenden angeführt. Die relevanten IT-Grundschutz-Bausteine sind im Literaturverzeichnis am Ende des Dokuments aufgelistet.

Inhaltsverzeichnis

1 Geltungsbereich

Diese Passwortrichtlinie gilt für die von der Technischen Universität Darmstadt (TUDa) betriebene IT-Infrastruktur, bestehend aus Informationsverarbeitungssystemen, Kommunikationssystemen und weiteren Hilfseinrichtungen sowie die Beauftragung von Subunternehmen im Bereich IT-Infrastruktur.
Diese Passwortrichtlinie gilt für alle Nutzenden und Betreibenden von IT-Infrastruktur der Technischen Universität Darmstadt.

2 Passwort Anforderungen

Im Folgenden werden die grundlegenden Gestaltungsrichtlinien für Passwörter festgelegt.

2.1 Allgemeine Passwort Anforderungen

- Ein Passwort muss mindestens 12 Zeichen lang sein.
- Erlaubte Zeichensätze:
  - 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: @ # $ % ^ & * - _ ! + = [ ] { } | \ : ’ , . ? / ‘ ~ " ( ) ; < >
- Es dürfen keine persönlichen Daten, Namen oder die Kennung von Nutzenden enthalten sein.

- Es dürfen keine einzelnen bekannten Wörter aus einem Wörterbuch verwendet werden - auch nicht von Fremdsprachen. Sollte in zufallsgenerierten Passwörtern mit entsprechender Länge zufällig Wörter enthalten sein, so ist dies zulässig.
- Die Nutzung von Passphrases, bestehend aus mindestens 6 aneinandergereihten, zufällig ausgewählten Wörtern ist zulässig.

Damit ergibt sich bei Verwendung der Mindestlänge und zufällig erzeugten Passwörtern eine Entropie von ca. 77 Bit. Passphrases mit 6 Wörtern ergeben je nach Wörterbuch ein etwa vergleichbares Sicherheitsniveau.

2.2 Passwort Anforderungen für administrative Accounts sowie Proxy- und Gateway-Accounts

- Das Passwort muss mindestens 20 Zeichen lang sein.
- Das Passwort stammt aus einem Random-Passwortgenerator (zum Beispiel pwgen 20 oder KeePass).
- Erlaubte Zeichensätze siehe 2.1.

Damit ergeben sich Passwörter mit einer Entropie von ca. 128 Bit.

2.3 Passwort Anforderungen für Verschlüsselungspasswörter

Passwörter werden häufig von Programmen als Input genutzt, um daraus einen Verschlüsselungsschlüssel zur Dateiverschlüsselung abzuleiten[1]. Genaue Sicherheitsanforderungen an Verschlüsselungsschlüssel (insbesondere eine Schlüssellänge von mindestens 128 Bit) sind in der Transport Layer Security Richtlinie [2] zu finden. Es gelten hierfür die folgenden Passwort Anforderungen:

- Das Passwort muss mindestens 20 Zeichen lang sein.
- Das Passwort stammt aus einem Random-Passwortgenerator (zum Beispiel pwgen 20 oder KeePass).
- Erlaubte Zeichensätze siehe 2.1.

Damit ergeben sich Passwörter mit einer Entropie von ca. 128 Bit.

3 Rechte und Pflichten beim Umgang mit Passwörtern

Im Folgenden werden die Rechte und Pflichten der Nutzenden von Passwörtern in ihrer jeweiligen Rolle als Anwender:innen oder Administrator:innen beschrieben.

3.1 Initiale Wahl von Passwörtern

- Für jeden Dienst ist ein eigenes Passwort zu verwenden.[2]
- 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 (bspw. KeePass) wird empfohlen.
- Um gut merkbare Passwörter zu erhalten, können Passwort-Sätze verwendet werden.[3]
- Es sollten möglichst viele der in 2.1 aufgeführten erlaubten Zeichensätze verwendet werden.

[1] A1Tool Empfehlungen sind beispielsweise hier [1] zu finden
[2] Bei Verwendung des TUDa-SSO (Single Sign-On) https://login.tu-darmstadt.de ist dieser als ein Dienst zu betrachten.
[3] Denken Sie sich einen Satz aus und benutzen Sie von jedem Wort nur den 1. Buchstaben (oder nur den 2. oder letzten etc.). Anschließend verwandeln Sie bestimmte Buchstaben in Zahlen oder Sonderzeichen. Ein Beispiel: Morgens stehe ich früh auf und putze meine Zähne drei Minuten lang. Nur die ersten Buchstaben: MsifaupmZdMl. i sieht aus wie 1, & ersetzt das und: Ms1fa&pmZdMl.

3.2 Nutzung von Passwörtern

- Bei der Eingabe von Passwörtern ist darauf zu achten, dass die Eingabe nicht beobachtet wird.
- Passwörter die in den Geltungsbereich dieser Richtlinie fallen dürfen nicht an unsicheren (fremden) Systemen eingegeben werden.
- 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 TU Darmstadt), 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.

