



Sicheres Arbeiten im Home-Office

Derzeit laufen in den unterschiedlichsten Bereichen des privaten und beruflichen Lebens Maßnahmen zur Verlangsamung der Ausbreitung des Corona-Virus. Als eine solche Maßnahme bittet Sie die Universität kurzfristig und vorübergehend bestimmte dienstliche Tätigkeiten von zu Hause aus zu erledigen (Telearbeit/Home-Office). Damit Sie gut, aber auch sicher von zu Hause arbeiten können, haben wir die wichtigsten Punkte für Sie zusammengefasst:

Allgemeine Hinweise und Regelungen zur Handhabung von dienstlichen Daten im Home-Office

- Denken Sie daran: Bearbeiten Sie dienstliche Daten bitte ausschließlich im häuslichen Bereich und nicht in der Öffentlichkeit (z.B. in einem Café, wo ihnen jemand zusehen kann).
- Die Ihnen bereits bekannten Dienste zur Speicherung bzw. Verarbeitung dienstlicher Daten stehen Ihnen auch weiterhin zur Verfügung. Dazu zählen beispielsweise die Netzlaufwerke, Sciebo¹, DFNconf² etc. Darüber hinaus können auch externe, durch die Universität freigegebene Dienste³ verwendet werden wie beispielsweise Skype. Eine Liste der freigegebenen IT-Dienste stellt das BITS bereit.
- Die Nutzung von Skype ist aus rechtlichen Gründen nur eingeschränkt möglich. Bitte nutzen Sie es ausschließlich für Videokonferenzen. Es sollten keine Personaldaten, Gesundheitsdaten oder Dienstgeheimnisse übermittelt werden. Zusätzlich soll kurzfristig mit Zoom eine weitere Alternative bereitgestellt werden. Bitte beachten Sie dazu die Hinweise auf der BITS Homepage⁴.
- Bitte schützen Sie dienstliche Daten gegen unbefugten Zugriff. Dazu zählt auch der Zugriff durch Personen, die mit Ihnen in häuslicher Gemeinschaft leben.

Maßnahmen sind hier insbesondere:

- Keinen Einblick auf den Bildschirm
 - Sperrung des Gerätes bei Nichtgebrauch
 - Sichere Verwahrung von Unterlagen
- Wir möchten Sie und die Universität vor dem Verlust von vertraulichen, dienstlichen Daten schützen. Aus diesem Grund sind die Festplatten aller durch das BITS ausgegebenen Laptops verschlüsselt. Sofern Ihr Gerät nicht durch das BITS ausgegeben wurde, sprechen Sie bitte Ihre EDV-Betreuung auf die Festplattenverschlüsselung an. Bitte achten Sie auch darauf, Datenträger (z.B. USB-Sticks) nur verschlüsselt⁵ zu transportieren.

¹ <https://www.uni-bielefeld.de/einrichtungen/bits/services/speicher/sciebo/>

² <https://www.conf.dfn.de/>

³ <https://uni-bielefeld.de/einrichtungen/bits/arbeiten-unterwegs.xml>

⁴ Siehe Fußnote 3

⁵ Anleitung zur Verschlüsselung mobiler Datenträger: https://www.tsb.uni-hannover.de/encrypt_usb.html



- Klären Sie bitte mit Ihrer*m Vorgesetzten, welche Akten ggf. im häuslichen Bereich bearbeitet werden müssen und dokumentieren Sie deren Mitnahme. Akten, die vertrauliche Daten enthalten, sollten nur dann mitgenommen werden, wenn dies aus Gründen der Arbeitsorganisation unter den gegenwärtigen Bedingungen unbedingt erforderlich ist.
- Transportieren Sie Papierunterlagen bitte ausschließlich in verschlossenen Behältnissen (z.B. einem Rucksack) und auf dem kürzesten Weg zwischen heimischem Arbeitsplatz und Dienststelle.
- Vernichten Sie vertrauliche Papierunterlagen bitte nur in der Dienststelle.

