HSLU Hochschule Luzern

Neu mit **Informationen zum mobil-flexiblen Arbeiten!**

Merkblatt Informationssicherheit und Datenschutz

Die Hochschule Luzern unternimmt grosse Anstrengungen, um Ihre Infrastruktur und Ihre Daten vor den Gefahren aus dem Cyberspace zu schützen. Diese technischen Vorkehrungen müssen zwingend durch umsichtiges Verhalten der Mitarbeitenden unterstützt werden. Nur so kann ein umfassender Schutz gewährleistet werden. Helfen Sie dabei mit!

Allgemeine Verhaltenshinweise

Ihre E-Mails

- Klären Sie die Echtheit von verdächtigen E-Mails beim Absender oder bei der Absenderin ab oder löschen Sie solche E-Mails sofort.
- Öffnen Sie nie Links oder Anhänge von verdächtigen E-Mails.
  Tipp: Wenn Sie die Maus ohne zu klicken über den Link führen, wird die Link-Adresse angezeigt und damit ein mögliches Missbrauchsmerkmal erkennbar.
- Schützen Sie sich vor gefälschten Service Desk Mails: E-Mails vom Service Desk der Hochschule Luzern zeigen die folgenden Absenderinformationen:
  Von: Servicedesk HSLU <servicedesk@hslu.ch>
  Werden andere Absenderinformationen angezeigt, liegt eine Fälschung vor. Oft sind solche gefälschten E-Mails auch auf Englisch oder in fehlerhaftem Deutsch geschrieben.
- Schützen Sie sich vor gezielten Phishing-Angriffen (sog. Spear Phishing): Gefälschte E-Mails, die gezielt für eine bestimmte Person erstellt werden, können sehr gut gemacht sein. Achten Sie deshalb auch auf Unstimmigkeiten in den Details und befolgen Sie insbesondere nie ungewöhnliche Aufforderungen ohne deren vorgängige Überprüfung, auch wenn Druck gemacht wird.

Ihre Passwörter

- Nutzen Sie für verschiedene Logins unterschiedliche und komplexe Passwörter.
- Verwenden Sie für die Erstellung von neuen Logins nie das Passwort des Hochschule Luzern-Benutzerkontos.
- Verwenden Sie für private Logins Ihre private Mail-Adresse.
- Schützen Sie Ihre Passwörter mit einem elektronischen Passwort-Tresor. Handschriftlich aufgeschriebene Passwörter müssen vor unberechtigter Einsicht geschützt aufbewahrt werden. Ein Notizzettel unter der Tastatur erfüllt diese Anforderung nicht!
- Geben Sie Passwörter nie weiter, auch nicht an Personen, die sich am Telefon als Administrator ausgeben.
- Ändern Sie bei Missbrauchsverdacht das betroffene Passwort umgehend.
- Nutzen Sie immer die Zweifaktor-Authentifizierung, wenn ein Dienstleister eine solche anbietet.

Ihre Daten und Dokumente

- Geben Sie Daten und Dokumente nur an berechtigte Personen weiter.
- Schützen Sie Daten, Dokumente und Personendaten vor unberechtigtem Zugriff. Konsultieren Sie die Richtlinie zur Datenklassifizierung.
- Erstellen Sie ein Backup von Daten und Dokumenten, die nicht die Abteilung IT Services für Sie sichert. Verbinden Sie das Backup-Medium nur während des Backups mit Ihrem PC.
- Öffnen Sie keine Daten und Dokumente aus unsicheren Quellen (USB-Sticks, die herumliegen etc.).
- Vernichten Sie vertrauliche Dokumente, wenn Sie diese entworgen wollen (z. B. im Reisswolf oder in einem Aktenentsorgungscontainer).

Ihre Geräte

- Sperren Sie Ihre Geräte bei Abwesenheit.
- Lassen Sie mobile Geräte bei Abwesenheit nicht unbeaufsichtigt.
- Verschlüsseln Sie vertrauliche Daten auf mobilen Geräten und mobilen Datenträgern.
- Verwenden Sie keine USB-Sticks, deren Inhalt und Ursprung Ihnen nicht bekannt ist.
- Beachten Sie die Lizenz- und Urheberrechte bei der Verwendung von Applikationen und multimedialen Inhalten.

