TECHNISCHE UNIVERSITÄT DRESDEN

Mobiles Arbeiten an der TU Dresden

Ungeachtet der Vielzahl gesetzlicher und rechtlicher Regelungen zum Datenschutz und zur IT-Sicherheit sind bei der mobilen Arbeit die im folgenden genannten Grundsätze zu beachten. Sollten Sie sich unsicher sein, wie und ob Sie diese einhalten können, so steht Ihnen das Sachgebiet Informationssicherheit gern beratend zur Seite.

DATENSCHUTZ

Papierunterlagen werden nur in geeigneten Behältnissen mit nach Hause genommen.

Arbeiten Sie immer, so möglich, mit Kopien von Papierunterlagen und nicht mit Originaldokumenten.

Die Entsorgung von Papierunterlagen erfolgt nicht über den Hausmüll, sondern ausschließlich im Büro über die Datenschutzcontainer der TU Dresden.

Achten Sie darauf, dass Telefongespräche nicht von unbefugten Personen mitgehört werden (z. B. offenes Fenster, laufende andere Videokonferenz, ...).

Bei der mobilen Arbeit ist die Umgebung so auszugestalten, dass vom Grundsatz her die Vertraulichkeit und Verfügbarkeit der Daten wie im Büro sichergestellt ist.

Stellen Sie sicher, dass Papierunterlagen beim Transport nach/von zu Hause nicht erhöhten Risikosituationen (z.B. Rücksitz beim Einkaufen, Rucksack im Restaurant, ...) ausgesetzt werden sollen.

Nehmen Sie nur die Unterlagen (Akten und elektronische Daten) mit, die Sie unbedingt zur Erledigung Ihrer Aufgaben benötigen. Im Zweifelsfall stimmen Sie sich mit Ihrer bzw. Ihrem Vorgesetzten ab.

Sollte Sie einen Verlust von Dokumenten feststellen, so sind Sie verpflichtet, dies unverzüglich Ihrer/Ihrem Vorgesetzten mitzuteilen. Dies betrifft sowohl Papierunterlagen als auch elektronische Daten.

Der Arbeitsplatz ist so gewählt, dass Dritte keinen Blick auf den PC bzw. das Notebook oder in die Papierunterlagen werfen können. Es gilt eine Clean-Desk-Policy am Ende des Arbeitstages, d.h. das die Papierunterlagen aufgeräumt und geschützt aufbewahrt werden.

Kontakt:
informationssicherheit@tu-dresden.de | Tel. +49 (0) 351 463 32839

TECHNISCHE UNIVERSITÄT DRESDEN

Mobiles Arbeiten an der TU Dresden

Besonders schützenswerte Daten (z.B. sensible Forschungs- oder Personendaten) sollten grundsätzlich nur mittels von der TU Dresden bereitgestellter oder genehmigter Hard- und Software verarbeitet werden.
Die TU Dresden trägt die Verantwortung für die Verarbeitung. Die Nutzung privater IT für dienstliche Zwecke erfolgt eigenverantwortlich und sollte nur in Ausnahmefällen erfolgen und auch nur dann, wenn keine besonders schützenswerten Daten verarbeitet werden. Die Nutzung privater IT für dienstliche Zwecke kann nicht angewiesen werden. Bei mobiler Arbeit mit privaten Geräten gelten folgende Mindestanforderungen:

IT-SICHERHEIT

A–Z — Verwenden Sie zum Anmelden an Ihren privaten PC/Notebook immer starke Passworte (mindestens 9 und maximal 127 Zeichen / es sollte mindestens 1 Zeichen aus jeder der folgenden Gruppen enthalten: a - z A- Z 0 - 9 ! $ % / ( ) = ? [ ] { } + # < > , ; : . - _

Zur Kollaboration und Speicherung von dienstlichen Daten verwenden Sie bitte ausschließlich die vom ZIH bereitgestellten Ressourcen (Gruppenlaufwerke, Sharepoint, Cloudstore).

Trennen Sie auf Ihren privaten Geräten unbedingt private von dienstlichen Daten durch die Verwendung verschiedener Benutzerkonten (privat/dienstlich).

Bitte beraten Sie sich dokumentiert vorab mit Ihrer/Ihrem Vorgesetzten, welche Daten auf der privaten IT verarbeitet werden dürfen und welche nicht.

Bitte beachten Sie, dass Support für private Endgeräte durch IT-Administratorinnen und IT-Administratoren nicht möglich ist.

Verwenden Sie zur Fernadministration und zum Fern-Support die Remote-Support-Software der TU Dresden (ISL Light).

Nutzen Sie für Ihre Arbeitsaufgaben nur für die dienstliche Nutzung an der TU Dresden zugelassene Software.

Berücksichtigen Sie bei der Entscheidung zur Verwendung privater IT auch haftungsrechtliche Fragen.

Nutzen Sie für Video- und Telefonkonferenzen die seitens der TU Dresden bereitgestellten Dienste.

Installieren Sie die kostenfrei von der TU Dresden zur Verfügung gestellte Virenschutzsoftware.

VPN — Verwenden Sie, um auf Ressourcen im Campusnetz zuzugreifen, den VPN-Dienst der TU Dresden.

Nutzen Sie zum mobilen Datentransport ausschließlich verschlüsselte Datenträger.

Kontakt:
informationssicherheit@tu-dresden.de | Tel. +49 (0) 351 463 32839