W101 Weisung: Benutzernamen und Passwörter (Passwort-Policy)

Version 1.3, 22. Februar 2017

Diese Regelung stützt sich auf § 13 Absatz 3 der Verordnung über die Informatiksicherheit und über die Nutzung von Informatikmitteln (Informatiksicherheitsverordnung, SRL Nr. 26b) vom 22. November 2016.

I. Einleitung

Zweck: Für die Mitarbeitenden des Kantons Luzern und die Lernenden an kantonalen Schulen sollen klare Regeln für den Umgang mit Benutzernamen und Passwörtern gelten und bekannt sein. Dazu gehören insbesondere Regeln für das Erstellen und das Anpassen von Benutzernamen und Passwörtern. So wird das Risiko des Eindringens eines Angreifers in die IT-Systeme des Kantons infolge nicht gesetzter, schwacher oder bekannter Passwörter reduziert.

Geltungsbereich:

- Geltungsbereich richtet sich nach § 2 der Informatiksicherheitsverordnung.
- Dazu gehören auch Vertragspartner mit Zugriff auf kantonale Informatikmittel und Informationen des Kantons Luzern.

Adressaten: Mitarbeitende und Lernende im Geltungsbereich

Quelle: Dieses Dokument basiert auf den Empfehlungen des BSI (Bundesamt für Sicherheit in der Informationstechnik der Bundesrepublik Deutschland). Diese Empfehlungen stellen dabei Minimalvorgaben dar.[1]

II. Benutzerkonto

- Ein Benutzerkonto besteht mindestens aus einem Benutzernamen und dem dazugehörigen Passwort (Kennwort).
- Es dürfen ausschliesslich persönliche Benutzerkonten (Accounts) verwendet werden.
- Die Benutzernamen müssen eindeutig und zuweisbar sein.
- IT- und Systemadministratoren verwenden für Konfigurationsarbeiten ein zusätzliches persönliches Benutzerkonto, welches mit mehr Rechten (höheren Privilegien) ausgestattet ist.
- Es dürfen generell keine Gruppen-Benutzerkonten verwendet werden.

Bieten Systeme keine Multiuser-Funktion oder wird aus organisatorischen oder funktionalen Gründen ein Gruppen-Benutzerkonto benötigt, kann vom zuständigen OIB zusammen mit dem Informationssicherheitsbeauftragten des Kantons Luzern eine Ausnahme definiert werden. Für solche Gruppen-Benutzerkonten gelten zusätzlich folgende Vorgaben:

- Für jedes Gruppen-Benutzerkonto ist ein zuständiger Mitarbeitender oder eine zuständige Mitarbeiterin zu bestimmen.
- Der oder die zuständige Mitarbeitende ist für die Einhaltung dieser Weisung verantwortlich.
- Bei Verstössen gegen geltende Vorgaben, welche über das Gruppen-Benutzerkonto begangen werden, ist der oder die zuständige Mitarbeitende verantwortlich.

Die Vorgaben gelten auch für technische Benutzerkonten (z.B. Service Accounts).

Anmelde-, Abmelde- sowie weitere Vorgänge können unter Einhaltung der Informatiksicherheitsverordnung protokolliert werden.

[1] https://www.keylength.com/en/8/ respektive https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

III. Passwortvorgaben (Kennwortvorgaben)

- Passwörter oder Kennwörter müssen nach der ersten Benutzung geändert werden.
- Es dürfen keine Standardpasswörter verwendet werden, welche von den Herstellern oder Partnern definiert werden.
- Folgende Vorgaben müssen beim Erstellen eines Passworts eingehalten werden:
    - Es muss aus mindestens 8 Zeichen bestehen
    - Es muss aus der Kombination von mindestens drei der folgenden vier Zeichen-Gruppen bestehen:
        - Grossbuchstaben
        - Kleinbuchstaben
        - Zahlen
        - Sonderzeichen
- Passwörter müssen alle 90 Tage geändert werden.

