Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

IT Services Support

Werftestrasse 4, Postfach 2969, CH-6002 Luzern
T +41 41 228 21 21
hslu.ch/helpdesk, informatikhotline@hslu.ch

Weisung Kennwortsicherheit

Kurzbeschrieb:	Kennwort-Richtlinien für Angehörige der Hochschule Luzern (HSLU), der Pädagogischen Hochschule Luzern (PHLU) und der Bildungsdirektoren Konferenz Zentralschweiz (BKZ-GS).	
Klassifikation:	☐ IT intern ☐ Andere	☒ Public
Kundengruppe:	☒ HSLU ☒ BKZ-GS	☒ PHLU
Rolle:	☒ Mitarbeitende/Doz. ☐ Andere	☒ Studierende
Geräteverwaltungstyp:	☐ HSLU/PHLU-Geräte ☐ Andere	☐ Private Geräte
Betriebssystem:	☐ Windows ☐ Andere	☐ Mac
Publikation:	☒ hslu.ch/helpdesk ☐ Andere	☒ inside.hslu.ch

Support:

Web:	hslu.ch/helpdesk
E-Mail:	informatikhotline@hslu.ch
Tel:	041 / 228 21 21
Portal:	helpdesk.hslu.ch

Änderungsverzeichnis

Version	Datum	Status	Änderungen und Bemerkungen	Bearbeitet von
Nr. 1.1	24.04.2014		Überführung in CD/CI	mih
Nr. 1.2	13.08.2014	Überarbeitet	Web12	enp
Nr. 1.3	25.02.2016	Überarbeitet	Regelungen für Dienst-, administrative und unpersönliche Konten in ein separates Dokument ausgelagert.	poa
Nr. 1.4	01.12.2016	Überarbeitet	Geltungsbereich und Regeln aktualisiert	poa
Nr. 1.5	11.10.2018	Überarbeitet	Erlaubte Sonderzeichen	buc
Nr. 1.6	31.10.2018	Überarbeitet	Erlaubte Sonderzeichen	buc
Nr. 1.7	17.05.2019	Überarbeitet	Erlaubte Sonderzeichen	buc
Nr. 1.8	13.01.2019	Überarbeitet	Änderung D-EDK zu BKZ-GS	rem

Inhaltsverzeichnis

1. Zweck

Die von der Hochschule Luzern (HSLU) angebotenen IT-Dienste werden mithilfe von Kennwörtern vor unberechtigtem Zugriff geschützt. Zu diesen Diensten gehören z.B. das Windows Benutzerkonto, ILIAS, EventoWeb, Webmail, SAP, VPN, AAI, WLAN usw. Kennwörtern kommt deshalb in sicherheitstechnischer Hinsicht an der HSLU eine grosse Bedeutung zu. Geraten Kennwörter in falsche Hände, kann grosser Schaden entstehen. Die vorliegende Weisung macht Vorgaben zum richtigen Umgang mit Kennwörtern. Dazu gehören insbesondere die Verwendung von starken Kennwörtern und die Sicherstellung von deren Vertraulichkeit.

2. Adressaten

Die Weisung richtet sich an alle Studierenden und Mitarbeitenden der HSLU, welche Daten in elektronischer Form bearbeiten, d.h. über ein oder mehrere Benutzerkonten verfügen. Sie gilt auch für Dritte, welche im Auftrag der HSLU auf HSLU-Systemen Daten bearbeiten.

3. Geltungsbereich

An der HSLU ist kein flächendeckendes Single Sign-on implementiert. Dies bedeutet, dass es IT-Dienste gibt, welche nach der Anmeldung an der Domäne[1] eine zusätzliche Anmeldung erfordern. Zu diesen Diensten gehört z.B. die Unterrichtsplattform «ILIAS». Im Weiteren gibt es Plattformen, die die Anmeldeinformationen unabhängig von der Windows-Anmeldung verwalten. Zu dieser Kategorie gehört z.B. die «Plattform für die Administration von studentischen Arbeiten», kurz «PASTA». Die in der vorliegenden Weisung gemachten Vorgaben für Kennwörter gelten für sämtliche Dienste (unabhängig von der Art der Kennwort-Verwaltung).

