Universität Regensburg

Passwortrichtlinie

Dateiname	Version	Änderungsdatum	Autor/in
Passwortrichtlinie	1.0	04.12.2024	Elena Kellinghaus
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
Öffentlich	Hauptversion	05.12.2024	Dr. Christoph Bauer

Inhalt

1. Einleitung

Die Passwortrichtlinie dient dem Schutz sensibler Daten und Systeme an der Universität Regensburg vor unbefugtem Zugriff. Da Passwörter die erste Verteidigungslinie gegen Sicherheitsverletzungen darstellen, ist es unerlässlich, starke und sichere Passwörter zu verwenden. Die Richtlinie hat zum Ziel, klare Vorgaben zu formulieren, wie komplexe Passwörter erstellt werden sollen, verwendet und regelmäßig aktualisiert werden sollen, um die Integrität und Vertraulichkeit der Universitätsressourcen zu gewährleisten.

2. Geltungsbereich

Der Anwendungsbereich dieser Richtlinie umfasst alle Nutzerinnen und Nutzer, die auf IT-Systeme der Universität Regensburg zugreifen, einschließlich Mitarbeitende, externer Dienstleister und anderer autorisierter Personen.

3. Regelungen

3.1. Grundsätze

- Das Passwort für den RZ-Account muss ausschließlich dafür und keinesfalls für andere Konten genutzt werden.
- Nutzende sind verpflichtet, alle notwendigen Maßnahmen zu ergreifen, um sicherzustellen, dass Passwörter nicht an Dritte weitergegeben werden oder diesen zugänglich sind.
- Bei Verdacht auf Offenlegung des Passwortes sind die Nutzenden verpflichtet, umgehend den Vorfall an den zuständigen Servicedesk des Rechenzentrums zu melden.

3.2. Passwortanforderungen

Mindestens folgende Einstellungen für die Verwendung von Passwörtern bei Benutzerkonten sollten in einer Gruppenrichtlinie gesetzt werden:

Länge:

- Minimal: 12 Zeichen

Komplexität:

- Mindestens eine Ziffer
- Mindestens ein kodierungssicheres Sonderzeichen (-$#[]{}!().,*:;_)
- Sequenzen mit 4 und mehr aufeinanderfolgenden gleichen Zeichen sind nicht erlaubt.

Verbotene Inhalte:

- Das Passwort darf keine Umlaute, keine Leerstellen und nur kodierungssichere Sonderzeichen (-$#[]{}!().,*:;_) enthalten.

3.3. Passwortänderungen

Das maximales Kennwortalter darf 365 Tage nicht überschreiten.

Das UR-System merkt sich die 10 zuletzt verwendeten Passwörter als Hashes, die mindestens volle 24 Stunden gültig waren (Kennwortchronik).

3.4. Passwortverwaltung

Im Serviceportal des Rechenzentrums besteht die Möglichkeit, den RZ-Account zu verwalten und das Passwort zu ändern. Um bei einem vergessenen oder verloren gegangenen Passwort den Zugang eigenständig wiederherstellen zu können, wird empfohlen, im Serviceportal eine private E-Mail-Adresse oder Mobilfunknummer zu hinterlegen.

Passwörter sind sicher und vor unbefugtem Zugriff Dritter zu speichern. Zur Verwaltung mehrerer Passwörter wird die Nutzung eines Passwort-Managers empfohlen, um Passwörter nicht zu vergessen und nicht aufschreiben zu müssen. Das Rechenzentrum empfiehlt und bietet hierfür einen Passwort-Manager im Software-Katalog sowie entsprechender E-Schulung an.

3.5. Betriebssystemzugänge und Anmeldungen

Für die Anmeldung an Betriebssystemen auf Clients sind sichere Passwörter zu nutzen. Die Clients sollten, wo möglich, in einen administrativen Bereich und einen Bereich mit eingeschränkten Zugriffsrechten eingerichtet werden. Hierfür müssen unterschiedliche Passwörter verwendet werden.

Für die Anmeldung an Betriebssystemen auf Smartphones sowie Tablets sind sichere Verfahren wie Passwort, Pin-Eingabe, Fingerabdruck oder Gesichtserkennung zu aktivieren.

3.6. Zugangsschutz

Zum Schutz von Benutzerkonten sind zusätzliche Sicherheitsmaßnahmen wie das temporäre Sperren von Konten nach einer festgelegten Anzahl fehlerhafter Anmeldeversuche (Sperrung nach 20 Fehlversuchen) zu aktivieren. Der Kontosperrungszähler wird nach 30 Minuten zurückgesetzt.

Darüber hinaus muss nach 10 Minuten Inaktivität der Zugang zum Endgerät gesperrt werden.

3.7. Verantwortlichkeiten

Nutzerinnen und Nutzer sind verpflichtet, die Vorgaben dieser Richtlinie einzuhalten, um die Sicherheit ihrer Konten und Daten zu gewährleiten.

Administrierende sind für die Implementierung und Durchsetzung der Richtlinie verantwortlich.

3.8. Schulung und Sensibilisierung

Die Universität Regensburg bietet GRIPS-Kurse zum Thema IT-Sicherheit, Datenschutz und Telearbeit an. Die Kurse decken unter anderem die Themen Passwortsicherheit und -management ab. Die Kurse werden in regelmäßigen Abständen evaluiert und aktualisiert.

Für das wissenschaftsstützende Personal der Universität gilt einmal jährlich eine Fortbildungspflicht im Bereich der IT-Sicherheit und Datenschutz. Das wissenschaftliche Personal ist dazu angehalten, mindestens einmal jährlich sich zu den oben genannten Themen zu informieren.

3.9. Ausnahmen

Weitreichendere Regelungen für die RZ-Administratorinnen und Administratoren sind in der „Richtlinie zur Administration im RZ“ festgelegt.

4. Schlussbestimmungen

4.1. Bekanntmachung

Diese Richtlinie ist IT-Nutzenden der UR in geeigneter Weise zugänglich zu machen, veröffentlicht auf den Webseiten des RZ.

4.2. Gültigkeit und Dokumenten-Handhabung

Das Rechenzentrum behält sich das Recht vor, diese Richtlinie bei Bedarf zu ändern. Änderungen können insbesondere erforderlich werden, um gesetzlichen Vorgaben, bindenden Verordnungen, Forderungen der zuständigen Aufsichtsbehörde oder internen Verfahren an der Universität Regensburg zu entsprechen.

Der/die Verantwortliche für dieses Dokument ist der/die IT-Sicherheitsbeauftragte(n), welche/r die Richtlinie in regelmäßigen Abständen auf inhaltliche Richtigkeit und Konsistenz mit anderen Richtlinien, Handlungsanweisungen usw. prüft und aktualisiert. Nach Freigabe muss die nächste Überprüfung in zwei Jahren erfolgen.

4.3. Inkrafttreten

Diese Richtlinie tritt am Tage nach ihrer Bekanntmachung in Kraft.

Regensburg, den 05.12.2024

Dr. Christoph Bauer

Leiter des Rechenzentrums