Informationssicherheitsrichtlinie zum Umgang mit Passwörtern

Ausfertigungsdatum:

6. August 2025

Stand:

Bislang keine Änderungen

Fundstellen:

Originalrichtlinie vom 6. August 2025: Bekanntmachungen des Rektorats (BekR) Nr. 08/2025, Seite 4ff.

Bei der vorliegenden Version handelt es sich um eine nichtamtliche Lesefassung, in der die oben genannten Änderungssatzungen eingearbeitet sind. Maßgeblich und rechtlich verbindlich ist weiterhin nur der in den Bekanntmachungen des Rektorats veröffentlichte Text.

Inhalt

1 Präambel

[1]Diese Richtlinie definiert die Anforderungen für die Erstellung, Verwendung und Verwaltung von Passwörtern an der Universität Mannheim. [2]Sie dient dem Schutz vertraulicher Informationen, universitärer Systeme und Anwendungen vor unbefugtem Zugriff,

unrechtmäßiger Manipulation und Beeinträchtigung der Verfügbarkeit. [3]Nutzende sind verpflichtet, diese Richtlinien zu befolgen, um die Sicherheit ihrer Konten, der darin enthaltenen Daten und die Integrität der universitären Systeme zu gewährleisten.

2 Geltungsbereich

[1]Diese Richtlinie regelt den Umgang mit Passwörtern und gilt für die gesamte Universität Mannheim; die Anforderungen an die Erstellung von Passwörtern (Nr. 4.1) gelten nur, sofern dies technisch möglich und praktikabel ist (wie z. B. bei der Erstellung des Passworts für die Uni-ID; zu Ausnahmen siehe Nr. 7). [2]Sie gilt für alle Personen, auch Dritte, die Informationen der Universität Mannheim im Rahmen Ihrer beruflichen Tätigkeit verarbeiten bzw. deren informationsverarbeitende Systeme oder Prozesse in diesem Rahmen nutzen.

3 Begriffe

3.1 Authentisierung

Mit der Authentisierung weisen Nutzende eine bestimmte Identität nach, welche das jeweilige System prüfen und verifizieren muss, z.B. durch die Eingabe von Uni-ID und Passwort in die Anmeldemaske.

3.2 Authentifizierung

[1]Unter der Authentifizierung versteht man die technische Überprüfung des Authentisierungsversuchs durch ein System im Hintergrund. [2]Eine Authentifizierung ist erfolgreich, wenn Nutzende und Authentisierungsmerkmal übereinstimmen.

3.3 Autorisierung

Unter Autorisierung versteht man die Zuweisung von Rechten nach einer erfolgreichen Authentifizierung.

3.4 Biometrie

Authentifizierungsmethode basierend auf individuellen körperlichen oder verhaltensbezogenen Merkmalen wie Fingerabdruck, Gesichtserkennung oder Iris-Scan.

3.5 Mehr-Faktor-Authentifizierung (MFA)

Darunter versteht man die Authentifizierung auf Basis von mindestens zwei unabhängigen Faktoren (z.B. Passwort + Token).

3.6 Persönliche Identifikationsnummer (PIN)

Eine PIN ist eine kurze numerische Zeichenfolge, die zur Authentifizierung von Nutzenden dient, insbesondere auf mobilen Endgeräten, Smartcards oder speziellen Authentifizierungstoken.

3.7 Privilegierte Accounts

[1]Privilegierte Accounts umfassen alle Konten, die über erhöhte Zugriffsrechte verfügen, z. B. zur Systemkonfiguration, Benutzerverwaltung oder Installation von Software. [2]Hierzu zählen klassische Systemkonten wie root oder Administrator ebenso wie Sudo-Nutzer, Admin-Rollen in Anwendungen und technische Dienstkonten mit erweiterten Rechten.