4. Regeln

1. Die HSLU verzichtet bei sämtlichen *personalisierten* Konten[2] auf *regelmässige*, d.h. zeitabhängige Kennwortwechsel. Kennwörter müssen jedoch unter den folgenden Bedingungen *zwingend* geändert werden:
   - Bei Verdacht auf Diebstahl oder Missbrauch des Kennworts. In diesem Fall muss das betroffene Kennwort unverzüglich geändert werden. Bei Mehrfachverwendung des gleichen Kennworts muss es bei sämtlichen Diensten geändert werden.
   - Bei Verlust des Kennworts, d.h. wenn es vergessen wurde. IT Services setzt in diesem Fall auf dem betroffenen Dienst ein neues Kennwort, das vom Benutzer durch ein eigenes ersetzt werden muss. Bei Mehrfachverwendung des gleichen Kennworts muss es bei sämtlichen Diensten geändert werden.
2. Komplexitätsanforderungen an Kennwörter:
   - Minimale Kennwortlänge: 10 Zeichen aus untenstehendem Zeichensatz, wobei aus drei der vier Gruppen mindestens je ein Zeichen verwendet werden muss

[1] Diese ist bei den HSLU-Standardrechnern an die Anmeldung an das lokale Windows Benutzerkonto gekoppelt.
[2] Als personalisierte Konten gelten Konten, welche ausschliesslich von einer Person verwendet werden (in diesem Sinne also persönlich sind). Die gewöhnlichen Windows Benutzer-Konten zählen zu den personalisierten Konten.

- Zeichensatz:
  - Kleinbuchstaben: a-z
  - Grossbuchstaben: A-Z
  - Zahlen: 0-9
  - Sonderzeichen (gültige Sonderzeichen: hslu.ch/helpdesk/benutzerkonto/kennwort)
- Wörter, welche in einem Lexikon zu finden sind (egal in welcher Sprache), dürfen nicht als Kennwörter 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 Kennwörter 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 Kennwörter: *Olympiade*, *Olympiade21* oder *4Olympiade5*.
- Ebenfalls leicht zu erraten und deshalb unbedingt zu vermeiden sind 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 etc.
- Kennworthistory: Einmal benutzte und dann gewechselte Kennwörter sollten nicht wieder eingesetzt werden. Aus diesem Grund wird die Wiederverwendung von Kennwörtern mithilfe einer Kennworthistory, welche 24 Einträge enthält, verhindert.

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

3. Sicherheitskopien von Kennwörtern:

   - Handschriftlich aufnotierte Kennwörter (zwecks Verhinderung von Kennwortverlust) sind an einem sicheren Ort zu verwahren, idealerweise unter Verschluss.[4]
   - Elektronische Ablagen sind sicher zu verschlüsseln. Am besten wird dazu ein so genannter Kennwort-Safe verwendet. Dabei ist darauf zu achten, dass das Zugangskennwort zum Safe stark ist (komplexes Kennwort mit einer Minimallänge von 10 Zeichen).

4. Kennwörter, welche für den Zugriff auf IT-Dienste der HSLU verwendet werden, dürfen nicht gleichzeitig für kennwortgeschützte Dienste im Web (Web-Shops, soziale Netzwerke, andere Mail-Dienste etc.) benutzt werden.

5. Kennwörter dürfen nicht mit anderen Mitarbeitenden oder Privatpersonen geteilt werden. Alle Mitarbeitenden der HSLU haben ihre eigenen Kennwörter und greifen über diese auf die benötigten IT-Dienste zu.[5]

6. Kennwörter 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 Kennwörtern. Kennwörter sind persönlich und nur für die persönliche Nutzung bestimmt.

7. Die in unterschiedlichen Anwendungen und Betriebssystemen eingebaute „Kennwort speichern / merken“-Funktion sollte nach Möglichkeit für HSLU-Kennwörter nicht verwendet werden, da die zugehörigen Kennwort-Datenbanken in der Regel unzureichend geschützt sind und mit einfachen Mitteln ausgelesen werden können. Von dieser Empfehlung ausgenommen sind Kennwort-Safes, welche für verknüpfte Anwendungen eine „Kennwort speichern / merken“-Funktion bereitstellen.

---

[3] Diese Varianten werden als hybride Attacken bezeichnet; bei diesen werden den durchzuprobierenden Wörtern Zahlen und/oder Sonderzeichen vorangestellt oder danach angefügt.
[4] Die Aufbewahrung unter der Tastatur oder unter der Schreibmatte ist nicht als sicher zu betrachten.
[5] Ausnahme: Nicht personalisierte Konten, welche von IT Services verwendet werden.

5. Sanktionen

Bei Missachtung der Regelungen in dieser Weisung werden die folgenden Sanktionsmassnahmen ergriffen:

1. Verwarnung
2. Beschränkung der Zugriffsberechtigungen auf die eigenen Daten (Home-Verzeichnis)
3. Meldung an den Vorgesetzten oder Studiengangsleiter