KONTAKT

IT-Servicezentrum

Eingang B, Raum 1209
Ernst-Abbe-Platz 4
07743 Jena

Zum Service-Desk: serviceportal.uni-jena.de

Zu den Anleitungen: wiki.uni-jena.de

Scannen Sie den QR-Code für weitere Kontaktmöglichkeiten

Herausgeber: Stabsstelle für Sicherheit informationstechnischer Systeme
Autor: Oliver Schoßee Fotos: Oliver Schoßee
nach einer Vorlage der Abteilung Hochschulkommunikation

Stand: August 2022

www.uni-jena.de/urz

FESTPLATTE VERSCHLÜSSELN

Alle Laufwerke müssen mit einer geeigneten Software verschlüsselt sein. Gerade bei Laptops, welche mobil verwendet werden, ist die Festplattenverschlüsselung im Fall eines Verlusts oder Diebstahls wichtig. Windows stellt die vorinstallierte Verschlüsselungssoftware BitLocker zur Verfügung.

Anleitung für Windows 10 & 11

⇒ Systemsteuerungen
⇒ System und Sicherheit
⇒ BitLocker-Laufwerksverschlüsselung
⇒ BitLocker aktivieren
⇒ Wiederherstellungsschlüssel speichern oder ausdrucken
⇒ Nur verwendeten Speicher verschlüsseln (bei neuen bzw. leeren Laufwerken)
oder
Gesamtes Laufwerk verschlüsseln (für bereits verwendete Laufwerke)
⇒ Zusätzliche Prüfung aktivieren und neu starten

Beim Verschlüsselungsprozess generierte Schlüssel (auch mittlerweile nicht mehr benutzte) dürfen nie ungeschützt, das heißt auslesbar oder unverschlüsselt, abgelegt werden. Sie müssen getrennt vom verschlüsselten Gerät aufbewahrt werden.

WLAN NUTZUNG

Die Verbindung zu öffentlichen Hotspots sollte vermieden werden, da diese meist nicht ausreichend gesichert sind. Für die kabellose Internetverbindung in Einrichtungen der Universität steht Eduroam zur Verfügung.

VPN CLIENT

Für eine sichere Kommunikation zwischen dem Rechner und dem internen Universitätsnetz kommt eine VPN-Verbindung zum Einsatz. Um eine VPN-Verbindung aufzubauen, steht die Software Cisco AnyConnect Client zur Verfügung.

Anleitung für Windows 10 & 11

⇒ Downloadseite:
„www.uni-jena.de/vpn-windows-apple-mobile“
⇒ Für Windows 10 & 11 die folgende Datei nutzen:
„anyconnect-win-4-10-05111-core-vpn-predeploy-k9.msi“
⇒ Installations Dialog folgen
⇒ „Cisco AnnyConnect Secure Mobility Client“ starten
⇒ „vpn.uni-jena.de“ als Server eingeben
⇒ URZ Login für die Anmeldung verwenden

FRIEDRICH-SCHILLER-
UNIVERSITÄT
JENA Universitätsrechenzentrum

WINDOWS 10 & 11

Sicherheits– und Datenschutzeinstellungen

Nicht relevant für zentral administrierte Geräte

Scannen Sie den QR-Code um zur digitalen Anleitung zu gelangen

DATEN SICHER SPEICHERN

Für die Datensicherung wird die Verwendung von storage.uni-jena.de oder Nextcloud als zentraler Speicher empfohlen. Der Clouddienst von Microsoft darf nicht verwendet und muss deaktiviert werden.

Anleitung für Windows 10 & 11

⇒ Windows-Taste + r
⇒ „gpedit.msc“ eingeben
⇒ Mit Strg + Shift + Eingabetaste bestätigen
⇒ Computerkonfiguration -> Administrative Vorlagen -> Windows-Komponenten -> OneDrive
⇒ Verwendung von OneDrive für die Datenspeicherung verhindern
⇒ Aktiviert wählen

Bei der Datensicherung auf externen Festplatten ist darauf zu achten, dass die Backup-Datenträger verschlossen aufbewahrt werden. Zusätzlich muss der externe Datenträger verschlüsselt sein. (Anleitung siehe Festplattenverschlüsselung)

WINDOWS AKTUELL HALTEN

Es ist wichtig, das Betriebssystem und die Anwendung möglichst aktuell zu halten. Nur so kann verhindert werden, dass eventuell offene Schwachstellen am System ausgenutzt werden können. Die Windows Updates sollten automatisch installiert werden.