3.8 System

[1]Ein System verwaltet oder verarbeitet Informationen. [2]Es kann aus einer oder mehreren Komponenten bestehen (z.B. Hardware, Software, Netzwerke). [3]In dieser Richtlinie fallen unter den Begriff System auch zugangsgeschützte Räumlichkeiten.

3.9 Systembetreibende

Systembetreibende sind Personen, die ein System im Auftrag für die Universität betreiben, z. B. durch die Pflege von Servern, das Einrichten von Benutzerkonten oder das Verwalten eines zentralen Ablagesystems.

3.10 Uni-ID: Persönliche Kennung

[1]Die Uni-ID ist eine persönliche Kennung zur Identifikation von Personen (Mitglieder) an der Universität Mannheim. [2]Sie authentifiziert die Mitglieder der Universität Mannheim und wird zusammen mit dem jeweiligen Passwort als Legitimation benötigt. [3]Die Uni-ID wird unter anderem für die Anmeldung in Portal2 und MyUni-ID benötigt.

3.11 Funktions-ID

[1]Funktions-IDs werden verwendet, z.B. um ein Postfach oder MS Teams zu nutzen, die von mehreren Personen verwendet werden, z. B. ein Sekretariat. [2]Sie ist nicht personalisiert, aber wird einer verantwortlichen Person zugeordnet.

3.12 File-Service-ID

File-Service-IDs dienen dazu, gemeinsam auf einen File-Service zuzugreifen.

3.13 Verwaltungskennung

[1]Die Verwaltungskennung ist eine eigenständige Kennung in der Domäne AD-VERWALTUNG. [2]Sie kommt zur Authentifizierung in der Verwaltung zum Einsatz, u.a. für den Zugriff auf den Terminalserver.

4 Rechte und Pflichten für Anwendende

4.1 Erstellung

- Passwörter müssen mindestens 14 Zeichen lang sein.
- Das Passwort muss mindestens drei der folgenden vier Zeichentypen enthalten: Großbuchstaben (A-Z), Kleinbuchstaben (a-z), Ziffern (0-9) und Sonderzeichen.
- [1]Passwörter dürfen keine leicht erratbaren Informationen wie Namen oder Geburtsdaten enthalten. [2]Die Verwendung mehrerer Begriffe oder deutlich veränderter Schreibweisen (z. B. durch Zahlen oder Sonderzeichen) ist zulässig, wenn die Gesamtkomplexität des Passworts dadurch ausreichend erhöht wird. [3]Im Zweifel haben Nutzende ihr Passwort mit der universitären Passwortprüfung zu überprüfen. [4]Wird das Ergebnis als grün angezeigt, ist das Passwort ausreichend komplex.
- Es dürfen keine Zeichenwiederholungen mit mehr als zwei gleichen Zeichen hintereinander verwendet werden.
- Es dürfen keine Tastaturmuster (wie z.B. QWERTZ) verwendet werden.
- [1]Passwörter müssen für jedes verwendete Konto einzigartig sein. [2]Abweichend davon dürfen Konten oder Geräte im Rahmen einer initialen Konfiguration mit einem identischen Initialpasswort ausgestattet sein, welches nach der ersten Nutzung unverzüglich geändert werden muss.
- Die Nutzung eines Passwortmanagers für die Erstellung von Passwörtern wird empfohlen.

- [1]Wo möglich soll ein weiterer Faktor neben Anmeldungs-ID und Kennwort genutzt werden (MFA). [2]Für Systeme und Funktionen auf der folgenden Webseite https://www.uni-mannheim.de/rl-mfa/ muss ein weiterer Faktor genutzt werden.
- In der Vergangenheit verwendete Passwörter dürfen nicht erneut verwendet werden.
- Passwörter, die im Rahmen eines Datenverlusts (beim Nutzenden oder Dienstanbieter) abgeflossen sind, dürfen nicht mehr verwendet werden.