Falls möglich, sind diese Vorgaben technisch umzusetzen respektive vorzugeben (siehe Konfigurationsbeispiele K101: Benutzernamen und Passwörter).

IV. Umgang mit Benutzernamen und Passwörtern (Kennwörtern)

- Benutzernamen und Passwörter (Kennwörter) sind persönlich und nicht übertragbar (§ 21 Abs. 2e und 3d Informatiksicherheitsverordnung).
- Passwörter sind geheim zu halten, eine Weitergabe ist nicht erlaubt, auch nicht an Vorgesetzte oder an IT-Fachpersonen (§ 21 Abs. 2e und 3d Informatiksicherheitsverordnung).
- Die Benutzerkonto-Informationen müssen in einem geregelten und kontrollierbaren Verfahren zugeteilt werden (§ 13 Abs. 3 Informatiksicherheitsverordnung).
- Für private und kantonale Benutzerkonten sind nicht dieselben Passwörter zu benutzen.
- Für das Speichern von Passwörtern ist ausschliesslich die von der Dienstelle Informatik zur Verfügung gestellte Passwortverwaltungs-Software zu verwenden[2].
- Das ungesicherte schriftliche Festhalten von Passwörtern ist nicht gestattet.

Falls der Verdacht besteht, dass ein Passwort erraten, ausgeplaudert oder kompromittiert wurde, so ist es unverzüglich zu wechseln. Falls dies wegen systemseitiger Passworteinstellungen nicht möglich ist, ist der Service-Desk zu benachrichtigen (unter anderem falls sich das Passwort nur einmal pro Tag wechseln lässt).

V. Anforderungen an Systeme

- Inaktive Benutzer-Sessions müssen spätestens nach 15 Minuten gesperrt werden.
  Inaktive mobile Geräte (Mobiltelefone, Tablets) müssen spätestens nach 5 Minuten gesperrt werden.
  Bietet das System keine Sperrfunktion, muss die Benutzer-Session beendet werden.
  Bietet das System keine Funktion zum automatischen Abmelden oder Sperren einer Benutzer-Session, muss sich der oder die Mitarbeitende abmelden, sobald er oder sie die Arbeitsstation verlässt.
- Bietet ein System zum Schutz der Konfiguration eine Passwort-Funktionalität, ist diese Funktion zwingend zu benutzen.

Falls möglich, sind diese Vorgaben technisch umzusetzen respektive vorzugeben (siehe Konfigurationsbeispiele K101: Benutzernamen und Passwörter).

[2] wird mit dem iWP2.0 (Windows 10) verfügbar

VI. Ausnahmen

Ausnahmen können vom zuständigen OIB zusammen mit dem Informationssicherheitsbeauftragten des Kantons Luzern definiert werden.

Ausgenommen von der Sperrung nach 15 Minuten Inaktivität sind:

- öffentliche Systeme (Kioskmodus, Public Displays)
- Benutzer-Sessions auf Servern (ausgenommen Terminal Server)
- technische Benutzerkonten (Service Accounts, s. Kap. Übergangsfristen)

VII. Übergangsfristen

Für technische Benutzerkonten gelten Übergangsfristen bis 31. Dezember 2019.
Für alle anderen Benutzerkonten gibt es keine Übergangsfristen.

Dokumentenlenkung

Version	1.3	**Datum Erstellung**	22.02.2017
Dokumentbesitzer	DIIN CISO/MUM	**Datum Freigabe**	16.03.2016
Tritt in Kraft per:	01.04.2017		
Freigegeben durch	Informationssicherheitsbeauftragter, OVG		
Übergeordnete Dokumente	- Informatikgesetz vom 7. März 2005 (SRL Nr. 26) - Informatiksicherheitsverordnung vom 22 November 2016 (SRL Nr. 26b)		
Mitgeltende Dokumente	keine		
Weiterführende Dokumente	Konfigurationsbeispiele K101: Benutzernamen und Passwörter		