Sicheres Arbeiten im Home-Office

Sie sind gelegentlich oder ausschließlich, vorübergehend oder dauerhaft im Home-Office tätig?
Egal, ob Sie lehrend, forschend oder verwaltend arbeiten – damit Sie gut, aber auch sicher von zu Hause arbeiten können, haben wir die wichtigsten Dinge für Sie zusammengefasst:

Umgang mit dienstlichen Daten im Home-Office

- Bearbeiten Sie dienstliche und insbesondere vertrauliche und personenbezogene Daten bitte ausschließlich im häuslichen Bereich und nicht in der Öffentlichkeit.

- Schützen Sie auch im häuslichen Umfeld die Daten gegen unberechtigten Zugriff oder Verlust, auch durch Personen, die mit Ihnen in häuslicher Gemeinschaft leben. Sie sollten
  - ✓ möglichst einen abschließbaren Raum für das Arbeiten im Home-Office nutzen,
  - ✓ schriftliche Unterlagen verschlossen/sicher verwahren und nicht ausgebreitet liegen lassen und einen Ausdruck dienstlicher Dokumente möglichst vermeiden,
  - ✓ besonders vertrauliche Unterlagen möglichst nicht im Home-Office verwahren oder baldmöglichst in die Hochschule zurückführen,
  - ✓ nicht mehr benötigte dienstliche Unterlagen datenschutzkonform vernichten (Schreddern, Zerreißen oder Vernichtung über die Datentonnen der Hochschule),
  - ✓ dienstliche/vertrauliche Telefonate nicht in Anwesenheit anderer Personen führen.

- Bitte nutzen Sie ausschließlich die bereitgestellte oder den Sicherheitsanforderungen der Hochschule genügende Hard- und Software. Insbesondere sollten Sie
  - ✓ dienstliche Daten nicht auf privaten Datenträgern (USB-Sticks) speichern,
  - ✓ dienstlich zur Verfügung gestellte Hard- oder Software nicht privat nutzen oder durch Dritte (dienstlich oder privat) nutzen lassen,
  - ✓ für dienstliche Korrespondenz ausschließlich die dienstliche E-Mail-Adresse nutzen und diese jedenfalls nicht permanent an Postfächer privater Anbieter (gmail, gmx, web.de) weiterleiten,
  - ✓ keinen Einblick auf den Bildschirm gewähren,
  - ✓ dienstlich genutzte IT-Geräte bzw. –Anwendungen bei (auch nur kurzem) Nichtgebrauch sperren.

- Für die dienstliche Nutzung von Videokonferenz-Tools beachten Sie bitte das Merkblatt Sichere Nutzung von Video-/Webkonferenz-Tools.

- Bei der dienstlichen Nutzung von Messenger-Diensten sollten diese für Zweier- und Gruppenunterhaltungen eine Ende-zu-Ende-Verschlüsselung gewährleisten. Über Messenger sollten grundsätzlich keine sensiblen Informationen und Daten ausgetauscht werden.

Allgemeine Regelungen für die Nutzung dienstlicher IT-Geräte

- Zum Zugriff auf Netzlaufwerke beim Arbeiten von zu Hause aus benötigen Sie eine VPN-Verbindung. Andere Dienste (E-Mail, Videokonferenzen) können auch ohne VPN-Verbindung verwendet werden.

- Eine Nutzung öffentlicher oder unverschlüsselter WLAN-Netze (z. B. in Cafés) für die dienstliche Tätigkeit sollte unterbleiben bzw. ist nur mit verbundenem VPN im Profil „Tunnel All" gestattet.
- Zur Speicherung Ihrer Daten stehen Ihnen wie gewohnt die Netzlaufwerke der Hochschule zur Verfügung. Sollten dies aus technische Gründen einmal nicht erreichbar sein, denken Sie bitte daran, lokal bearbeitete Daten umgehend auf den Netzlaufwerken abzulegen, sobald diese wieder erreichbar sind. Nur so sind Ihre Daten gegen Datenverlust gesichert.

Allgemeine Regelungen für die dienstliche Nutzung privater IT-Geräte

- Beschäftigten der zentralen und dezentralen Verwaltung ist die dienstliche Nutzung von privaten IT-Geräten grundsätzlich nicht gestattet.

- Für die Beschäftigten im Bereich der Lehre gilt, dass für die Bearbeitung von dienstlichen Daten grundsätzlich ebenfalls dienstliche Geräte genutzt werden sollen. Sollten dienstliche IT-Geräte nicht oder nicht in ausreichender Anzahl zur Verfügung stehen, ist folgendes zu beachten:
  - ✓ Es gibt Daten, die aufgrund gesetzlicher oder vertraglicher Anforderungen besonders gut geschützt werden müssen. Dazu zählen bspw. Studierendendaten, Personaldaten, Gesundheitsdaten oder bestimmte wissenschaftliche Daten. Private Geräte sind jedoch aus Gründen des Datenschutzes und der Informationssicherheit für eine Verarbeitung solcher Daten mit hohem Schutzbedarf nicht geeignet und dürfen daher jedenfalls für diese Datenverarbeitungen nicht genutzt werden.
  - ✓ Die Hochschule kann Sie bei technischen Problemen mit privaten IT-Geräten – auch im Rahmen einer dienstlichen Nutzung – grundsätzlich nicht unterstützen.

  Darüber hinaus sind bei der dienstlichen Nutzung privater IT-Geräte und Netze folgende Mindest-anforderungen zu beachten:
  - ✓ Verwenden Sie bitte ein aktuelles Betriebssystem mit allen relevanten Sicherheitsupdates. Ein aktueller Virenscanner schützt gegen schädliche Software. Ebenso ist eine aktuelle Firewall-Software notwendig.
  - ✓ Schützen Sie Ihr IT-Gerät durch ein ausreichend sicheres Passwort, das nur Ihnen bekannt ist.
  - ✓ Das im Home-Office genutzte WLAN muss mit einem sicheren Passwort (WPA2 oder WPA3) geschützt werden. Der private Internetanschluss kann mitverwendet werden.
  - ✓ Für Speicherung und Austausch dienstlicher Daten sollten – soweit technisch möglich – die Netzlaufwerke sowie der Webmailer der Hochschule genutzt werden. (s. o.)
  - ✓ Achten Sie bitte darauf, spätestens bei Beendigung der dienstlichen Nutzung eines Privatgeräts alle dienstlichen Daten vollständig von diesem zu löschen.

Umgang mit Datenpannen

Sollten Sie im Rahmen Ihrer Tätigkeit im Home-Office eine mögliche Datenpanne – also die Möglichkeit einer unberechtigten Kenntnisnahme oder eines Verlusts personenbezogener Daten – feststellen, haben Sie dies unverzüglich nach Maßgabe der Meldekette für einen (potentiellen) Datenschutzverstoß gemäß EU-DSGVO zu melden. Dies gilt auch bei einem Verlust dienstlich genutzter (mobiler) IT-Geräte.

Ansprechpartner

Technische Fragen:	IT-Abteilung	support@hfm-weimar.de
(Datenschutz)rechtliche Fragen:	Justiziariat | Datenschutz	datenschutz@hfm-weimar.de