Anlage 4:
**Merkblatt zu Datenschutz und IT-Sicherheit** Stand: 12/2020

**Entnehmen Sie nur erforderliche Daten.**
Entnehmen Sie nur die dienstlichen Daten aus der Beschäftigungsstelle, die unbedingt erforderlich sind. Personenbezogene und vertrauliche Daten sollen nicht entnommen werden.

Bei dienstlicher Notwendigkeit können analoge Ressourcen vorab digitalisiert werden. Über die tubCloud oder VPN kann dann auf die Daten und das TU-Netz zugegriffen werden. In Ausnahmefällen können Daten verschlüsselt auf einem USB-Stick gespeichert werden.

**Geben Sie keine Daten an Unbefugte weiter.**
Schützen Sie alle Daten und Unterlagen, insbesondere die personenbezogenen und vertraulichen so, dass ein unberechtigter Zugang oder Zugriff wirksam verhindert wird. Sie dürfen weder an Dritte weitergegeben noch zur Einsicht zur Verfügung gestellt werden.

**Schützen Sie Ihre Geräte.**
Lassen Sie Ihren mobilen Arbeitsplatz nicht unbeaufsichtigt. Sperren Sie die von Ihnen genutzten Geräte bei Inaktivität und bewahren Sie sie sicher auf. Eine Weitergabe dienstlicher Geräte an Dritte ist untersagt. Nutzen Sie auf privaten Geräten ein separates Nutzerprofil für den dienstlichen Gebrauch und schützen Sie dieses mit einem Passwort. Halten Sie Passwörter geheim. Verwenden Sie bei Bedarf eine Blickschutzfolie für Ihren Laptop.

**Nutzen Sie geeignete Software-Produkte.**
Verwenden Sie auf privaten Geräten möglichst die gleichen Produkte wie am dienstlichen Arbeitsplatz. Lizenzen stehen in der Regel über die ZECM zur Verfügung. Um dienstliche E-Mails, Kalender und Adressbuch zu nutzen, nutzen Sie die von der ZECM empfohlenen Produkte. Achten Sie darauf, für den dienstlichen Gebrauch auch auf Tablets und Smartphones datenschutzgerechte Apps und Dienste einzusetzen. Löschen Sie Apps und deinstallieren Sie Software, die Sie nicht (mehr) benötigen. Verwenden Sie nur an der TU mitbestimmte und zugelassene Produkte, externe Cloud-Dienste wie Skype, DropBox, GoogleDrive und iCloud dürfen beispielsweise nicht genutzt werden.

**Halten Sie die Technik Ihrer Geräte sicher.**
Stimmen Sie sich bei dienstlichen Geräten regelmäßig mit Ihrer lokalen Arbeitsplatzbetreuung ab, damit diese die erforderlichen Systemeinstellungen und Aktualisierungen vornehmen kann.

Konfigurieren Sie Ihre privaten Geräte entsprechend den Empfehlungen der ZECM und der Datenschutzbeauftragten. Nutzen Sie für diese Aufgaben ein separat einzurichtendes Administrations-Profil. Aktualisieren Sie regelmäßig das Betriebssystem und alle installierten Programme/Apps. Installieren Sie eine Virenschutzsoftware und aktivieren Sie die Firewall auf Ihren Geräten. Deaktivieren Sie die Rufnummernanzeige auf ihren privaten Telefonen, wenn Sie diese den Gesprächspartnern nicht anzeigen möchten.

**Fragen Sie nach.**
Die Datenschutzbeauftragten und ZECM helfen, wenn Sie Unterstützung benötigen.

**Bleiben Sie auf dem aktuellen Stand:**

- Unter https://www.tu-berlin.de/asv/menue/datenschutz, finden Sie Informationen zum Datenschutz. Zahlreiche Hinweise und ausführliche Anleitungen finden Sie im Datenschutz-Blog https://blogs.tu-berlin.de/datenschutz_notizen/category/anleitungen
- Gern beraten wir Sie telefonisch und per E-Mail info@datenschutz.tu-berlin.de
- Nutzen Sie die Weiterbildungsangebote der TU, z.B. unter https://www.wb.tu-berlin.de
- Informationen erhalten Sie auch auf den Webseiten der ZECM https://www.campusmanagement.tu-berlin.de/