

Die Nutzung privater IT-Endgeräte für dienstliche Zwecke ist gem. § 15 Abs. 8 der IT-Ordnung der TU Dresden wie folgt geregelt:

„Die Nutzung privater Endgeräte (Laptops, Smartphones, Tablets) für dienstliche Zwecke ist zulässig, wenn die gleichen Standards wie für TUD IT-Technik angewendet werden, dies betrifft vor allem die Datensicherung und Verschlüsselung der Daten. Ein Anspruch auf Support für private Endgeräte durch IT-Administratorinnen und IT-Administratoren besteht nicht.“

Das **cfaed** legt daher die folgenden Standards fest:

- **Verbindliche Nutzung der Antiviren Software Sophos** (auch für das Privatgerät einsetzbar auf Mac OSX, Windows und Linux)
https://tu-dresden.de/zih/dienste/service-katalog/arbeitsumgebung/dir_software/softwareliste/virenschutz/sophos/index
Der Einsatz einer Antivirensoftware auf Smartphones ist mit der IT abzustimmen.
- Der Benutzer hat auf seinem Endgerät für die dienstliche Nutzung unter einem **normalen Benutzeraccount** zu arbeiten. Die Arbeit direkt als Administrator oder root im dienstlichen Kontext ist grundsätzlich nicht zulässig. Es gelten die Passwortrichtlinien des ZIH.
- **Verbindlicher Einsatz einer Verschlüsselungssoftware** für die dienstlichen Daten bei Notebooks (vorzugsweise Festplattenverschlüsselung, z.B. Windows mit integriertem BitLocker, Mac OSX mit integriertem File Vault und Linux integrierte Festplattenverschlüsselung).
- Auf Smartphones ist die Nutzung der **Outlook App für iOS und Android blockiert**, andere Mailprogramme sind zugelassen für die Anbindung von Exchange, die **Synchronisation des Globalen Adressbuches** (5000 TUD Kontakte) ist dabei zu **deaktivieren** -> online Zugriff ist aber möglich.
https://tu-dresden.de/zih/die-einrichtung/zih-info/zih_info_91#1
<https://tu-dresden.de/zih/dienste/service-katalog/zusammenarbeiten-und-forschen/groupware/exchange/Anleitungen#section-5>
- Für die **Nutzung der Netzlaufwerke von außerhalb** der TUD ist der Aufbau einer **VPN-Verbindung** erforderlich. Zu verwenden ist die Software Cisco AnyConnect:
https://tu-dresden.de/zih/dienste/service-katalog/arbeitsumgebung/zugang_datennetz/vpn
- Für die **dienstlichen Daten ist ein Datenbackup sicherzustellen**. Für ein Backup stehen folgende Möglichkeiten zur Verfügung:
 - Netzlaufwerke (cfaed vFiler oder Home-Laufwerk am ZIH), oder

- cfaed Clientbackup, welches über das cfaed VPN bzw. im Campusnetz (nicht Gästernetz) alle 12 Stunden ein Backup von definierten Verzeichnissen erstellt. Für die Nutzung des Clientbackups bitte an die cfaed IT wenden.
- Für **dienstliche Zwecke installierte Software (Home-Use-Recht des Herstellers muss vorliegen)** muss nach **Beendigung des Dienstverhältnisses** wieder **entfernt werden**. Es sind die jeweils gültigen Lizenzbestimmungen einzuhalten. Derzeit nutzbare Software (https://tu-dresden.de/zih/dienste/service-katalog/arbeitsumgebung/dir_software/softwareliste):
 - MS Office 2016 Pro ca. 13€
 - Software der Firma Corel
 - Sophos, Cisco Any Connect
 - Home-Use-Recht für Adobe-Einzelplatzlizenzen
 - Mathematica
 - Origin Pro (Studentenlizenz)
- Bei **Beendigung des Dienst- oder Arbeitsverhältnisses** sind die **dienstlichen Daten** auf dem privaten Endgerät der **TU Dresden zu übergeben** und anschließend **vom Gerät zu löschen**.

Hiermit bestätige ich oben genannte Hinweise und Vorgaben gelesen und verstanden zu haben. Ich verpflichte mich, diese Vorgaben einzuhalten.

Ich wurde darauf hingewiesen, dass ein Verstoß gegen die vorgenannten Standards als grobe Fahrlässigkeit anzusehen ist.

Ich stimme einer notwendigen Überprüfung der Einhaltung der vorgenannten Standards meines Gerätes durch den zuständigen IT-Administrator in meinem Beisein zu.

Datum, Unterschrift Mitarbeiter