4.2 Meldepflicht

[1]Verdächtige Aktivitäten müssen unmittelbar beim IT-Support gemeldet werden. [2]Beispiele für verdächtige Aktivitäten sind unter anderem unbekannte Anmeldungen, Informationen über nicht selbst vorgenommene Passwortänderungen, unbekannte Downloads, unerklärlich hohe Auslastung der CPU oder des Arbeitsspeichers, vermehrte Systemabstürze.

4.3 Nutzung

- Bei Verdacht auf Kompromittierung muss das entsprechende Passwort unmittelbar geändert werden (z.B. bei Eingabe von Zugangsdaten im Rahmen eines Phishing-Angriffs, bei Verlust von Geräten etc.).
- Anlassbezogen (z.B. bei einem Sicherheitsvorfall, bei der Aktualisierung der Passwortrichtlinie) darf ein Passwortwechsel durch die Universität Mannheim erzwungen werden.
- Initialpasswörter müssen unmittelbar nach Erhalt geändert werden.
- Beim Ausscheiden von zugeordneten Beschäftigten muss das Passwort einer Funktions-ID zurückgesetzt werden, sofern diese Person Zugang zum Passwort hatte.
- Die Nutzung des universitären WLANs auf privaten Mobilgeräten (z. B. Smartphones) ist nur zulässig, wenn dafür ein separates, speziell für diesen Zweck vergebenes WLAN-Passwort verwendet wird.

4.4 Aufbewahrung von Passwörtern

4.4.1 Speicherung und Weitergabe

- Passwörter sollen nicht auf Papier notiert werden, es sei denn, das Papier ist entsprechend geschützt (z.B. in einem Safe).
- Passwörter dürfen nicht unverschlüsselt auf Systemen gespeichert werden, es sei denn, es besteht eine gleichwertige technische Schutzmaßnahme, die den Zugriff auf

die Datei wirksam verhindert (z. B. geschützte Konfigurationsdateien mit restriktiven Zugriffsrechten).

- [1]Passwörter für personenbezogene Konten sind ausschließlich für die persönliche Nutzung vorgesehen und dürfen nicht an Dritte weitergegeben werden. [2]Passwörter von Konten mit gemeinschaftlicher Nutzung dürfen ausschließlich an andere Befugte weitergegeben werden.
- [1]Passwörter dürfen nicht über unverschlüsselte oder anderweitig ungeschützte Kommunikationskanäle (z. B. unverschlüsselte E-Mails oder öffentliche Chat-Plattformen) weitergegeben werden. [2]Eine Übertragung darf nur über verschlüsselte, authentifizierte und institutionell freigegebene Wege erfolgen.
- Passwörter zu Dateien dürfen nicht über denselben Kommunikationskanal übermittelt werden wie die zugehörigen Dateien.

4.4.2 Passwortmanager

- Wo möglich soll ein Passwortmanager genutzt werden.
- [1]Das Masterpasswort darf nicht gespeichert werden. [2]Es muss bei Aufruf des Passwortmanagers zwingend eingegeben werden.
- Das Masterpasswort muss mindestens 14 Zeichen lang sein (für die Zusammensetzung dieses Passworts gelten die Regelungen in 4.1).
- Wird ein Passwort für einen privilegierten Account in einem Passwort-Manager gespeichert, muss das zugehörige Masterpasswort eine Länge von mindestens 20 Zeichen aufweisen.
- Wenn möglich soll der Passwortmanager mit einem zweiten Faktor geschützt werden.

4.5 Anforderungen für privilegierte Accounts, insbesondere Admin-Accounts

- Das Passwort muss mind. 20 Zeichen lang sein.
- Das Passwort soll mit einem geeigneten Passwort-Generator erstellt werden.
- Der Account dient ausschließlich der Administration von Systemen und darf nicht zum regulären Arbeiten genutzt werden.
- MFA soll für privilegierte Accounts eingesetzt werden.
- Bestehen Unsicherheiten darüber, ob die Anforderungen für privilegierte Accounts zutreffen, muss vorsorglich ein Passwort mit mindestens 20 Zeichen gewählt werden.

