

DIE ZEHN GOLDENEN REGELN DER IT-SICHERHEIT





DIE SECHSTE GOLDENE REGEL DER IT-SICHERHEIT:
VORSICHT VOR USB-STICK, CD & CO.!

GÄNGIGE FEHLER

WAS MAN NICHT TUN SOLLTE

- Wechselmedien an **Computern ohne Virenschutz** oder **sensiblen Computern**, die aus Sicherheitsgründen nicht mit dem Internet verbunden sind (z. B. aufgrund veralteter Betriebssysteme), nutzen
- Sensible Daten (insbesondere Personendaten) **unverschlüsselt** auf einem Wechselmedium speichern
- USB-Sticks verwenden, die Sie irgendwo (z. B. in der Mensa, in der Bibliothek, auf der Straße) **gefunden** oder **auffallend günstig** auf Plattformen wie eBay erworben haben
- Das **Administrator-Passwort** eingeben, wenn Sie nach dem Einstecken eines Wechselmediums dazu aufgefordert werden



WECHSELMEDIEN? AM LIEBSTEN GAR NICHT MEHR NUTZEN!

Verwenden Sie Wechselmedien zur Datenweitergabe nur, wenn es nicht anders geht!

- Nutzen Sie für die Datenweitergabe bevorzugt **verschlüsselte E-Mails** oder die **Speicherdienste** myShare (empfohlen, da Leuphana-Dienst), Academic Cloud Sync & Share oder Microsoft 365 OneDrive
- Wenn Sie universitätsintern als Arbeitsgruppe gemeinsam Daten ablegen möchten, richtet Ihnen das MIZ gern ein **Gruppenlaufwerk** ein



WENN ES DOCH EIN WECHSELMEDIUM SEIN MUSS... **MINDESTSTANDARDS BEACHTEN!**

- Verwenden Sie nur Wechselmedien **sicherer Herkunft**, z. B. von persönlich bekannten Menschen oder – beim Neukauf – von seriösen Händlern
- Nutzen Sie Wechselmedien niemals an Computern **ohne aktuelle Virenschutzsoftware**
 - (Solche Computer sollten Sie aber auch generell nicht nutzen!)



(NICHT NUR) BEI SENSIBLEN DATEN: **WECHSELMEDIEN WIRKSAM VERSCHLÜSSELN!**

**Speichern Sie sensible Daten ausschließlich verschlüsselt auf Wechselmedien
– oder verschlüsseln Sie gleich das ganze Medium!**

—Einen guten Kompromiss aus Bedienfreundlichkeit und Sicherheit bietet das Arbeiten mit verschlüsselten Dateicontainern und der Software **VeraCrypt**. Eine Anleitung finden Sie im Anleitungs-Wiki des MIZ.



Mit VeraCrypt verschlüsselte Daten oder Datenträger können Sie nur an Computern entschlüsseln, auf denen VeraCrypt installiert ist!



KONTAKT

**WENDEN SIE SICH BEI ALLEN FRAGEN RUND UM DAS THEMA
„IT-SICHERHEIT“ AN DEN IT-SERVICE!**

IT-SERVICE

Hotline 04131.677–1212

it-service@leuphana.de

Service-Counter: C7.004

Öffnungszeiten:

www.leuphana.de/services/miz/service-support/it-support.html

NOCH MEHR GOLDENE REGELN DER IT-SICHERHEIT?

www.leuphana.de/it-sicherheit

