Kurzüberblick zum Datenschutz und zur Informationssicherheit bei Mobiler Arbeit für Beschäftigte der Technischen Universität Chemnitz vom 21. November 2022[1]

DATENSCHUTZ während der Mobilen Arbeit

Die Verarbeitung dienstlicher Informationen/Daten im Rahmen der Mobilen Arbeit ist auf das **ERFORDERLICHE MASS ZU BESCHRÄNKEN**. Nicht mehr benötigte Informationen/Daten sind unverzüglich an die Dienststelle zurückzuführen.

Dienstliche Informationen/Daten dürfen nur in **HINREICHEND SICHEREN UND GEEIGNETEN BEHÄLTNISSEN** zwischen der Dienststelle und dem Mobilen Arbeitsplatz transportiert werden. Das Transportrisiko ist geeignet zu begrenzen (bspw. unmittelbarer Weg ohne Zwischenstopps).

Der Mobile Arbeitsbereich sollte **ABSCHLIESSBAR** bzw. zumindest **ABTRENNBAR** und für Unberechtigte nicht einsehbar gestaltet sein und hinreichende **VERSCHLUSS- UND VERSTAUMÖGLICHKEITEN** bieten („aufgeräumter Arbeitsplatz“), so dass unberechtigte Personen (gilt auch für Familienangehörige) keinerlei Zugang oder Zugriff auf dienstliche Informationen/Daten (gilt bspw. auch für das unberechtigte Mithören von Telefonaten, Videokonferenzen) erhalten können (Vertraulichkeit).

Der Mobile Arbeitsplatz ist unter **WAHRUNG DES GESUNDHEITSSCHUTZES UND DER ARBEITSSICHERHEIT** zu gestalten, um mögliche Fehlerrisiken bei der Informations-/Datenverarbeitung zu minimieren (bspw. hinreichende Beleuchtung, Belüftung).

Um einen Verlust von Informationen/Daten möglichst ausschließen zu können, ist auf eine hinreichende **PHYSISCHE SICHERHEIT** u. a. der IT-Systeme zu achten (bspw. Diebstahlschutz).

Dienstliche Informationen/Daten werden grundsätzlich über **GEEIGNETE ENTSORGUNGSEINRICHTUNGEN AM DIENSTLICHEN ARBEITSPLATZ** und nicht im privaten Hausmüll entsorgt und bis dahin sicher verwahrt und transportiert.

Werden **BESONDERS SCHÜTZENSWERTE INFORMATIONEN/DATEN** (z. B. Beschäftigten-, Prüfungs-, Gesundheitsdaten) verarbeitet, sind regelmäßig **BESONDERE SCHUTZMASSNAHMEN** erforderlich (bspw. Einzeldatenverschlüsselung, Zwei-Faktor-Authentifizierung).

SICHERHEITSRELEVANTE VORKOMMNISSE UND DATENSCHUTZVERLETZUNGEN (bspw. Verlust von Informationen/Daten, Phishing-Angriffe) sind dem Fachvorgesetzten **UNVERZÜGLICH ZU MELDEN**, welcher gegebenenfalls weitere Meldungen an das URZ, den Datenschutzbeauftragten der TU Chemnitz etc. veranlasst.

Kontakt: https://www.tu-chemnitz.de/rektorat/dsb/ | Datenschutzbeauftragter der TU Chemnitz

Informationen/Empfehlungen des Datenschutzbeauftragten:
https://www.tu-chemnitz.de/rektorat/dsb/vorlagen.html#dokumentation

[1] Aus Gründen der besseren Lesbarkeit wird im Folgenden in der Regel das generische Maskulinum verwendet. Sämtliche Personenbezeichnungen gelten aber selbstverständlich für alle Geschlechter.

INFORMATIONSSICHERHEIT während der Mobilen Arbeit

Die **TU CHEMNITZ TRÄGT DIE VERANTWORTUNG FÜR DIE DIENSTLICH BEREITGESTELLTE UND FREIGEGEBENE / ADMINISTRIERTE HARD- UND SOFTWARE**, welche nicht privat und nicht durch unberechtigte Dritte genutzt werden darf. Veränderungen oder Manipulationen sind grundsätzlich unzulässig. Eine **SICHERE VERWAHRUNG** ist zu gewährleisten, ein Verlust ist unverzüglich zu melden.