5 Weitere Authentisierungsmöglichkeiten für Systembetreibende

5.1 Biometrie

- Biometrische Verfahren wie die Erkennung von Fingerabdrücken, Gesichtern oder der Iris dürfen ebenfalls zur Authentisierung genutzt werden.
- Die eingesetzten biometrischen Systeme müssen dem Stand der Technik entsprechen und datenschutzrechtliche Anforderungen erfüllen.
- [1]Biometrische Merkmale gelten als besonders schützenswerte personenbezogene Daten. [2]Im Rahmen ihrer verpflichtenden Erhebung und Nutzung muss die Servicestelle Datenschutz vorab miteinbezogen werden.
- Bei Systemen mit biometrischer Authentisierung muss eine alternative Authentifizierungsmethode bereitgestellt werden (z. B. Passwort + Token), um Ausweichmöglichkeiten zu gewährleisten.

5.2 PIN

- [1]Ein PIN darf nur als ein Faktor zur MFA genutzt werden. [2]Ausgenommen hiervon sind dienstliche Smartphones.
- Durch PIN geschützte Geräte müssen einen Sperrmechanismus nutzen, der eine Sperre nach einer festgelegten Anzahl von Falscheingaben vorsieht (weitere Informationen, siehe bitte Anhang).
- PINs, die als mehrstufiges Authentisierungsmittel dienen, sollen in Verbindung mit einem Sperrmechanismus genutzt werden, der eine Sperre nach einer festgelegten Anzahl von Falscheingaben vorsieht (weitere Informationen, siehe bitte Anhang).
- PINs müssen aus nicht leicht erratbaren oder persönlichen Informationen bestehen (z. B. 1234, Geburtsdaten, einfache Muster).
- PINs dürfen nicht identisch mit vorherigen PINs oder anderen Authentifizierungsmerkmalen (z. B. Teilen von Passwörtern) sein.

6 Rechte und Pflichten für Systembetreibende und Vorgesetzte

- Systeme müssen die in dieser Richtlinie beschriebenen Anforderungen für Anwendende technisch erzwingen.
- Passwörter müssen mit dem Stand der Technik vor unbefugtem Zugriff geschützt werden.

- [1]Standardpasswörter (z.B. herstellerseitig) müssen unmittelbar nach der Installation geändert werden. [2]**Beispiel:** Router, Webanwendungen oder Datenbanksysteme, die mit voreingestellten Zugangsdaten wie „admin/admin“ oder „root/root“ ausgeliefert werden, dürfen nicht mit diesen Standardpasswörtern betrieben werden.
- [1]Administrationspasswörter dürfen nicht auf Papier notiert werden. [2]Ausgenommen sind Passwörter, welche für den Notfall in einem physischen Tresor hinterlegt werden. [3]Hier muss jedoch ein geregelter Prozess etabliert und dokumentiert werden, der mindestens folgende Aspekte abdeckt:
  - Klare Regelung, wer Zugriff auf den Tresor hat (Zugangsberechtigung)
  - Benennung und Regelung einer Vertretung
  - Sicherstellung des physischen Schutzes des Tresors
  - Ein Notfallkonzept für den Zutritt, falls reguläre Zugriffsmöglichkeiten nicht verfügbar sind
  - Regelmäßige Überprüfung sowie Protokollierung aller Zugriffe auf den Tresor
- Ein anlassloser, erzwungener Passwortwechsel soll vermieden werden.
- Wo möglich soll mindestens ein weiterer Faktor (MFA) zur Authentifizierung angeboten und dessen Nutzung erzwungen werden.
- Vorgesetzte müssen die Ausgabe und Rückgabe eines zweiten Faktors (z.B. Yubikey) dokumentieren.
- Weitere Faktoren, die zur Authentifizierung dienen (z.B. Chipkarten), sollen auf dem Stand der Technik sein.
- Wo möglich soll eine passwortlose Authentifizierung (z.B. PassKeys) angeboten und dessen Nutzung vorgeschlagen werden.
- [1]Anmelde-Fehlversuche müssen dokumentiert werden. [2]Die Logs sollen regelmäßig auf Auffälligkeiten untersucht werden.
- Nach einer definierten Anzahl aufeinanderfolgender Fehlversuche bei der Anmeldung muss das Benutzerkonto automatisch gesperrt werden, um unbefugte Zugriffsversuche zu verhindern.

