Anlage 1

Anforderungen an mobile IT-Geräte

Bei mobiler Arbeit gelten die gleichen Anforderungen an Datenschutz und Informationssicherheit, wie bei der Tätigkeit in der Dienststelle. Da u. a. das Risiko für einen unberechtigten Zugriff auf zu schützende Daten durch Dritte außerhalb der Dienststelle als höher einzuschätzen ist, müssen Sicherheitsvorkehrungen getroffen werden. In Abhängigkeit von der Tätigkeit und dem Schutzbedarf der zu verarbeitenden Daten ergeben sich verschiedene Anforderungen an die verwendeten mobilen IT-Geräte.

Wesentlich für die mobile Arbeit an der Hochschule Wismar sind die durch das BSI (Bundesamt für Sicherheit in der Informationstechnik) vorgegebene Maßnahmen des IT-Grundschutz-Kompendiums *) in aktueller Version.

Der Einsatz dienstlicher IT-Geräte im Umfeld der mobilen Arbeit ist zu bevorzugen, allerdings wird der Einsatz privater IT-Geräte im Umgang mit Daten, welche keinen oder geringen Schutzbedarf unterliegen, nicht ausgeschlossen. Im Umgang mit besonders sensiblen und schutzbedürftigen Daten (bspw. Personal- oder Finanzdaten, Studierendendaten, Daten kritische Infrastruktur betreffend) hingegen, ist der Einsatz privater Geräte nicht erlaubt.

Folgende Anforderungen sind bei mobiler Arbeit zu beachten:

1 Die dienstliche Nutzung mobiler Endgeräte muss so erfolgen, dass durch unberechtigte Dritte keine Einsicht genommen werden kann. Dies muss auch bei dienstlichen Telefonaten berücksichtigt werden, die so zu führen sind, dass es zu keinem ungewollten Informationsabfluss kommt.

2 Der Zugriff auf dienstlich genutzte Geräte muss durch einen Zugriffsschutz (Passwort, Zugriffscode, Fingerabdruck oder ähnliches) abgesichert sein.

3 Dienstlich genutzte Geräte müssen über ein aktuelles Betriebssystem verfügen. Updates, vor allem Sicherheitsupdates, sind umgehend einzuspielen. Zudem sollten dienstlich genutzte Geräte über ein aktuelles Antivirenprogramm verfügen.

4 Der Zugriff auf Dienste der Hochschule Wismar darf nur über gesicherte Kommunikationswege erfolgen.

5 Der Zugriff auf interne Dienste und Netzbereiche darf nur über besonders abgesicherte Verbindungen erfolgen. Die Einrichtung dieser Verbindungen obliegt ausschließlich autorisierten IT-Mitarbeitern der Hochschule Wismar.
Beim Einsatz privater Geräte ist keine direkte Anbindung an interne Dienste oder Netzbereiche erlaubt. Der Zugriff wird auf ausschließlich bildübertragende Kommunikationsverbindungen (Web VPN, Citrix, VDI oder ähnliches) beschränkt.

6 Das Speichern dienstlicher Daten auf privaten Geräten ist grundsätzlich untersagt. Dies betrifft vor allem auch das Speichern dienstlicher Kennwörter auf privaten Geräten. Ein Speichern dienstlicher Daten ist nur in bzw. auf dienstlichen Speichermedien gestattet. Hierunter fallen u.a. die dienstliche Netzlaufwerke, dienstliche USB-Sticks oder die hochschuleigene CampusCloud.

7 Da das Speichern von Daten auf dienstlichen Geräten gestattet ist, sind diese im Speziellen gegen Verlust abzusichern.

7.a Die dienstlichen Endgeräte sind stets sicher zu verwahren und dürfen in öffentlichen Bereichen nicht unbeaufsichtigt bleiben.

7.b Der geschäftliche Bereich lokaler Datenspeicher bei Laptops, Tablet oder auch Smartphone ist gegen Datenverlust bspw. durch Verlorengehen oder Diebstahl abzusichern. Der Einsatz adäquater (Verschlüsselungs-) Technologien, insbesondere in sensiblen Bereichen, ist mit den IT-Mitarbeitern abzustimmen und umzusetzen.

7.c Der Verlust eines dienstlichen Gerätes ist umgehend den IT-Mitarbeitern zu melden.

.....	.....
Datum	Unterschrift der/des Beschäftigten

*) https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html