Technische Universität Berlin

TU Berlin Passwortrichtlinie

Inhaltsverzeichnis

1. Kurzbeschreibung

Der Zugang zu allen IT-Diensten wird durch Authentifizierungsverfahren abgesichert. Im Regelfall werden dazu passwortbasierte Verfahren eingesetzt. Die vorliegende Sicherheitsrichtlinie regelt den Einsatz, die Verwendung und den Aufbau von Passwörtern für den Einsatz an IT-Systemen der TU Berlin, sowie die Rechte und Pflichten aller Nutzer der IT-Systeme bei der Verwendung von passwortbasierten Authentifizierungsverfahren.

2. Geltungsbereich

Diese Richtlinie gilt für alle Benutzer der TU Berlin, deren Nutzerkonten über das zentrale Provisioning durch tubIT erzeugt und verwaltet wurden. Grundsätzlich stellt diese Regelung nur den Mindestschutz dar und kann von jedem Betreiber von IT-Systemen im Bedarfsfall durch strengere Regelungen ergänzt werden.

Für die administrativen Passwörter der Serverumgebungen von tubIT gilt eine separate, strengere Vorschrift.

3. Komplexität von Passwörtern

Die verwendeten Passwörter müssen folgende Kriterien erfüllen:

- Das Passwort enthält 8 – 20 Zeichen
- Das Passwort besteht aus Zeichen der vier Zeichengruppen:
  - Großbuchstaben, A-Z,
  - Kleinbuchstaben a-z,
  - Ziffern 0-9 und
  - Sonderzeichen !“#$%&\’()*+,-./:;<=>?
- Mindestens drei der vier Zeichengruppen (Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen) müssen im Passwort vertreten sein.
- Gruppen von mehr als zwei Zeichen, die auch in Vornamen, Nachnamen oder Benutzernamen vorkommen, sind unzulässig.
- Es dürfen nicht mehr als zwei gleiche Zeichen in Folge auftreten.
- Jedes Zeichen darf insgesamt nicht mehr als dreimal im Passwort vorkommen.
- Aus jeder Zeichengruppe dürfen höchstens vier Zeichen in Folge vorkommen.
- Das Passwort muss mindestens fünf verschiedene Zeichen enthalten.
- Keine Gruppe von drei oder mehr Zeichen darf sich im Passwort wiederholen.
- Gruppen von mehr als drei Zeichen, die der Anordnung des Alphabets oder der Tastatur entsprechen, sind zu vermeiden. Höchstens eine solche Gruppe ist zulässig.

4. Ablauf von Passwörtern

Passwörter müssen nach einer dem Schutzbedarf angemessenen Frist gewechselt werden. Der Benutzer ist für das Wechseln des Passwortes selbst verantwortlich. Es wird empfohlen das Passwort halbjährlich zu wechseln.

5. Regeln bei der Verwendung von Passwörtern

- Passwörter sind geheim zu halten. Sie dürfen nicht an andere Personen weitergegeben oder diesen zugänglich gemacht werden.
- Mitarbeiter von tubIT werden nie telefonisch, per E-Mail oder persönlich nach Passwörtern fragen.
- Passwörter sind von fremden unbeobachtet einzugeben.
- Passwörter dürfen nicht unverschlüsselt auf Rechnern gespeichert werden.
- Initiale Passwörter oder Passwörter die Nutzer nach der Rücksetzung durch den Helpdesk erhalten sind unmittelbar durch den Nutzer zu ändern.

6. Inkrafttreten

Diese Leitlinie wurde von der CIO der TU Berlin verabschiedet und tritt mit Beschluss in Kraft.

Technische Universität Berlin

TU Berlin Passwortrichtlinie

Inhaltsverzeichnis

1. Kurzbeschreibung

Der Zugang zu allen IT-Diensten wird durch Authentifizierungsverfahren abgesichert. Im Regelfall werden dazu passwortbasierte Verfahren eingesetzt. Die vorliegende Sicherheitsrichtlinie regelt den Einsatz, die Verwendung und den Aufbau von Passwörtern für den Einsatz an IT-Systemen der TU Berlin, sowie die Rechte und Pflichten aller Nutzer der IT-Systeme bei der Verwendung von passwortbasierten Authentifizierungsverfahren.

2. Geltungsbereich

Diese Richtlinie gilt für alle Benutzer der TU Berlin, deren Nutzerkonten über das zentrale Provisioning durch tubIT erzeugt und verwaltet wurden. Grundsätzlich stellt diese Regelung nur den Mindestschutz dar und kann von jedem Betreiber von IT-Systemen im Bedarfsfall durch strengere Regelungen ergänzt werden.

Für die administrativen Passwörter der Serverumgebungen von tubIT gilt eine separate, strengere Vorschrift.

3. Komplexität von Passwörtern

Die verwendeten Passwörter müssen folgende Kriterien erfüllen:

- Das Passwort enthält 8 – 20 Zeichen
- Das Passwort besteht aus Zeichen der vier Zeichengruppen:
  - Großbuchstaben, A-Z,
  - Kleinbuchstaben a-z,
  - Ziffern 0-9 und
  - Sonderzeichen !“#$%&\’()*+,-./:;<=>?
- Mindestens drei der vier Zeichengruppen (Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen) müssen im Passwort vertreten sein.
- Gruppen von mehr als zwei Zeichen, die auch in Vornamen, Nachnamen oder Benutzernamen vorkommen, sind unzulässig.
- Es dürfen nicht mehr als zwei gleiche Zeichen in Folge auftreten.
- Jedes Zeichen darf insgesamt nicht mehr als dreimal im Passwort vorkommen.
- Aus jeder Zeichengruppe dürfen höchstens vier Zeichen in Folge vorkommen.
- Das Passwort muss mindestens fünf verschiedene Zeichen enthalten.
- Keine Gruppe von drei oder mehr Zeichen darf sich im Passwort wiederholen.
- Gruppen von mehr als drei Zeichen, die der Anordnung des Alphabets oder der Tastatur entsprechen, sind zu vermeiden. Höchstens eine solche Gruppe ist zulässig.

4. Ablauf von Passwörtern

Passwörter müssen nach einer dem Schutzbedarf angemessenen Frist gewechselt werden. Der Benutzer ist für das Wechseln des Passwortes selbst verantwortlich. Es wird empfohlen das Passwort halbjährlich zu wechseln.

5. Regeln bei der Verwendung von Passwörtern

- Passwörter sind geheim zu halten. Sie dürfen nicht an andere Personen weitergegeben oder diesen zugänglich gemacht werden.
- Mitarbeiter von tubIT werden nie telefonisch, per E-Mail oder persönlich nach Passwörtern fragen.
- Passwörter sind von fremden unbeobachtet einzugeben.
- Passwörter dürfen nicht unverschlüsselt auf Rechnern gespeichert werden.
- Initiale Passwörter oder Passwörter die Nutzer nach der Rücksetzung durch den Helpdesk erhalten sind unmittelbar durch den Nutzer zu ändern.

6. Inkrafttreten

Diese Leitlinie wurde von der CIO der TU Berlin verabschiedet und tritt mit Beschluss in Kraft.