Ihre privaten Geräte

- Schützen Sie Ihre privaten Geräte mit einem Virenschutzprogramm und einer Firewall.
- Halten Sie Betriebssystem und Anwendungen mithilfe von Updates immer aktuell.
- Arbeiten Sie nach Möglichkeit nicht als «Administrator» sondern als sog. «Standardbenutzer».

Mobil-flexibles Arbeiten

Ihre Arbeit zuhause

- Verwenden Sie für Ihre Arbeit zuhause einen Computer, der ausschliesslich von Ihnen benutzt wird. Familien-, Gaming- oder Homeschooling-Computer sollten nicht dafür verwendet werden.
- Stellen Sie sicher, dass während Ihrer Heimarbeit niemand Zugriff auf Ihren Computer hat.
- Nutzen Sie immer den VPN-Zugang, wenn Sie ausserhalb der Hochschule Luzern arbeiten.
- Verwenden Sie für den Versand von geschäftlichen E-Mails ausschliesslich Ihre Hochschul-E-Mail-Adresse.
- Leiten Sie geschäftliche E-Mails nicht an private E-Mail-Accounts weiter.
- Stellen Sie beim Drucken sicher, dass vertrauliche Dokumente nicht auf dem ausgewählten Drucker liegen bleiben (z. B. auf einem Gerät an der HSLU).

Ihre Arbeit unterwegs

- Verwenden Sie unterwegs – insbesondere bei der Arbeit im Zug – einen Blickschutzfilter, der unberechtigten Personen die Sicht auf den Bildschirm erschwert.
- Nutzen Sie immer den VPN-Zugang, wenn Sie ausserhalb der Hochschule Luzern arbeiten.

Ihre Webkonferenzen

- Konferieren Sie nur dort, wo keine unberechtigten Personen mithören können. Verwenden Sie immer ein Headset – auch wegen der besseren Tonqualität.
- Verlassen Sie während einer aktiven Konferenz Ihren Arbeitsplatz nur, wenn Sie den Desktop gesperrt haben. Drahtlose Headsets verleiten dazu, den Arbeitsplatz zu verlassen.
- Nutzen Sie Screen Sharing sparsam und achten Sie darauf, welche Informationen Sie für andere Konferenzteilnehmende freigeben.
- Nutzen Sie für den Austausch von vertraulichen Informationen oder für besonders schützenswerte Personendaten nur Konferenztools, die dafür von IT Services vorgesehen sind.
- Lassen Sie Einladungen (Links) respektive Zugangsinformationen (ID und Passwort) zu Konferenzen ausschliesslich den Konferenzteilnehmenden zukommen; bitten Sie letztere, die Einladungen nicht an nicht autorisierte Personen weiterzuleiten.
- Bitten Sie Teilnehmende, sich mit Vor- und Nachname einzuwählen (keine Nicknames) und sperren Sie unbekannte Teilnehmende aus.
- Verwenden Sie in einer laufenden Konferenz keine anderen Konferenztools. Möglicherweise werden Audio- und Videosignal in beiden Konferenzen übertragen – z. B. ein Telefonanruf in der laufenden Zoom-Konferenz.
- Lassen Sie den Fernzugriff auf den eigenen Rechner (Fernsteuerung) während einer Webkonferenz nur bei ausgewiesenem Bedarf und für einen begrenzten Zeitraum zu.
- Decken Sie die Kamera bei Nicht-Gebrauch ab.
- Beachten Sie die Urheber- und Persönlichkeitsrechte (insbesondere das Recht am eigenen Bild). Dokumente, Videos und andere Informationen, die in Konferenzen gezeigt werden, dürfen nicht an Dritte weitergegeben werden. Konferenzen dürfen zudem nicht ohne das vorgängige und ausdrückliche Einverständnis aller Beteiligten aufgezeichnet werden.

Seien Sie aufmerksam und geben Sie Betrügern keine Chance!

- Melden Sie Vorfälle und Verdachtsfälle umgehend beim Service Desk.
- Weitere Infos finden Sie im Inside unter hslu.ch/infosec bzw. hslu.ch/dataprotection sowie auf der Website unter hslu.ch/servicedesk/sicherheit.