



^b
**UNIVERSITÄT
BERN**

Verwaltungsdirektion
Abteilung Informatikdienste

Richtlinien zum Umgang mit Passwörtern

Versionskontrolle und Prüfstellen			
Version	Bearbeitung	Ersteller	Datum
X0100	Neues Dokument erstellt	Rolf Kräuchi	27.01.2010
X0101	Ueberarbeitung CH, rz	Renato Zumstein	21.01.2011
V0100	Freigegebene Version	Renato Zumstein	01.02.2011

Geltungsbereich	Mitarbeitende und Studierende der Uni Bern
Klassifikation	Für uni-internen Gebrauch
Dokumentenstatus	Freigegeben
Freigabe	Leiter ID, 1.2.2011

1. Zweck

Ein kompromittiertes Passwort kann zu einer Gefährdung der gesamten IT-Infrastruktur der Uni Bern führen. Die Richtlinien zum Umgang mit Passwörtern haben zum Ziel, die IT-Ressourcen, insbesondere das Netzwerk, Systeme und die Datenintegrität zu schützen.

2. Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeiterinnen und Mitarbeiter sowie Studierende, die ein Passwort für die Nutzung von IT-Ressourcen an der Universität Bern besitzen. Insbesondere richtet sie sich an alle Inhaber eines Campus Account.

3. Kriterien für Passwörter (Campus Account)

- Länge: mindestens 8 Zeichen
- Komplexität: Drei der vier folgenden Zeichen müssen enthalten sein:
 1. Kleinbuchstaben
 2. Grossbuchstaben
 3. Zahlen
 4. Sonderzeichen
- Generell keine Namen oder Wörter aus einem Wörterbuch verwenden. Der Benutzername darf nie Teil des Passworts sein.
- Keine lokalisierten Sonderzeichen wie "äöüàèéè"
- Sperrung: nach 10 Fehlversuchen bei der Passworteingabe wird das Konto gesperrt für die Zeitdauer von 15 Minuten

4. Umgang mit Passwörtern

- Passwörter sind persönlich und dürfen nicht weitergegeben werden (gemäss "Weisungen über die Benutzung der IT-Ressourcen")
- Bei Verdacht, dass Unberechtigte ein Passwort kennen, ist dieses umgehend zu ändern
- Passwörter dürfen grundsätzlich nicht aufgeschrieben oder unverschlüsselt übermittelt oder gespeichert werden, weder auf Arbeitsstationen noch auf Servern, Notebooks, PDA's oder Smartphones
- Das Passwort für den Campus Account darf nicht identisch sein mit dem für andere, uni-externe Dienste wie z.B. EMail oder soziale Netzwerke
- Wenn andere Personen in der Nähe sind, ist entsprechende Vorsicht bei der

Eingabe des Passworts walten zu lassen

- Es wird empfohlen, das Passwort nach spätestens einem Jahr zu ändern

5. Wahl eines sicheren Passworts

- Keine Trivial-Passwörter wie Benutzername, Name, Vorname, Geburtsdatum, Telefonnummer etc.
- Kein Ersetzen von Buchstaben durch ähnlich aussehende Zahlen (Leetspeak, z.B. gr34t_p4ssw0rd)
- Keine Zeichenfolgen auf der Tastatur verwenden (z.B. qwertz)
- Eine Kombination von Buchstaben, Zahlen und Sonderzeichen ist sicherer, da die Kombinationsmöglichkeiten um ein Vielfaches zunehmen
- Zahlen und Sonderzeichen stehen mit Vorteil in der Mitte des Passworts
- Bewährt hat sich die Methode, ein Passwort aus einem Satz zu bilden. Aus "Ich brauche jetzt endlich! ein sicheres Passwort" kann folgendes Passwort gebildet werden: "lbje!1sP"
- Wenn Sie unsicher sind benutzen Sie einen Passwortgenerator

6. Allgemeine Bestimmungen

Die Einhaltung der Richtlinien zum Umgang mit Passwörtern kann von dem Sicherheitsbeauftragten der Informatikdienste überprüft werden.

Informatikdienste der Universität Bern
Bern, 1. Februar 2011

Leiter Informatikdienste