PRIVATE
PÄDAGOGISCHE HOCHSCHULE
DER DIÖZESE LINZ

IT-Nutzung an der Privaten Pädagogischen Hochschule der Diözese Linz

# BENUTZERRICHTLINIEN:

Diese Nutzungsrichtlinie wird durch das Rektorat der Privaten Pädagogischen Hochschule der Diözese Linz definiert und gilt für alle Studierenden, Lehrenden und Bediensteten der Privaten Pädagogischen Hochschule der Diözese Linz (im Folgenden als „Hochschule“ bezeichnet) für die gesamte Laufzeit des Vertrags. Jegliche Datenschutzbestimmungen gelten auch über das Ende des Vertragsverhältnisses hinaus.

Personenbezogene Bezeichnungen richten sich jeweils an beide Geschlechter. Diese Nutzungsrichtlinie gilt im Netzwerk der Hochschule.

Die Hochschule behält sich das jederzeitige Widerrufsrecht dieser Nutzungsrichtlinie vor und kann die Bestimmungen abändern oder aufheben. In jedem Fall wird die Hochschule alle betroffenen Personen davon in Kenntnis setzen.
Studierende, Lehrende und Bedienstete verpflichten sich zur Einhaltung der Nutzungsrichtlinie und sind angehalten, dieser Nutzungsrichtlinie zuwiderlaufende Handlungen und Missstände dem IT-Sicherheitsbeauftragten (ZID) zu melden. Des Weiteren verpflichten sich die Studierenden, Lehrenden und Bediensteten zur Einhaltung der in der IT-Sicherheitsrichtlinie festgelegten Bestimmungen.

Zuwiderhandlungen bzw. reglementwidrige Benützung der Internetdienste oder jedes andere Verhalten, das einen Verstoß gegen die Pflichten aus dem Arbeitsverhältnis darstellt, können arbeits- und / oder disziplinarrechtliche Sanktionen sowie strafrechtlichen Untersuchungen zur Folge haben.

# Inhalt

# 1. IT-Systeme und Daten

## 1.1 Grundsätze der Nutzung (inkl. Privatnutzung)

Die zur Verfügung gestellten IT-Systeme dienen der Erfüllung dienstlicher Aufgaben. Die private Nutzung innerhalb der Hochschule ist nur dann zulässig, wenn der Lehrbetrieb dadurch nicht gestört wird und die Inhalte dieser Benutzerrichtlinie eingehalten werden. Die Privatnutzung der IT-Systeme außerhalb der Hochschule (z. B. das mit-nach-Hause-nehmen von IT-Systemen zur Verwendung in der Freizeit) ist nicht erlaubt.

Sämtliche durch die Hochschule bereitgestellten Betriebsmittel müssen pfleglich behandelt werden (fix aufgestellte Geräte, Geräte aus dem Medienverleih,…)

Durch die Hochschule bereitgestellte Notebooks oder PCs werden auf Betriebssystem-Ebene regelmäßig mit sicherheitsrelevanten Updates versorgt. Dienstnehmer, die alternative Hard- oder Software betreiben, müssen eigenverantwortlich regelmäßig sicherheitsrelevante Updates auf ihren Geräten (Notebooks, PCs, Mobile Devices,…) einspielen. Für alle durch die Hochschule bereitgestellten IT-Systeme gilt zudem, dass die Umgehung von vorhandenen bzw. integrierten Sicherheitsmechanismen nicht erlaubt ist.

Jegliche Manipulation an den EDV- bzw. IT-Geräten der Hochschule, beispielsweise Abstecken von Peripheriegeräten, Entfernen von Komponenten, Änderungen in der Konfiguration oder des Aufstellortes, etc. bedürfen unbedingt vorab der Information und der Zustimmung des ZID der PHDL.

Beim Umgang mit Daten sind die Bestimmungen des Abschnitts „Datenschutz und Datenanonymisierung“ zu beachten.

## 1.2 IT-Systeme

### 1.2.1 Private IT-Systeme

Die Installation von privater Hard- und / oder Software im Netzwerk der Hochschule ist grundsätzlich nicht zulässig. Private IT-Systeme dürfen mit dem Netzwerk der Hochschule in Verbindung gebracht werden (z. B. private Notebooks / Smartphones mit dem WLAN der Hochschule).

