HSLU Hochschule Luzern

Richtlinie
Passwortsicherheit

Änderungsverzeichnis

Version	Datum	Status	Änderungen und Bemerkungen	Bearbeitet von
Nr. 0.1	19.6.2023		Dokument bearbeitet und fertiggestellt	poa/zic
Nr. 0.2	27.6.2023		Dokument bearbeitet	IT Services
Nr. 1.0	6.7.2023	Final	In Kraft gesetzt durch A. Kallmann	

Inhaltsverzeichnis

Der Verwaltungsdirektor

gestützt auf Artikel 6 der Weisung über die Benutzung von Informatikmitteln der Hochschule Luzern, FH Zentralschweiz vom 14. Juni 2018,

beschliesst:

I. Allgemeine Bestimmungen

Art. 1 *Zweck*

Die von der Hochschule Luzern angebotenen IT-Dienste werden mithilfe von Passwörtern vor unberechtigtem Zugriff geschützt. Zu diesen Diensten gehören z.B. das HSLU-Benutzerkonto zur Anmeldung an der HSLU-Domäne, ILIAS, EventoWeb, Webmail, SAP, VPN, AAI, WLAN und diverse Cloud-Services. Passwörtern kommt deshalb in sicherheitstechnischer Hinsicht eine grosse Bedeutung zu. Geraten Passwörter in falsche Hände, kann grosser Schaden entstehen. Die vorliegende Richtlinie macht Vorgaben zum richtigen Umgang mit Passwörtern. Dazu gehört insbesondere die Verwendung von starken Passwörtern und die Sicherstellung von deren Vertraulichkeit.

Art. 2 *Adressaten*

Die Richtlinie richtet sich an alle Angehörigen[1] der Hochschule Luzern, welche Daten in elektronischer Form bearbeiten, d.h. über ein oder mehrere Benutzerkonten verfügen. Sie gilt auch für Dritte, welche im Auftrag der Hochschule Luzern auf HSLU-Systemen Daten bearbeiten.

Art. 3 *Geltungsbereich*

Die Richtlinie gilt für sämtliche Passwörter, die für die Anmeldung an den von IT Services bereitgestellten IT-Diensten verwendet werden. Dazu gehören insbesondere die Anmeldung am HSLU-Benutzerkonto, an lokal zur Verfügung gestellten IT-Diensten aber auch an Cloud-Diensten, die von IT Services bereitgestellt werden.

[1] Angehörige der Hochschule Luzern sind deren Mitarbeitende und Studierende (Artikel 11 Absatz 1 Zentralschweizer Fachhochschul-Vereinbarung vom 15.9.2011)

II. Regeln

Art. 4 *Passwortwechsel*

Die Hochschule Luzern verzichtet bei den von ihr bereitgestellten IT-Diensten auf regelmässige, d.h. zeitabhängige Passwortwechsel. Passwörter müssen jedoch zwingend geändert werden, wenn der Verdacht besteht, dass ein Passwort gestohlen oder auf andere Art und Weise bekannt wurde. Darüber hinaus muss es auch geändert werden, wenn es Anzeichen gibt, dass ein Dienst missbräuchlich (d.h. von nicht autorisierten Personen) genutzt wird.

Art. 5 *Komplexitätsanforderungen an Passwörter*

[1] Minimale Passwortlänge: 12 Zeichen aus untenstehendem Zeichensatz, wobei aus drei der vier Gruppen mindestens je ein Zeichen verwendet werden muss

Zeichensatz:

- Kleinbuchstaben: a-z
- Grossbuchstaben: A-Z
- Zahlen: 0-9
- Sonderzeichen (abschliessende Liste): _ + - ? # * @ ! $ % ~ = / \ ( ) . , ; :[2]

[2] Einzelne Wörter, welche in einem Lexikon zu finden sind (egal in welcher Sprache), dürfen nicht als Passwörter verwendet werden. Auch wenn diese Wörter durch eine Reihe von Zahlen und/oder Sonderzeichen am Anfang oder Ende ergänzt werden, sind sie nicht zulässig. Diese Anforderungen stellen sicher, dass Passwörter nicht einfach erraten und vor allem auch nicht durch automatisiertes Durchprobieren mithilfe von Wortlisten (so genannte lexikalische Attacken und Varianten davon[3]) ermittelt werden können. Beispiele für nicht zulässige Passwörter: *Komposthaufen, Komposthaufen21* oder *4Komposthaufen5*.

[3] Ebenfalls leicht zu erraten und deshalb untersagt ist die Verwendung von Namen von Familienangehörigen, Freunden oder Haustieren, Geburtsdaten, Adressen, Nummern von Kontrollschildern oder Telefonnummern und Anmeldenamen von Benutzerkonten. Gleiches gilt für Buchstaben oder Zahlensequenzen, wie 123456, abcdef, qwertz usw.