3.3 Aufbewahrung von Passwörtern

- Eine unverschlüsselte Speicherung von Passwörtern auf IT-Systemen ist unzulässig.[4]
- Eine verschlüsselte Speicherung in einem Passwortmanager (bspw. KeePass oder KeePassXC) ist zulässig.
- 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.

4 Rechte und Pflichten für Systembetreiber

Betreibende von Authentisierungssystemen haben für ihre Systeme einige grundlegende Regelungen einzuhalten und können darüber hinaus auch weitere Schutzmechanismen etablieren. Systembetreibende können über diese Richtlinie hinausgehende Anforderungen an Passwörter definieren. Diese müssen mindestens das Sicherheitsniveau der vorliegenden Richtlinie erfüllen. Die Einhaltung der Passwortrichtlinie ist soweit technisch möglich systemseitig sicherzustellen. Hierbei ist mindestens die Passwortlänge zu prüfen.

4.1 Speicherung und Zugriffsschutz

- Der Zugriff auf den Passwortspeicher ist kryptografisch gemäß dem Stand der Technik gegen unerlaubten Zugriff zu schützen.
- Bei der Übertragung über unsichere Netze, muss die Übertragung von Passwörtern verschlüsselt erfolgen. Regelungen zu anzuwendenden Verschlüsselungsverfahren finden sich in [2].

4.2 Intrudersperre und Angriffsschutz

- Es ist ein Verfahren zum Zurücksetzen von Passwörtern zu definieren.
- Eine automatische Accountsperre muss nach 5 Fehleingaben des Passwortes in Kraft treten.
- Bei einem Fehlversuch darf kein Hinweis gegeben werden, ob Nutzername oder Passwort falsch sind.
- Sperrfrist des Accounts bei einer automatischen Accountsperrung beträgt mindestens 5 Minuten.
- Die automatisch erteilte Accountsperre darf (ggf. automatisiert) frühestens nach der Sperrfrist wieder aufgehoben werden.

[4] Ausgenommen sind Passwörter, die speziell für den Zweck der Maschine-to-Machine Kommunikation zur wechselseitigen Authentisierung auf den IT-Systemen hinterlegt sind.

4.3 Qualitätssicherung der Passwörter

- Betreibende können direkt beim Setzen eines Passwortes technische Maßnahmen zum überprüfen der geltenden Policy einsetzen. Hierbei ist unter anderem ein Plausibilitätstest, der trivial oder leicht zu erratende Passwörter verhindern soll, möglich.
- Betreibende können automatisierte Testprogramme über den Nutzendenstamm laufen lassen. Diese müssen so gestaltet sein, dass Betreibende zu keinem Zeitpunkt Kenntnis der konkreten Passwörter der Nutzenden erhält. Sollten hierbei ungültige oder unsichere Passwörter detektiert werden, so darf der dazugehörige Account direkt gesperrt werden. Entsprechende Nutzende müssen zur Änderung des Passwortes aufgefordert werden.

5 Regelungen zum verpflichtenden Einsatz von 2-Faktor-Authentisierung (2FA)

Grundsätzlich ist jeder von der TU Darmstadt bereitgestellte und aus dem Internet erreichbare Dienst (bspw. Webanwendungen, VPN) bei dem die Authentisierung mittels Nutzername und Passwort realisiert ist, zusätzlich mittels 2FA abzusichern.

5.1 Sicherheitsniveau des eingesetzten 2FA Verfahrens

Das Sicherheitsniveau des jeweiligen 2FA Verfahrens hängt maßgeblich von der Sicherheit des eingesetzten Sicherheitsbausteins - auch genannt Token - ab, welcher für die Bereitstellung des zweiten Faktors verwendet wird. Das Sicherheitsniveau des Tokens wird als Tokenstufe bezeichnet. An der TUDa werden die folgenden 3 Sicherheitsstufen unterschieden:

- Stufe 1 basis: Selbstregistrierte Software-Token, bspw. TOTP-Verfahren über eine App auf dem Smartphone.
- Stufe 2 mittel: Selbstregistrierte Hardware-Token.
- Stufe 3 hoch: Durch das HRZ nach Identifikation der Person registrierte Hardware-Token.

5.2 Rechte und Pflichten für Nutzende

- Bei Accounts, für die 2FA zur Verfügung steht, ist diese grundsätzlich zu aktivieren. Dies gilt insbesondere für die TU-ID und personengebundene TU-TechIDs (zentrale Nutzendenaccounts an der TUDa).
- Es ist mindestens ein 2FA Verfahren mit Token der Sicherheitsstufe 1 basis zu verwenden. Höherwertige Verfahren können genutzt werden, sofern diese für den jeweiligen Dienst zur Verfügung stehen.