### 1.2.2 Schäden und Verlust von Hochschul-Eigentum

Schäden, Verlust und / oder Diebstahl von Hochschul-Eigentum sind umgehend an den jeweiligen Vorgesetzten und die Technik zu melden.

## 1.3 Netzwerk

Das Betreiben von Hotspots (z. B. über WLAN) in einem Gebäude der Hochschule, nur um dadurch Sicherheitsmechanismen der Hochschule (z. B. Firewall) zu umgehen, ist ausnahmslos verboten.

## 1.4 Speichern von Daten

### 1.4.1 Dateiablage

Das Speichern von privaten Daten auf durch die Hochschule bereitgestellten IT-Systemen ist nur dann zulässig, wenn

- nicht gegen die Inhalte der Benutzerrichtlinie verstoßen wird

- der Lehr- und Dienstbetrieb dadurch nicht beeinträchtigt wird
- diese Daten unmittelbar dem Lehr-/Lernbetrieb dienen

### 1.4.2 Externe Speichermedien

Externe Speichermedien (CD, DVD, USB-Sticks usw.) sind vor Umwelteinflüssen (z. B. Hitzeeinwirkungen) und Diebstahl bzw. Verlust sicher zu verwahren.
Unbekannte Datenträger (z. B. gefundener USB-Stick am Parkplatz) dürfen nicht mit IT-Systemen der Hochschule verbunden werden. Derartige Datenträger müssen ausnahmslos dem IT-Sicherheitsbeauftragten übergeben werden.
Von extern mitgebrachte USB Sticks werden nach dem Anstecken an PCs der Hochschule automatisiert auf Viren und Schadstoffsoftware überprüft.

### 1.4.3 Cloud Services

Aufgrund der derzeit geltenden gesetzlichen Bestimmungen der Datenschutzrichtlinien ist die Verwendung von öffentlichen Cloud-Diensten (z.B. Dropbox, Google Drive,…) zur Speicherung personenbezogener Daten im Auftrag des Dienstgebers nicht erlaubt.

# 2. Security

## 2.1 Sicherheitsrelevante Ereignisse und Schwachstellen

Alle sicherheitsrelevanten Ereignisse sowie erkannte Schwachstellen sind sofort dem IT-Sicherheitsbeauftragten (siehe Pkt.5 – Ansprechperson) zu melden, welcher die Ursache prüft und gegebenenfalls weitere Personen hinzuzieht.
Beispiele für sicherheitsrelevante Ereignisse sind:

- unerklärliches Systemverhalten
- Verlust oder Veränderung von Daten und Programmen
- Verdacht auf Missbrauch der eigenen Benutzererkennung
- usw.

Beispiele für Schwachstellen sind:

- ungewünschte Veröffentlichung von Daten im Internet
- usw.

Für die Aufklärung der Ereignisse sind sämtliche zur Aufklärung notwendigen und hilfreichen Informationen an den IT-Sicherheitsbeauftragten weiterzugeben.

## 2.2 Virenschutz auf Client-Systemen

Die Deaktivierung des Virenschutzes auf den durch die Hochschule bereitgestellten IT-Systemen ist nicht erlaubt.

## 2.3 Verwahrung von Datenträgern

Studierende, Lehrende und Bedienstete der Hochschule sind dafür verantwortlich, vertrauliche Dokumente und/oder Informationsträger (z.B.: USB Sticks, …) sicher zu verwahren.

# 3. Internet und E-Mail

## 3.1 Grundsätze der Nutzung

Studierende, Lehrende und Bedienstete der Hochschule erhalten Zugang zum Internet und ein persönliches E-Mail-Konto (im Folgenden als Internetdienste bezeichnet).

- Das Recht zur Nutzung der Internetdienste darf nicht missbraucht werden. Ein Missbrauch liegt vor, wenn die Internetdienste für strafbare, diffamierende, rassistische, gewaltverherrlichende oder sexistische Aktivitäten genutzt werden (siehe „unzulässige Inhaltsdaten und Aktivitäten“).

