



# Inhaltsverzeichnis

<b>Passwortrichtlinie der Hochschule Merseburg .....</b>	<b>1</b>
<b>Inhaltsverzeichnis .....</b>	<b>1</b>
<b>1. Geltungsbereich .....</b>	<b>2</b>
<b>2. Anforderungen an Passwörter.....</b>	<b>2</b>
a.    Allgemeine Anforderungen .....	2
b.    Zusätzliche Anforderungen an Passwörter für administrative Accounts ..	2
c.    unerlaubte Zeichen .....	3
<b>3. Pflichten der Nutzer beim Umgang mit Passwörtern.....</b>	<b>3</b>
a.    Initialpasswort.....	3
b.    Nutzung von Passwörtern.....	3
c.    Aufbewahrung von Passwörtern.....	4
d.    Nutzen der Zwei-Faktor-Authentifizierung (2FA) .....	4
<b>4. Technische Maßnahmen.....</b>	<b>4</b>
a.    Speicherung und Zugriffsschutz.....	4
b.    Angriffsschutz durch technische Maßnahmen .....	4
<b>5. Organisatorische Maßnahmen .....</b>	<b>5</b>
<b>6. Verfahren für automatisierte Passwortrücksetzung .....</b>	<b>5</b>
<b>7. Inkrafttreten .....</b>	<b>5</b>

In einer akademischen Institution wie der Hochschule Merseburg ist der Schutz von sensiblen Daten von höchster Bedeutung. Dazu gehören vertrauliche Informationen über Studierende, Forschungsergebnisse, Verwaltungsdaten und andere sensible Informationen. Diese Passwortrichtlinie wurde entwickelt, um sicherzustellen, dass alle Mitglieder und Angehörigen der Hochschule Merseburg – einschließlich Studierender, Lehrender und Mitarbeitender – sichere Passwörter verwenden. Die Einhaltung dieser Richtlinie trägt dazu bei, unbefugten Zugriff zu verhindern, den Schutz der digitalen Ressourcen der Hochschule zu gewährleisten und die Integrität unserer akademischen und administrativen Systeme abzusichern.

## **1. Geltungsbereich**

- (1) Diese Passwortrichtlinie findet Anwendung auf alle Mitglieder und Angehörigen der Hochschule Merseburg gem. § 58 Abs. 1 – 3 HSG-LSA sowie alle sonstigen Nutzerinnen und Nutzer von IT-Diensten. Für administrative Zugänge können zusätzlich gesonderte Richtlinien gelten.
- (2) Die Passwortrichtlinie ist auf alle IT-Dienste anzuwenden, deren Ressourcen und Daten durch Passwörter vor unberechtigtem Zugriff und missbräuchlicher Verwendung oder Veränderung geschützt werden sollen.
- (3) Alle technischen Systeme wie Netzwerkschweiche, USV etc., die in einem gekapselten, vom Internet isolierten VLAN betrieben werden, sind von dieser Regelung ausgenommen. Diese sind durch organisationsbezogene Richtlinien abzusichern.

## **2. Anforderungen an Passwörter**

### **a. Allgemeine Anforderungen**

Die nachstehenden Anforderungen sind IT-seitig gesetzt und können von Ihnen nicht geändert werden. Danach gilt folgendes:

- Das Passwort muss mindestens 12 Zeichen lang sein! (Je länger, desto besser).
- Das Passwort muss mindestens einen Großbuchstaben enthalten.
- Das Passwort muss mindestens einen Kleinbuchstaben enthalten.
- Das Passwort muss mindestens eine Zahl enthalten.
- Das Passwort muss mindestens ein Sonderzeichen enthalten.
- Das Passwort darf ausschließlich die folgenden Zeichen enthalten: A-Z a-z 0-9 + - \* / = # \$ % & @ \_.
- Bereits vergebene Passwörter sind unzulässig und können nicht vergeben werden.

### **b. Zusätzliche Anforderungen an Passwörter für administrative Accounts**

- Das Passwort soll im Rahmen der technischen Anforderungen mindestens 20 Zeichen lang sein.

- Das Passwort sollte vorzugsweise mit einem Passwortgenerator generiert werden.

### **c. unerlaubte Zeichen**

Leicht zu erratende Passwörter dürfen nicht verwendet werden. Zu vermeiden sind insbesondere:

- Zeichenwiederholungen,
- Zahlen und Daten aus dem Lebensbereich des Nutzers/der Nutzerin,
- Zeichenkombinationen, die nur unwesentlich von den vorherigen Passwörtern abweichen,
- einfache Ziffern- und Buchstabenkombinationen,
- Zeichen, die durch nebeneinanderliegende Tasten eingegeben werden oder
- Zeichenkombinationen, die Suchbegriffe in Wörterbüchern und Lexika entsprechen (Trivialpasswörter).

## **3. Pflichten der Nutzer beim Umgang mit Passwörtern**

### **a. Initialpasswort**

- Durch das ITZ oder systemseitig gesetzte Passwörter müssen beim Erstzugriff geändert werden.
- Passwörter sollten möglichst zufällig erzeugt werden. Die Verwendung eines Passwortgenerators in Verbindung mit einem Passwortmanager wird empfohlen (z. B. Keepass oder Passwortmanager im Browser ihres Betriebssystems).
- Alternativ können Passphrasen verwendet werden, um gut merkbare Passwörter zu erhalten. Nähere, jeweils aktuelle Informationen erhalten Sie auf den Webseiten des Bundesamtes für Informationssicherheit ([www.bsi.de](http://www.bsi.de)).

