

RICHTLINIE FÜR DIE NUTZUNG VON IT-SYSTEMEN

Das Präsidium hat am 16.05.2018 die folgende Richtlinie für die Nutzung von IT-Systemen an der Leuphana Universität Lüneburg beschlossen. Die Richtlinie wird nachfolgend in der redaktionell bearbeiteten Fassung vom 26.02.2020 neu veröffentlicht:

(A) Zielgruppe und Zweck der Richtlinie

1. Diese Richtlinie gilt für alle Beschäftigten der Leuphana Universität Lüneburg bei der Benutzung der IT-Systeme der Leuphana Universität Lüneburg.
2. In dieser Richtlinie werden Regeln zum bewussten, verantwortungsvollen und sicheren Umgang mit dienstlichen und personenbezogenen Daten und IT-Systemen festgelegt. Die personenbezogenen Daten der Mitglieder und Angehörigen und die datenverarbeiteten Systeme und Netzwerke der Leuphana Universität Lüneburg sollen geschützt werden. Mit der kontinuierlich zunehmenden Digitalisierung von Prozessen und Vernetzung der IT-Systeme werden diese immer angreifbarer und müssen zunehmend geschützt werden. Das MIZ verbessert laufend die technisch möglichen Schutzmaßnahmen, aber auch die Anwender*innen müssen ihr Verhalten gemäß den Notwendigkeiten für einen verbesserten Datenschutz anpassen. Mit den Regeln dieser Richtlinie soll bei vertretbarem Aufwand eine möglichst große IT- und Datensicherheit erreicht werden.
3. Die Regeln dienen nicht der Überwachung von Mitgliedern und Angehörigen der Universität oder ihrer Arbeitsleistung.

(B) Allgemeine Hinweise zum Umgang mit personenbezogenen Daten

4. Personenbezogene Daten dürfen innerhalb der Leuphana Universität Lüneburg ausschließlich über entsprechend sichere Kanäle übermittelt werden.
5. Dienstliche E-Mails müssen signiert und bei personenbezogenen Daten – wenn technisch möglich – zusätzlich verschlüsselt übertragen werden. Weitere Informationen dazu finden Sie im Abschnitt „Zertifikate“.

(C) Videokonferenzen und -übertragung

6. Für Videokonferenzen und -übertragungen sind die vom MIZ oder DFN-Verein angebotenen Systeme zu nutzen.

Weitere Informationen:

- www.leuphana.de/miz-videoübertragung
www.vc.dfn.de/videokonferenzen/dienstbeschreibung.html

(D) Terminvereinbarungen und Umfragen mit web-basierten Systemen

7. Die Organisation gemeinsamer Termine mit webbasierter Software wie z.B. *doodle* ist aus datenschutzrechtlichen Gründen nicht gestattet. Hierfür ist ausschließlich der DFN Terminplaner *Foodle+* zu nutzen.



8. Für Umfragen sind die auf einem Leuphana-Server gehosteten Online-Umfrageprogramme LimeSurvey oder EvaSys zu nutzen.

Weitere Informationen:

<https://terminplaner2.dfn.de/>

<https://www.leuphana.de/miz-survey>

(E) Online-Kalender

9. Die Nutzung von außereuropäisch oder bei US-Firmen gehosteten Cloud-Kalendern wie z.B. Google Kalender für dienstliche Zwecke oder unter Verarbeitung personenbezogener Daten von Mitgliedern und Angehörigen der Leuphana Universität Lüneburg ist nicht gestattet. Stattdessen ist der vom MIZ im Rahmen der Groupwarefunktionalität des Mailservers angebotene Kalender zu nutzen. Dieser kann – wie auch andere Accounts – in den E-Mail-Client eingebunden werden.
10. Private Kalender sind von dem dienstlichen Kalender zu trennen.

Weitere Informationen:

www.leuphana.de/miz-groupware

mailhost.leuphana.de/hpronto

(F) Datensicherung – individuelle Backups

11. Dienstliche Daten sind entweder individuell auf lokalen Speichern (nur mit entsprechenden Sicherheitsvorkehrungen) oder auf einem Leuphana-Netzlaufwerk, zu sichern. Die Sicherung auf einem Netzlaufwerk gewährleistet ein regelmäßiges und automatisches Backup und schützt so vor Datenverlust.
12. Die Speicherung dienstlicher Daten oder personenbezogener Daten von Mitgliedern und Angehörigen der Leuphana Universität Lüneburg auf Cloud-Plattformen Dritter ist nicht gestattet. Ausnahmen betreffen die dienstlich notwendige Speicherung von Daten auf gemeinsam mit Kooperationspartnern genutzten Cloud-Plattformen.
13. Folgende, vom MIZ angebotene Dienste sind für die gemeinsame Nutzung und den Austausch von Dateien zulässig.
 - *Netzlaufwerk*: Zentrales Speichern eigener Dateien (inkl. automatischem Backup)
 - *Gruppenlaufwerk*: Zentrales Speichern gemeinsamer Dateien für Leuphana-Arbeitsgruppen (inkl. automatischem Backup)
 - *Academic Cloud Sync&Share*: Sync-and-Share-Lösung analog zu Dropbox (Achtung: die Academic-Cloud eignet sich nicht für das sichere Backup von Daten!)
 - *myShare*: Bereitstellung einer Datei (oder mehrerer als ein ZIP-Archiv) zum Download per Downloadlink für einen begrenzten Zeitraum
 - *Öffentlicher FTP-Server*: Bereitstellen öffentlich lesbarer Dateien
 - *Nichtöffentlicher FTP-Server*: Bereitstellen von Dateien für Berechtigte