## 3.2 Unzulässige Inhaltsdaten und Aktivitäten

Unter keinen Umständen ist es gestattet, Daten abzurufen, zur Verfügung zu stellen oder zu verbreiten, die

- rechtliche und / oder betriebsgefährdende Risiken bergen,
- gegen datenschutzrechtliche und persönlichkeitsrechtliche Bestimmungen verstoßen (z. B. hochschulinterne Daten jeglicher Art, Daten über Studierende usw.),
- gegen urheberrechtliche und strafrechtliche Bestimmungen verstoßen (z. B. Raubkopien, generierte oder gestohlene Seriennummern, Cracks[1] usw.) oder
- widerrechtliche, herabwürdigende, beleidigende, verleumderische, verfassungsfeindliche, rassistische oder pornografische Äußerungen oder Abbildungen sowie Inhalte, die gegen das Verbotsgesetz 1947 (NS-Wiederbetätigung) verstoßen, enthalten.

Insbesondere ist es nicht zulässig,

- Verbindungen mit Diensten aufzunehmen, die (urheberrechtlich geschützte) Daten bereitstellen (z. B. P2P-Netze, BitTorrent usw.) oder selbst Daten über solcherart Dienste bereitzustellen,
- die Sicherheitsvorkehrungen des Dienstgebers zu umgehen (z. B. Proxy, Firewall usw.),
- Hacking[2] oder vergleichbare Handlungen auf interne und externe Systeme, egal in wessen Besitzes, durchzuführen,
- Spieleserver oder ähnliches zu nicht dienstlichen Zwecken zu betreiben,
- jegliche Art von Software herunterzuladen, die nicht für berufliche Zwecke notwendig ist,
- Software ohne gültigen Lizenzvertrag zu installieren bzw. zu verwenden,
- Kopien von urheberrechtlich geschützter Software für die Privatnutzung zu erstellen (insbesondere wenn deren Lizenzen im Besitz des Dienstgebers oder anderen Kunden sind),
- in Internetplattformen oder Diskussionsforen ohne entsprechenden Auftrag im Namen des Dienstgebers aufzutreten oder
- beruflichen E-Mail-Verkehr an ausschließlich privat genutzte E-Mail-Adressen weiterzuleiten.

Diese Aufzählung ist nicht als vollständig anzusehen. Vergleichbare, nicht aufgezählte Inhaltsdaten und Aktivitäten fallen möglicherweise ebenfalls in diese Beschränkung. Im Bedarfsfall ist der IT-Sicherheitsbeauftragte heranzuziehen.

[1] Cracks sind Programme, die Einschränkungen einer Software unrechtmäßig aufheben oder dessen Betrieb ohne gültigen Lizenzvertrag ermöglichen und somit illegal sind.
[2] Als Hacking wird allgemein jede Aktion verstanden, die in irgendeiner Art und Weise sonst geheime Daten hervorbringt, Systeme negativ beeinflusst oder andere Dienstnehmer und Kunden benachteiligt.

# 4. Datenschutz und Datenanonymisierung

## 4.1 Grundsätze

Alle personenbezogenen und sensiblen Daten von natürlichen sowie juristischen Personen (z. B. Personaldaten, Daten über Studierende usw.) unterliegen dem Österreichischen Datenschutzgesetz 2000 in der geltenden Fassung und dürfen nicht unbefugt verarbeitet, genutzt oder weitergegeben werden.

Die Bestimmungen des Österreichischen Datenschutzgesetzes 2000 in der geltenden Fassung sind uneingeschränkt einzuhalten. Datenschutzbestimmungen gelten auch über das Ende des Dienstverhältnisses hinaus.

# 5. Ansprechperson

Als zentrale Ansprechperson für alle datenschutzrechtlichen Anliegen steht der IT-Sicherheitsbeauftragte im ZiD zur Verfügung. (IME Sekretariat: 0732 77 26 66 DW 4702)
Derzeit: ZID – Michael Atzwanger, MSc – helpdesk@ph-linz.at – 0732 77 26 66 DW 4652