Allgemeine Regelungen für dienstliche IT-Geräte

- Zum Arbeiten von Zuhause aus benötigen Sie insbesondere für die Arbeit mit SAP oder den Netzlaufwerken eine VPN-Verbindung⁶. Dienste wie beispielsweise E-Mail oder das BIS können auch ohne VPN-Verbindung verwendet werden. Eine Nutzung öffentlicher WLAN-Netze (z.B. in Cafés) ist nicht gestattet.
- Zur Speicherung Ihrer Daten stehen Ihnen wie gewohnt die Netzlaufwerke der Universität zur Verfügung. Sollten diese aus technischen Gründen einmal nicht erreichbar sein, denken Sie bitte daran, lokal bearbeitete Daten umgehend auf den Netzlaufwerken abzulegen, sobald diese wieder verfügbar sind. Nur so sind Ihre Daten gegen einen Datenverlust gesichert. Alternativ steht Ihnen auch weiterhin „Sciebo“, die Campus-Cloud der Universität, zur Verfügung.
- Verwenden Sie für dienstliche E-Mail-Kommunikation bitte ausschließlich die E-Mail-Adresse(n) der Universität. Aus rechtlichen Gründen ist eine permanente Weiterleitung von dienstlichen E-Mails an private Anbieter wie Gmail, GMX, web.de etc. nicht gestattet.

Regelungen für die Nutzung privater IT-Geräte

- Als Beschäftigte der zentralen oder dezentralen Verwaltung beachten Sie bitte, dass die Nutzung von privaten IT-Geräten nicht gestattet ist.
- Für die Beschäftigten aus den Bereichen Forschung und Lehre gilt, dass für die Bearbeitung von dienstlichen Daten grundsätzlich ebenfalls dienstliche IT-Geräte genutzt werden sollen. Sollten dienstliche IT-Geräte nicht in ausreichender Zahl zur Verfügung stehen, beachten Sie bitte folgendes:
 - Es gibt Daten, die z.B. durch gesetzliche oder vertragliche Anforderungen besonders gut geschützt werden müssen und daher einen hohen Schutzbedarf haben. Dazu zählen beispielsweise Studierendendaten, Personalaktendaten, Gesundheitsdaten oder bestimmte wissenschaftliche Daten. Bitte beachten Sie, dass private Geräte aus Gründen des Datenschutzes und der Informationssicherheit nicht für eine Verarbeitung von Daten mit hohem Schutzbedarf geeignet sind.

⁶ <https://www.uni-bielefeld.de/einrichtungen/bits/services/netzzugang/vpn/>



- Darüber hinaus kann die EDV-Betreuung Sie bei technischen Problemen mit privaten IT-Geräten nicht unterstützen.

Mindestanforderungen an ein privates IT-Gerät

- Verwendung Sie bitte ein aktuelles Betriebssystem⁷ mit allen relevanten Sicherheitsupdates.
- Ein aktueller Virenschanner (kostenlos beim BITS⁸) schützt Sie gegen schädliche Software.
- Ebenso ist eine aktuelle Software-Firewall notwendig (ist z.B. bei Windows 10 bereits integriert).
- Ihr IT-Gerät wird durch ein ausreichend sicheres Passwort geschützt, dass nur Ihnen bekannt ist.
- Zur Bearbeitung dienstlicher E-Mails nutzen Sie bitte den Uni-Webmailer⁹. Auf Smartphones kann auch die installierte E-Mail-App genutzt werden.
- Dienstliche Daten sollten, soweit technisch möglich, ausschließlich auf den Netzlaufwerken bearbeitet werden.
- Achten Sie bitte darauf, bei Beendigung der dienstlichen Nutzung des Privatgerätes alle dienstlichen Daten vollständig von diesem zu löschen.

Ansprechpersonen

Ansprechfall	Person/Bereich	Kontakt
Technische Fragen zum Home-Office	EDV-Betreuung der Fakultät oder Einrichtung	PEVZ ¹⁰ unter „Funktionsträger“
Fragen zu diesem Dokument	Informationssicherheitsbeauftragte*r	-3032 oder informationssicherheit@uni-bielefeld.de

Stand: 24.03.2020

⁷ Dazu zählen z.B. Windows 8 und 10, MacOS High Sierra, Mojave und Catalina sowie etliche Linux-Varianten.

⁸ <https://www.uni-bielefeld.de/einrichtungen/bits/services/allgemein/virenschutz/>

⁹ <https://www.uni-bielefeld.de/webmail/index.html>

¹⁰ https://ekvv.uni-bielefeld.de/pers_publ/publ/FunktionssucheAnzeige.jsp?einrArtId=12584082