Die **NUTZUNG PRIVATER HARD- UND SOFTWARE** erfolgt freiwillig, eigenverantwortlich und auf eigenes Risiko (**PERSÖNLICHES HAFTUNGSRISIKO**) und sollte deshalb nur ausnahmsweise und nur bei einem normalen Schutzbedarf der betroffenen Daten/Informationen unter Wahrung einer hinreichenden Datentrennung (dienstlich vs. privat) erfolgen. **EIN SUPPORT DURCH DIE TU CHEMNITZ FINDET NICHT STATT.** Installieren Sie wenn möglich und lizenzrechtlich zulässig die kostenfrei von der TU Chemnitz zur Verfügung gestellte Virenschutzsoftware.

Installierte **SOFTWARE** (u. a. Betriebssystem, Virenschutzsoftware) muss regelmäßig auf **SICHERHEITSUPDATES** überprüft werden. Verfügbare Updates sind unverzüglich (möglichst automatisiert) zu installieren.

Bei regulären Tätigkeiten sind **KEINE ADMINISTRATIONSBERECHTIGUNGEN** zu nutzen.

Die **WEITERLEITUNG DIENSTLICHER E-MAILS** an private E-Mail-Accounts ist **UNZULÄSSIG**.

Auch bei kurzzeitiger Arbeitsunterbrechung ist ein **HINREICHENDER ZUGRIFFSSCHUTZ** sicherzustellen (bspw. passwortgeschützte Tastatur-/Bildschirmsperre, Security-Token).

Es sollten ausschließlich **SICHERE UND EINMALIGE PASSWÖRTER** verwendet werden (mindestens acht Stellen aus allen vier Zeichenklassen), welche vertraulich zu behandeln sind. **WIR FRAGEN SIE NIEMALS NACH IHREM PASSWORT!**

Grundsätzlich sollten von der TU Chemnitz zur Verfügung gestellte und **ZENTRAL KONFIGURIERTE DATENVERARBEITUNGSSYSTEME ÜBER EINE VPN-VERBINDUNG** der TU Chemnitz genutzt werden (u. a. TUCcloud, AFS-Verzeichnisse, BigBlueButton der TU Chemnitz).

FREMDE IT-SYSTEME (z. B. WLAN-Hotspot am Bahnhof, Flughafen) gelten grundsätzlich als **UNSICHER** und erfordern eigene Sicherungsmaßnahmen (bspw. VPN, SSH, HTTPS).

MOBILE DATENBESTÄNDE sollten zwangsweise und hinreichend **VERSCHLÜSSELT** sein. Gleichwohl ist die **VERFÜGBARKEIT UND WIEDERHERSTELLBARKEIT** zu gewährleisten. Fremde Datenträger sollten vor der Verwendung u. a. auf Schadsoftware geprüft werden.

Machen Sie sich bewusst, dass gerade während der Mobilen Arbeit die **GEFAHR SOG. SOCIAL ENGINEERING ANGRIFFE** besonders hoch ist. Auf einen **SORGSAMEN UMGANG** sollte geachtet werden (bspw. bei Downloads, Verlinkungen, Telefonanrufen, privaten Gesprächen).

Kontakt: *support@hrz.tu-chemnitz.de* | URZ-Nutzerservice

Informationen/Empfehlungen des URZ: *https://www.tu-chemnitz.de/urz/desktop/mobil/*

BESTÄTIGUNG DER KENNTNISNAHME / EINWILLIGUNGSERKLÄRUNG

Die Beschäftigten sind auch während der Mobilen Arbeit dazu verpflichtet und tragen hierfür die Verantwortung, sich an die geltenden Vorschriften betreffend den Datenschutz und die Informationssicherheit zu halten. Ausführlichere Hinweise entnehmen Sie bitte dem „Merkblatt zum Datenschutz und zur Informationssicherheit bei Mobiler Arbeit für Beschäftigte der Technischen Universität Chemnitz vom 21. November 2022“ (Anlage 3 der Dienstvereinbarung zur Mobilen Arbeit) sowie den einschlägigen Empfehlungen u. a. des Datenschutzbeauftragten der TU Chemnitz und des Universitätsrechenzentrums, insbesondere zu den Anforderungen an mobile Geräte.

Der „Kurzüberblick zum Datenschutz und zur Informationssicherheit bei Mobiler Arbeit für Beschäftigte der Technischen Universität Chemnitz vom 21. November 2022“ ist mir heute überreicht und von mir zur Kenntnis genommen worden. Darüber hinausgehend versichere ich, dass ich auch die von der Dienststelle zur Verfügung gestellten ausführlichen Hinweise betreffend den Datenschutz und die Informationssicherheit bei Mobiler Arbeit in der jeweils aktuell gültigen Fassung zur Kenntnis genommen habe und zukünftig nehmen werde sowie diese beachte.

Datum	Unterschrift Beschäftigte/r