[2] Leerschläge gehören nicht dazu.

[3] Diese Varianten werden als hybride Attacken bezeichnet; bei diesen werden den durchzuprobierenden Wörtern Zahlen und/oder Sonderzeichen vorangestellt oder danach angefügt.

[4] Passphrasen[4]: Die Verwendung von Passphrasen ist bei Einhaltung der folgenden Bedingungen erlaubt.

- Minimale Länge der Passphrase: 16 Zeichen (maximale Länge:128)
- Zeichensatzanforderung wie oben (mindestens je ein Zeichen aus drei der vier Gruppen)
- Keine bekannten Sätze oder Zitate aus Büchern oder Liedern
- Korrektes Beispiel: koriander=pilzFigurbaum

[5] Passworthistory: Einmal benutzte und dann gewechselte Passwörter dürfen nicht wieder eingesetzt werden. Aus diesem Grund wird die Wiederverwendung von Passwörtern mithilfe einer Passworthistory, welche 24 Einträge enthält, verhindert.

[6] Bei der Verwendung von Sonderzeichen in Passwörtern gilt es zu bedenken, dass diese Zeichen auf Tastaturen ohne bekannte (z.B. schweizerdeutsche) Tastaturbelegung an anderer, allenfalls unbekannter Stelle liegen (weil z.B. der entsprechende Tastaturaufdruck fehlt).

Art. 6 Sicherheitskopien von Passwörtern

[1] Handschriftlich aufnotierte Passwörter (zwecks Verhinderung von Passwortverlust) sind an einem sicheren Ort zu verwahren, idealerweise unter Verschluss.[5]

[2] Elektronische Ablagen sind sicher zu verschlüsseln. Am besten wird dazu ein so genannter Passwort-Safe verwendet. Dabei ist darauf zu achten, dass das Zugangspasswort zum Safe stark ist (komplexes Passwort mit einer Minimallänge von 12 Zeichen).

[3] Passwörter, welche für den Zugriff auf die HSLU-Domäne verwendet werden, dürfen nicht gleichzeitig für andere passwortgeschützte (Cloud-)Services benutzt werden. Grundsätzlich müssen für unterschiedliche Logins immer unterschiedliche Passwörter verwendet werden.

[4] Passwörter dürfen nicht mit anderen Mitarbeitenden oder Privatpersonen geteilt werden. Alle Mitarbeitenden der Hochschule Luzern haben ihre eigenen Passwörter und greifen über diese auf die benötigten IT-Dienste zu.[6]

[5] Passwörter dürfen weder am Telefon noch in elektronischen Fragebogen oder auf sonst eine Art und Weise preisgegeben werden, selbst wenn sie von IT Services nachgefragt werden. „Echte" System-Administratoren fragen nie nach Passwörtern. Passwörter sind persönlich und nur für die persönliche Nutzung bestimmt.

[6] Die insbesondere in Browsern eingebaute „Passwort speichern / merken"-Funktion darf für HSLU-Passwörter nicht verwendet werden, da die zugehörigen Passwort-Datenbanken in der Regel unzureichend geschützt sind und mit einfachen Mitteln ausgelesen werden können. Von dieser Empfehlung ausgenommen sind dedizierte Passwort Safes (z.B. KeePass).

[4] Eine Passphrase ist eine Aneinanderreihung von Wörtern, die zusammen mit einem Benutzernamen zur Anmeldung an einem Benutzerkonto verwendet wird. Passphrasen haben viele Ähnlichkeiten mit Passwörtern. Sie sind aber aufgrund der Zusammensetzung aus einzelnen Wörtern in der Regel länger.

[5] Die Aufbewahrung unter der Tastatur oder unter der Schreibmatte ist nicht als sicher zu betrachten.

[6] Ausnahme: Nicht personalisierte Konten, welche von IT Services verwendet werden.

III. Sanktionen

Art. 7

Bei Missachtung der Regelungen in dieser Richtlinie werden gestützt auf Art. 13 der Weisung über die Benutzung von Informatikmitteln der Hochschule Luzern vom 14. Juni 2018 die folgenden Sanktionsmassnahmen ergriffen:

1. Verwarnung,
2. Beschränkung der Zugriffsberechtigungen auf die eigenen Daten (Lokal und in der Cloud),
3. Bei Mitarbeitenden der Hochschule Luzern Meldung an das zuständige Mitglied der Hochschulleitung (für personalrechtliche Massnahmen) bzw. bei Studierenden Meldung an die zuständige Leitungsperson (für disziplinarische Massnahmen).

IV. Schlussbestimmung

Art. 8 *Inkrafttreten*

Die vorliegende Richtlinie tritt sofort in Kraft. Sie ersetzt alle bisher in ihrem Anwendungsbereich gültigen Regelungen.

Luzern, 6. Juli 2023

Andreas Kallmann
Verwaltungsdirektor