JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN

Die Präsidentin

Mitteilungen der Justus-Liebig-Universität Gießen

Ausgabe vom **08.04.2026**

2.26.30 Nr. 3a

Richtlinie für den sicheren Umgang mit Passwörtern

Richtlinie für den sicheren Umgang mit Passwörtern

Vom 24.02.2026

Diese Richtlinie für sichere Passwörter tritt nach ihrer Verabschiedung im Präsidium der JLU Gießen am Tage nach ihrer Bekanntmachung in Kraft.

Bisherige Fassungen:

	Präsidium	Verkündung
Urfassung	24.02.2026#	08.04.2026

Inhaltsverzeichnis

§1 Gegenstand und Geltungsbereich

Passwörter sind nach wie vor das dominierende Mittel zur Authentifizierung im digitalen Raum. Einerseits sind sie unverzichtbar für den Zugriff auf viele IT-Geräte und IT-Dienste, da sie oft der einzige Schutz vor unbefugtem Zugriff sind. Andererseits macht genau dies Passwörter zu einem attraktiven Ziel für Cyberkriminelle. Daher ist es umso wichtiger, dass alle Mitglieder, Angehörige und Gäste der Justus-Liebig-Universität (JLU) Gießen den sicheren Umgang mit Passwörtern beherrschen, um die Sicherheit unserer Systeme und Daten zu gewährleisten.

Diese Richtlinie legt einen Rahmen für den sicheren Umgang mit Passwörtern fest. Sie richtet sich an alle Mitglieder, Angehörige und Gäste der JLU Gießen und gilt für Passwörter aller Privilegienstufen (z.B. Endnutzende oder Administrierende) auf dienstlichen Endgeräten, Serversystemen, Netzwerkkomponenten und anderen IT-Systemen der JLU Gießen sowie von der JLU Gießen bereitgestellten Anwendungen und IT-Diensten. Da Passwörter allgegenwärtig sind, ist diese Richtlinie auch anwendbar und empfehlenswert für private Endgeräte und externe Dienste.

§2 Passwortstärke

Passwörter gelten als sicher (oder auch „stark“), wenn sie die aktuellen wissenschaftlichen und technischen Standards erfüllen. Diese Standards stellen sicher, dass **starke Passwörter** auch bei erheblichem Einsatz von Rechenkapazität nicht leicht erraten und in der Folge missbräuchlich verwendet werden können. Passwörter an der JLU Gießen müssen die folgenden Anforderungen erfüllen, um als starke Passwörter zu gelten, und diese sind von allen Mitgliedern und Angehörigen der JLU Gießen verpflichtend zu befolgen:

- Das Passwort besteht aus **mindestens 12 Zeichen**.
- Das Passwort beinhaltet **mindestens 4 Zeichenarten** (Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen).
- Das Passwort enthält **keine leicht zu ermittelnde Bestandteile**:
    - Persönliche Informationen (z.B. Namen, Geburtsdaten) von sich selbst, Familienmitgliedern, Haustieren usw.
    - E-Mail-Adresse
    - Kontoname
    - Jahreszahl (4 Zahlen in Folge)
    - Einzelne Worte (z.B. Sommer, Herbst, ...)
- Das Passwort enthält **keine Umlaute oder Leerzeichen**, um Inkompatibilitätsprobleme zu vermeiden.

Diese Anforderungen werden regelmäßig mit dem aktuellen Stand der Technik in einschlägigen Standards z.B. des Bundesamts für Sicherheit in der Informationstechnik (BSI) abgeglichen und ggf. aktualisiert.

§3 Umgang mit Passwörtern

Neben der Wahl starker Passwörter, sind die nachfolgenden **Verhaltensregeln** für einen sicheren Umgang mit Passwörtern entscheidend und daher verpflichtend für alle Mitglieder und Angehörigen der JLU Gießen:

- Passwörter sind **geheim** zu halten und nicht zu teilen.
- Die Eingabe von Passwörtern muss **unbeobachtet** erfolgen.
- Öffentlich gewordene Passwörter müssen **sofort geändert** werden.
- Default- bzw. Initial-Passwörter sind nach dem ersten Anmelden **sofort zu ändern**.
- Passwörter müssen **sicher aufbewahrt** werden.
- Jeder Dienst (z.B. E-Mail, SAP) und jedes Endgerät (z.B. PC, Laptop) muss ein **individuelles** Passwort haben.
- Wenn sich bei Funktionsaccounts die Gruppenzusammensetzung ändert (z.B. Person verlässt die Gruppe oder die Universität), muss das Passwort geändert werden.

Da für jeden Account ein eigenes starkes Passwort verwendet werden muss, ist es mit zunehmender Anzahl an Passwörtern schwierig, sich all diese Passwörter zu merken. Daher ist es ratsam ein starkes Passwort zu haben, dass man sich merkt, und die anderen starken Passwörter werden in einem **Passwortmanager** verwaltet. Passwortmanager gibt es als dedizierte Anwendungen oder als Online-Dienst. Beachten Sie bei der Auswahl eines Passwortmanagers auf die Empfehlungen einschlägiger Quellen wie z.B. dem HRZ oder dem BSI.

§4 Betrieb von Authentifizierungsdiensten

Betreibende von IT-Diensten an der JLU Gießen mit passwortbasierter Authentifizierung sind verpflichtet, die von den Nutzenden vergebenen Passwörter auf ihre Konformität mit den in dieser Richtlinie spezifizierten Komplexitätsanforderungen für starke Passwörter technisch zu überprüfen und bei Nichteinhaltung zu unterbinden.

§5 Ausnahmen

Sollte eine Ausnahme von den genannten Anforderungen erforderlich sein, weil z.B. ältere IT-Systeme diese Anforderungen technisch nicht verarbeiten können, muss diese mit dem/der Informationssicherheitsbeauftragten (ISB) abgestimmt werden.

§6 Zukünftige Authentifizierungsverfahren

Selbst ein starkes Passwort mit dem sicher Umgegangen wird, kann zu Gefährdungen führen, wenn es durch Datenlecks oder Social Engineering Angriffen wie z.B. Phishing in die falschen Hände gerät. Um die Sicherheit der Authentifizierung an der JLU Gießen weiter zu erhöhen, wird neben der sicheren Verwendung starker Passwörter zukünftig vermehrt die Nutzung alternativer Authentifizierungsverfahren eingeführt. Hierzu zählt insbesondere die Zwei-Faktor-Authentifizierung (2FA), die ein starkes Passwort mit einem zusätzlichen Authentifizierungsschritt auf z.B. Basis biometrischer Verfahren wie Fingerabdruck- und Gesichtserkennung oder Sicherheitsschlüsseln und Einmalcodes kombiniert. Zentrale Anwendungen der JLU Gießen werden zukünftig entsprechende Anmeldeverfahren unterstützen, um einen höheren Schutz gegenüber unbefugten Zugriff auf Universitäts-Ressourcen zu verhindern.

§7 Inkrafttreten

Diese Richtlinie für sichere Passwörter tritt nach ihrer Verabschiedung im Präsidium der JLU Gießen am Tage nach ihrer Bekanntmachung in Kraft.

Die Aufrechterhaltung der Informationssicherheit ist eine permanente Aufgabe und ein explizites Sicherheitsziel. Diese Richtlinie ist daher regelmäßig, mindestens alle zwei Jahre, auf ihre Aktualität hinsichtlich der aktuellen Anforderungen an die Informationssicherheit zu prüfen.

Gießen, den 24.02.2026
Prof. Dr. Katharina Lorenz
Präsidentin der Justus-Liebig-Universität Gießen