Weitere Informationen:

www.leuphana.de/miz-netzlaufwerke

www.leuphana.de/miz-gruppenlaufwerke

www.leuphana.de/miz-ac



www.leuphana.de/miz-myshare
www.leuphana.de/miz-ftp-server

(G) Betrieb von Servern und Speichersystemen

14. Das MIZ betreibt zentral eine Vielzahl von Servern und Speichersystemen für die grundständige IT-Infrastruktur an der Leuphana Universität. Für eine Reihe von Spezialanwendungen werden zentrale Server vom MIZ bereitgestellt. Die Server werden von festangestellten IT-Fachkräften wie Systemadministratoren und Netzwerkern in einem virtualisierten Serverpool betrieben. Die Server werden überwacht, regelmäßig gewartet und weisen eine hohe Verfügbarkeit auf. Die Server sind in automatische Backupprozesse eingebunden. Für die System-Administration bestehen Urlaubs- bzw. Krankheitsvertretungen.
15. Weitere Serversysteme – außerhalb des MIZ – sind grundsätzlich nicht zugelassen. In begründeten Ausnahmefällen kann eine Zulassung beim MIZ beantragt werden. Bei diesen Servern muss eine professionelle Betreuung sichergestellt werden. Serversysteme bei Drittanbietern zur Verarbeitung dienstlicher Daten oder personenbezogener Daten von Mitgliedern und Angehörigen der Leuphana Universität Lüneburg sind grundsätzlich nicht zulässig, sofern sich aus datenschutzrechtlichen Bestimmungen nicht etwas anderes ergibt.

Weitere Informationen:

www.leuphana.de/miz-netzlaufwerke
www.leuphana.de/miz-vserver

(H) Betrieb von Access Points und Netzwerkgeräten

16. Der Aufbau und Betrieb des kabelgebundenen Netzwerkes und des WLANs erfolgt ausschließlich durch das MIZ oder im Auftrag des MIZ. Die selbständige Installation von Netzwerkkomponenten wie Access Points oder Switches ist – auch unter Zuhilfenahme Dritter – nicht zulässig. Für Gäste werden separate Gastzugänge, z.B. eduroam oder das guest-WLAN bereitgestellt.

(I) E-Mail-Konten bei externen Providern

17. Die Leuphana-E-Mail-Accounts dürfen ausschließlich für die dienstliche Kommunikation verwendet werden.
18. E-Mail-Adressen externer Provider (z.B. WEB.DE Mail, Google Mail, Apple Mail) sind für dienstliche Zwecke nicht gestattet. Auch die automatisierte Weiterleitung des dienstlichen E-Mail-Accounts auf externe Mailboxen ist nicht gestattet. Der Empfang von E-Mails von externen Servern, die als Absendeadresse „@leuphana.de“ vorgeben, wird technisch unterbunden. Der Leuphana E-Mail-Account kann in allen gängigen E-Mail-Clients eingebunden werden.
19. Für Webmail ist die Adresse mymail.leuphana.de zu nutzen.

Weitere Informationen:

www.leuphana.de/miz-email

(J) Zertifikate / Verschlüsselung von E-Mails

20. Alle Beschäftigten der Leuphana Universität Lüneburg müssen ein Zertifikat installieren. Die Universität stellt die hierfür notwendige administrative Unterstützung sicher.
21. Das MIZ stellt als offizielle Registrierungsstelle des DFN-Vereins User- und Serverzertifikate aus.



Weitere Informationen:

www.leuphana.de/miz-zertifikate

(K) Antivirensoftware

22. Alle dienstlichen Rechner an der Leuphana Universität sind mit der zentral vorgehaltenen Virenschutzsoftware auszustatten.

Weitere Informationen:

www.leuphana.de/miz-virenschutz

(L) User-Accounts und Passwörter

23. Der Zugang zu den IT-Systemen der Leuphana Universität Lüneburg wird mit User-Accounts und zugehörigen Passwörtern geschützt. Diese Passwörter dürfen nicht in externen Systemen verwendet werden. Im Formular zur Passwortänderung sind ausführliche Regeln für den sicheren Umgang mit Passwörtern aufgelistet.
24. Dienstliche Endgeräte und private Endgeräte, die zu dienstlichen Zwecken verwendet werden, wie Rechner, Notebooks, Tablets oder Mobiltelefone, sind durch Passwörter zu schützen. Es sind getrennte Passwörter zu verwenden.

Zugang zum Passwortänderungsformular:

[www.leuphana.de/miz-passwort \(nur innerhalb des Leuphana-Netzwerkes erreichbar\)](http://www.leuphana.de/miz-passwort (nur innerhalb des Leuphana-Netzwerkes erreichbar))