DATENSCHUTZ ANPASSEN

Die Windows-Einstellungen müssen dahingehend angepasst werden, dass keine Telemetriedaten an Microsoft gesendet werden. Dafür müssen die folgenden Punkte deaktiviert werden: Datenschutzoptionen, Spracherkennung, Diagnosedaten, Aktivitätsverlauf und Positionserkennung.

Zur Unterstützung kann die kostenlose Software "O&O ShutUp10" verwendet werden (für Windows 10 & 11 geeignet). Eine Installation ist nicht nötig, da es sich um eine portable Version handelt.

Anleitung für Windows 10 & 11

⇒ Downloadseite: „www.oo-software.com/de/shutup10“ möglich.
⇒ Konfigurationsdatei mit vorgeschlagenen Einstellungen befindet sich in der digitalen Anleitung

Nach Windows-Funktionalupdates müssen die Datenschutzeinstellungen erneut zu prüfen.

VIRENSCHUTZ

Zum Schutz vor Schadsoftware muss ein aktiviertes Computer-Viren-Prüfprogramm installiert werden.

Anleitung für Windows 10 & 11

⇒ Downloadseite: „www.uni-jena.de/virenschutz“
⇒ Sophos-Softwaredownload
⇒ SophosSetup-mit-InterceptX_Win
⇒ Installations Dialog folgen
⇒ Sophos über Icon starten (Taskleiste -> Pfeil-Symbol)

FIREWALL AKTIVIEREN

Eine weitere Schutzkomponente ist die lokale Firewall, welche unbedingt aktiviert bleiben muss.

Anleitung für Windows 10 & 11

⇒ Systemsteuerungen
⇒ System und Sicherheit
⇒ Windows Defender Firewall
⇒ Windows Defender Firewall ein– oder ausschalten
⇒ Firewall in allen Bereiche aktivieren

SYSTEM ZURÜCKSETZEN

Bevor der verwendete Rechner weitergegeben wird, muss dieser vollständig zurückgesetzt werden.

Anleitung für Windows 10

⇒ Windows-Taste + i (Einstellungen)
⇒ Update & Sicherheit
⇒ Wiederherstellung
⇒ Diesen PC zurücksetzen -> Los geht´s
⇒ Alles entfernen
⇒ Daten entfernen und Laufwerk bereinigen

Anleitung für Windows 11

⇒ Windows-Taste + i (Einstellungen)
⇒ System
⇒ Wiederherstellung
⇒ PC zurücksetzen
⇒ Alles entfernen
⇒ Daten entfernen und Laufwerk bereinigen

SICHERE ANMELDUNG

Die Nutzung des Rechners mit einem Microsoft-Konto ist nicht erlaubt. Bei der Installation oder im Anschluss daran ist es möglich, einen lokalen bzw. Domänennutzer einzurichten.

Zudem sollte für die tägliche Arbeit am Rechner ein Standardbenutzer ohne Administratorrechte verwendet werden.

Für jeden Benutzer ist dabei ein unterschiedliches und ausreichend komplexes Passwort zu verwenden. Die Passwörter dürfen nicht unverschlüsselt gespeichert werden. Alternativ kann ein Tool wie KeyPass bei der Verwaltung der Anmeldedaten unterstützen.

Die Anforderungen an ein Passwort befinden sind im Dokument „rundschreiben-passwort.pdf“ unter hanfried.uni-jena.de.

FERNWARTUNG

Zur Fernwartung ist das Online-Fernhilfe-Tool ISL Light 4 zu nutzen. Dabei ist darauf zu achten, dass die Fernadministration nur durch Supportmitarbeiter der Uni Jena durchzuführen ist.