5.3 Rechte und Pflichten für Systembetreibende

- Alle aus dem Internet erreichbaren Dienste sind mit 2FA abzusichern. Für die Bereitstellung geeigneter Verfahren sind die Systembetreibenden verantwortlich. Es wird empfohlen, diese Absicherung mittels Anbindung an das zentralen Single-Sign-On System des HRZ zu realisieren.
- Es muss mindestens ein 2FA Verfahren mit Token der Sicherheitsstufe 1 basis realisiert werden. Systembetreibende können abhängig vom Schutzbedarf des Dienstes Token mit höherer Sicherheitsstufe fordern.
- Auch für Dienste, die nur im Netz der TU Darmstadt verfügbar sind, sollte die Verfügbarkeit von 2FA geprüft und wenn möglich aktiviert werden.
- Betreibende von 2FA-Authentisierungssystemen sollten für Nutzende die parallele Nutzung mehrerer Token ermöglichen (Robustheit gegen Verlust/Defekt eines Tokens). Mindestens ist ein sicherer Wiederherstellungsmechanismus zu etablieren.

5.4 Alternativen zur Absicherung mittels 2FA

Sollte es technisch nicht möglich sein (bspw. bei Legacy-Systemen), einen Dienst mittels 2FA abzusichern, müssen alternative Schutzmaßnahmen mit vergleichbarem Schutzniveau umgesetzt werden. Alternative Schutzmaßnahmen sind:

- Verwendung von gerätespezifischen Passwörtern. Diese Passwörter müssen mindestens die Passwort Anforderungen für administrative Accounts sowie Proxy- und Gateway-Accounts (siehe Abschnitt 2.2) erfüllen. Gerätespezifischen Passwörter sind an die Nutzung auf einem bestimmten Gerät (bspw. Hinterlegung in der E-Mail App auf dem eigenen Laptop) gebunden. Für jedes Gerät ist ein separates Passwort zu verwenden. Solche Passwörter dürfen nicht für die regelmäßige Nutzereingabe, bspw. in einem Webinterface, zur Nutzerauthentisierung genutzt werden.

- Beschränkung der Erreichbarkeit eines Dienstes auf das Netz der TUDa. Ein solcher Dienst darf aus dem Internet nur nach vorheriger VPN-Einwahl erreichbar sein. Falls die Authentisierung bei der VPN-Einwahl mittels Nutzername und Passwort erfolgt, muss die VPN-Einwahl mittels 2FA abgesichert sein.

Alternative Absicherungsmaßnahmen sind anzuzeigen und darzustellen.

6 Ausnahmeregelungen

Empfehlungen in internationalen Standards oder technische Gegebenheiten können eine Abweichung von dieser Richtlinie notwendig machen. Diese Abweichungen sind grundsätzlich zu dokumentieren. Es gelten die folgenden Regelungen.

6.1 Durch internationale Standards begründete Ausnahmen

Ausnahmen zu dieser Richtlinie, die auf zwingend zu unterstützenden internationalen Standards beruhen, sind zulässig, sofern die Standards dem aktuellen Stand der Technik entsprechen. Die Abweichungen sind zu dokumentieren und gegenüber dem CISO der TU Darmstadt anzuzeigen.

6.2 Weitere Ausnahmen

Ausnahmen - außer den zuvor erwähnten - zu dieser Richtlinie (beispielsweise der Verzicht von 2FA auf einem aus dem Internet erreichbaren Dienst) sind zu begründen und zu dokumentieren. Sie sind durch den CISO der TU Darmstadt freizugeben.

Literatur

[1] InfoSec, TU Darmstadt. Handreichung zum sicheren Löschen von Datenträgern. https://www.tu-darmstadt.de/it-sicherheit/regelwerke. 2024.

[2] InfoSec, TU Darmstadt. Transport Layer Security Richtlinie. https://www.tu-darmstadt.de/it-sicherheit/regelwerke. 2024.

[3] BSI. „ORP.4.A8 Regelung des Passwortgebrauchs [Benutzer, IT-Betrieb] (B)“. In: IT-Grundschutz-Kompendium. Bd. Edition 2023. Bundesamt für Sicherheit in der Infromationstechnik. 2023.

[4] BSI. „ORP.4.A11 Zurücksetzen von Passwörtern (S) [IT-Betrieb]“. In: IT-Grundschutz-Kompendium. Bd. Edition 2023. Bundesamt für Sicherheit in der Infromationstechnik. 2023.

[5] BSI. „ORP.4.A12 Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen (S) [IT-Betrieb]“. In: IT-Grundschutz-Kompendium. Bd. Edition 2023. Bundesamt für Sicherheit in der Infromationstechnik. 2023.

[6] BSI. „ORP.4.A21 Mehr-Faktor-Authentisierung (H) [IT-Betrieb]“. In: IT-Grundschutz-Kompendium. Bd. Edition 2023. Bundesamt für Sicherheit in der Infromationstechnik. 2023.

[7] BSI. „ORP.4.A22 Regelung zur Passwortqualität (B) [IT-Betrieb]“. In: IT-Grundschutz-Kompendium. Bd. Edition 2023. Bundesamt für Sicherheit in der Infromationstechnik. 2023.

[8] BSI. „ORP.4.A23 Regelung für passwortverarbeitende Anwendungen und IT-Systeme (B) [IT-Betrieb]“. In: IT-Grundschutz-Kompendium. Bd. Edition 2023. Bundesamt für Sicherheit in der Infromationstechnik. 2023.