6.1 Verfahren für Passwortrücksetzung

- Für das Zurücksetzen von Passwörtern muss ein angemessen sicheres Verfahren definiert und umgesetzt werden.

- Die Mitarbeitenden des IT-Betriebs, die Passwörter zurücksetzen können, müssen vorher entsprechend geschult werden.

7 Ausnahmeregelung

[1]Die einzelnen Anforderungen (z. B. an die Passwörter in Nr. 4.1) gelten nur, soweit sie jeweils technisch möglich und praktikabel umsetzbar sind. [2]Sofern dies nicht der Fall ist, müssen in Abstimmung mit der Stabsstelle Informationssicherheit angemessene alternative Schutzmaßnahmen definiert, dokumentiert und umgesetzt werden. [3]Diese Maßnahmen müssen dem erforderlichen Schutzniveau des jeweiligen Systems entsprechen und regelmäßig überprüft werden. [4]Hinweise hierzu werden auf der Intranetseite der Stabsstelle Informationssicherheit veröffentlicht.

8 Inkrafttreten

[1]Diese Richtlinie tritt am Tage nach ihrer Bekanntmachung in Kraft. [2]Für Beschäftigte gilt die Passwortrichtlinie ab dem 17.10.2025 und ist von ihnen unverzüglich und somit so schnell, wie subjektiv zumutbar, einzuhalten. [3]Für Systeme gilt die Passwortrichtlinie ab dem 01.01.2027, um technische Anpassungen und Migrationsprozesse angemessen planen und umsetzen zu können. [4]Ab dem Zeitpunkt sollen auch Dritte, soweit sie als Auftragnehmer für die Universität Leistungen erbringen, bei neu erfolgenden Ausschreibungen und Auftragserteilungen auf die Vorgaben dieser Passwortrichtlinie im notwendigen und sinnvollen Umfang entsprechend verpflichtet werden.

9 Anhang

9.1 Empfehlung: Max. Fehlversuche für PINs je nach Länge

4-stellige PIN:

- Max. 3 Fehlversuche.
- Sehr geringe Entropie (nur 10.000 Kombinationen).
- Hohes Risiko für Brute-Force-Angriffe.

5-stellige PIN:

- Max. 5 Fehlversuche.
- Etwas sicherer, aber weiterhin begrenzter Schutz.

6-stellige PIN:

- Max. 5–7 Fehlversuche.

- 1 Mio. Kombinationen.
- Wir empfehlen diese Einstellung für Smartphones.

7–8-stellige PIN:

- Max. 7–10 Fehlversuche.
- Gute Balance aus Sicherheit und Nutzerfreundlichkeit.

Mehr als 8 Stellen:

- Max. 10 Fehlversuche oder risikobasierte Bewertung.
- Entropie ausreichend hoch, ggf. Schutzbedarf entscheidend.

9.2 Beispiele für Tastaturmuster

- 123456
- qwertz *(deutsches Tastaturlayout)*
- asdfgh
- zxcvbn (englisches Tastaturlayout)
- yxcvbn (deutsches Tastaturlayout)
- 1q2w3e *(diagonal verlaufend)*
- qazwsx *(senkrecht verlaufend auf der Tastatur)*
- !“§$%& *(oberste Zahlenreihe mit Shift)*

9.3 Möglichkeiten zum Testen gegen Tastaturmuster

Nutzung entsprechender Libraries wie z.B.: https://github.com/bjeavons/zxcvbn-php