### **b. Nutzung von Passwörtern**

- Lassen Sie sich bei der Eingabe von Passwörtern nicht beobachten!
- Die Zeichen des Passwortes dürfen nicht im Klartext erscheinen.
- Geben sie persönliche Passwörter nicht an Dritte weiter!
- Sie müssen Ihr Passwort umgehend wechseln, wenn es unautorisierten Personen bekannt geworden ist (z. B. durch Ausspähen) oder der Verdacht dazu besteht. Die weitere Verwendung des bisher benutzten Passwortes ist nicht zulässig!
- System-Administratorenpasswörter dürfen nur den Personen bekannt sein, die sie zur Erledigung der ihnen übertragenen Aufgaben benötigen (need-to-know-Prinzip). Nach Änderung von Arbeitsaufgaben oder Verlassen der Hochschule ist der Nutzer oder die Nutzerin zu deaktivieren/zu löschen und falls der Account weiter besteht (je nach technischem Erfordernis), sind die betroffenen Passwörter der Accounts, auf welche die Person Zugriff hatte, umgehend zu ändern (z. B. bei gemeinsam genutzten Administratoren-/root-Accounts). Falls möglich ist pro Administrator ein entsprechender Account einzurichten. Maßgeblich soll die Mehrfachnutzung von Accounts durch verschiedene Nutzer unterbleiben. Eine Ausnahme bilden technische

Erfordernisse, falls z. B. eine derartige Einrichtung nicht möglich ist.

- Das Hochschule Merseburg empfiehlt, Passwörter sporadisch in unregelmäßigen Abständen für verschiedene Accounts zu ändern, um unwissentlich kompromittierte Passwörter zu wechseln.

### **c. Aufbewahrung von Passwörtern**

- Eine unverschlüsselte Speicherung von Passwörtern auf IT-Systemen ist unzulässig.
- Eine jeweils als aktuell sicher geltende verschlüsselte Speicherung, z. B. in einem Passwortmanager, (z.B. KeePass) ist zulässig.
- Das analoge Notieren von Passwörtern ist anzuraten, wenn die Sicherheitsmerkmale (Passwort/Nutzername) möglichst getrennt und verschlossen, geschützt vor unberechtigtem Zugriff aufbewahrt werden.
- Passwörter dürfen in IT-Systemen nicht im Klartext gespeichert werden. Eine Ausnahme bilden spezielle IT-Systeme/-Dienste, bei denen das Erfordernis besteht, Klartextpasswörter z. B. in Konfigurationsdateien, zu hinterlegen. Hier sind besondere Sicherheitsmaßnahmen einzuhalten (z. B. mindestens eingeschränkter Zugriff).
- Die Notfallhinterlegung von Passwörtern und übergeordneten Accounts in einem Tresor ist gewünscht und zulässig.

### **d. Nutzen der Zwei-Faktor-Authentifizierung (2FA)**

Zur Absicherung des Zugriffs auf die IT-Infrastrukturen (z.B. Nutzung VPN, Homeportal) der Hochschule Merseburg ist die Aktivierung und Nutzung der Zwei-Faktor-Authentifizierung erforderlich.

## **4. Technische Maßnahmen**

### **a. Speicherung und Zugriffsschutz**

- Der Zugriff auf die Nutzerdatenbanken der IT-Hochschulinfrastruktur ist mit geeigneten, zulässigen Methoden gemäß dem aktuellen Stand der Technik gegen unerlaubten Zugriff geschützt.
- Passwörter dürfen über unsichere Netze nur angemessen verschlüsselt und dem aktuellen Stand der IT-Sicherheit entsprechend übertragen werden.

### **b. Angriffsschutz durch technische Maßnahmen**

Durch technische Maßnahmen soll vorgegeben werden, dass

- nur Passwörter vergeben werden können, die den allgemeinen Sicherheitsanforderungen entsprechen,
- Passwörter nach dem Stand der Technik nicht im Klartext gespeichert werden,
- Passwörter in Netzwerken verschlüsselt übertragen werden oder
- Trivialpasswörter nicht vergeben werden können.
  
- Fehlversuche bei der Passworteingabe werden, sofern möglich, protokolliert. Die Protokolle sollen regelmäßig ausgewertet werden, um Angriffe und Missbrauch aufzudecken.

- Bei Verdacht auf einen Sicherheitsvorfall kann der Account durch das ITZ gesperrt werden. Der Fachbereich oder die Organisationseinheit, dem der gesperrte Nutzer/die gesperrte Nutzerin zugeordnet ist, informiert die Person auf geeignete Weise (z. B. per Post oder telefonisch).
- Nach mehrmaliger fehlerhafter Passworteingabe kann die Benutzerkennung manuell oder automatisiert gesperrt werden.

## **5. Organisatorische Maßnahmen**

- Die Gültigkeitsdauer von Passwörtern kann entsprechend den jeweils aktuellen Sicherheitsstand/ Empfehlungen des BSI angepasst werden.
- Alle Nutzer und Nutzerinnen der IT-Dienste der Hochschule Merseburg sind über den Inhalt dieser Richtlinie zu informieren.

## **6. Verfahren für automatisierte Passwortrücksetzung**

Soweit technisch und organisatorisch möglich, kann die Passwortrücksetzung durch ein automatisiertes Verfahren erfolgen.

## **7. Inkrafttreten**

Diese Richtlinie tritt mit der Veröffentlichung in den Amtlichen Bekanntmachungen der Hochschule Merseburg in Kraft.

Merseburg, den 09. Dezember 2024



Prof. Dr. Markus Krabbes  
Der Rektor