Richtlinie zum Umgang mit Passwörtern

Wahl des Passwortes

- Das Passwort muss mindestens 9, besser mehr Zeichen umfassen.
- Es sollte viele verschiedene Zeichen, sowie Ziffern, Sonderzeichen und Groß- und Kleinschreibung enthalten, jedoch keine Umlaute.
- Zeichenfolgen, die leicht zu merken sind, andere aber nicht erraten können, z.B. die Anfangsbuchstaben der Wörter eines Satzes.

Beispiele unsicherer Passwörter

- (Tier-, Monats-) Namen, Name des Rechners, Benutzername
- Wörter aus Wörterbüchern, alles gleiche Buchstaben
- Telefonnummern, Autonummern, PIN-Codes, Monatsnamen, Geburtstage oder andere typische persönlich Daten
- Alle oben genannten Zeichenfolgen in umgekehrter Reihenfolge oder mit einer vorangestellten bzw. nachfolgenden Zahl oder Zeichen

Regeln für den Umgang mit Passwörtern

- Jede Benutzer-Identifikation (Mitarbeiter, Dienste usw.) hat ein individuelles Passwort.
- Passwörter sollten periodisch geändert werden, bei Netzpasswörtern erfolgt alle 120 Tage eine automatische Erinnerung.
- Initialpasswörter sind bei der ersten Benutzung zu ändern.
- Neue Passwörter müssen sich vom alten Passwort, über mehrere Wechselzyklen hinweg, signifikant unterschieden.
- Die Passworteingabe darf durch Dritte nicht einsehbar sein.
- Nach 7 fehlerhaften Passworteingaben erfolgt bei Netzpasswörtern automatisch eine Sperrung von 15 Minuten.
- Passwörter nicht auf Funktionstasten, in Skripten oder in Programmen speichern.
- Passwörter dürfen nicht an Dritte weitergegeben werden (keine Bekanntgabe an Kollegen, in Internet-Formularen, in E-Mails etc.).
- Passwörter dürfen nicht aufgeschrieben und am Arbeitsplatz "versteckt" werden (Empfehlung: Hinterlegung in einem verschlossenen Umschlag in einem Safe).
- Diese Regeln gelten sowohl für alle Netzdienste sowie auch für alle lokalen Logins an Rechnern oder Geräten mit Benutzerzugang.
- Das durch den zuständigen IT-Verantwortlichen für den PC/Laptop eingerichtete lokale Administrator-Kennwort darf nicht eigenmächtig geändert werden.

Damit Passwörter nicht in falsche Hände geraten, erraten oder durch automatisierte Attacken leicht geknackt werden können, ist es erforderlich, diese Richtlinie einzuhalten. Somit kann ein unberechtigter Zugang zum Hochschulnetz bzw. zu internen oder auch personenbezogenen Daten vermieden werden. Bei der Nutzung von Netzdiensten ist darauf zu achten, dass Passwörter verschlüsselt übertragen werden (z.B. HTTPs statt HTTP, E-Mailempfang und -Versand über SSL-Verschlüsselung).