UNIVERSITÄT SIEGEN

Informationssicherheitsbeauftragte der Universität Siegen

Informationssicherheit: Voraussetzungen für Mobile Arbeit

Sehr geehrte Nutzende,

bei der Mobilen Arbeit entstehen höhere Anforderungen an die Informationssicherheit, da in den meisten Fällen eine weniger sichere Infrastruktur im Vergleich zu einem internen Büro-Arbeitsplatz vorliegt. Die dienstlichen Informationen könnten durch Unbefugte (auch durch Schadsoftware etc.) missbraucht, gelöscht, eingesehen oder manipuliert werden. Ein besonders erhöhtes Risiko besteht beim Einsatz von Geräten, die nicht entsprechend der Informationssicherheitsvorgaben der Universität Siegen konfiguriert sind (z.B. Fremd-Geräte).

Die folgenden Voraussetzungen für Mobile Arbeit sind zu befolgen und entsprechend umzusetzen:

- Mobile Arbeit ist nur für Informationen mit höchstens normalem Schutzbedarf erlaubt (Hinweise zum Schutzbedarf finden Sie im IT-Grundschutzkatalog für Anwender https://www.uni-siegen.de/it-sicherheit/richtlinien/downloads/it-grundschutzkatalog_anwender.pdf - Link nur intern erreichbar).

- Der Zugang zu allen universitätseigenen Systemen (z.B. NAS, UB-Dienste, Citrix etc.) muss verschlüsselt (bspw. durch Nutzung von https oder VPN) erfolgen.

- Werden unsichere Netzwerke (z.B. Hotspots, Hotel, Gratis-WLAN in Cafés etc.) für das Mobile Arbeiten genutzt, muss auf die verschlüsselte Kommunikation besonders geachtet werden.

- Die VPN-Verbindung darf nur für die notwendige dienstliche Kommunikation genutzt werden. Nach Beendigung der Kommunikation ist die Verbindung zu trennen.

- Es müssen regelmäßig Datensicherungen der dienstlichen Daten durch die mobil Arbeitenden angelegt werden.

- Dienstliche Daten dürfen nur auf Dienstgeräten bzw. innerhalb der Speicherdienste der Universität Siegen gespeichert werden (NAS, SharePoint, ggf. Sciebo).

- Es dürfen nur so wenige Daten wie unbedingt nötig auf mobilen Geräten und externen Speichermedien (USB-Sticks, Festplatten etc.) gespeichert werden. Bestenfalls sind die dienstlichen Daten durch lokale Verschlüsselung zu schützen. Die Geräte selbst sind mindestens mit einem Passwortschutz zu versehen.

- Die eingesetzten Systeme müssen über einen umfassenden Virenschutz sowie eine lokale Firewall verfügen. Der Virenschutz und die Firewall müssen aktuell gehalten werden.

- Die eingesetzten Systeme müssen regelmäßig mit Patches und Updates der Betriebssystem- und Anwendungssoftware versorgt werden.

- Es muss sichergestellt werden, dass Unbefugte nicht auf Geräte und papierbasierte Unterlagen (bspw. Notizen), die für die Mobile Arbeit genutzt werden, zugreifen können.

Bspw. sollten bei Verlassen des mobilen Arbeitsplatzes Türen abgeschlossen und Fenster geschlossen sowie die eingesetzten IT-Geräte gesperrt oder heruntergefahren werden.

- Alle relevanten Änderungen an den dienstlichen Clientsystemen (z.B. Installation neuer Software) müssen dokumentiert werden.

- Die IT-Geräte und Unterlagen dürfen während der Mobilen Arbeit bzw. der Nutzung der Dienste der Universität Siegen nicht an Dritte weitergegeben werden, auch nicht vorübergehend.

- Fremd-IT darf nur in Notfällen eingesetzt werden. Es dürfen keine Daten lokal auf diesen Geräten gespeichert werden. Entstehen temporäre Daten, werden diese nach Gebrauch der Geräte gelöscht.

- Die Verwendung von Blickschutzfolien wird für die Mobile Arbeit in öffentlichen Bereichen (Hörsaal, Zug, Tagungen etc.) grundsätzlich empfohlen.

- Informationssicherheitsvorfälle müssen zentral im ZIMT gemeldet werden: zimt-helpdesk@uni-siegen.de, 0271 / 740 4777

  Unter Informationssicherheitsvorfälle fallen bspw. der Befall von Systemen mit Schadsoftware oder auch der Verlust/Diebstahl von Informationen und IT-Geräten.

- Das ZIMT behält sich die vorübergehende Sperrung von Diensten und Zugängen (Accounts) bei sicherheitsrelevanten Vorfällen vor.

Anleitungen zu vielen Themen finden Sie auf den Internetseiten des ZIMTs (www.zimt.uni-siegen.de) und der Stabsstelle Informationssicherheit (www.uni-siegen.de/it-sicherheit).

Der mobile Arbeitsplatz muss vergleichbare Rahmenbedingen wie die Arbeit an einem Büroarbeitsplatz in den Gebäuden der Universität Siegen aufweisen. Insofern gelten die Regelungen zur Informationssicherheit sowie die Rahmen- und Benutzungsordnung des Zentrums für Informations- und Medientechnologie (ZIMT) gleichermaßen.
Es gelten daher auch für die Mobile Arbeit u.a.:

- Die Rahmen- und Benutzungsordnung des Zentrums für Informations- und Medientechnologie (ZIMT)**:** https://www.uni-siegen.de/start/news/amtliche_mitteilungen/jahrgang_2013/81_2013_rahmen-_und_benutzungso_des_zimt.pdf
- Die Regelungen zur Informationssicherheit an der Universität Siegen, insbesondere:
  - Die Leitlinie zur Informationssicherheit https://www.uni-siegen.de/start/news/amtliche_mitteilungen/2011/25-2011_leitlinien_zur_informationssicherheit.pdf
  - Die Passwortrichtlinie der Universität Siegen: https://www.uni-siegen.de/it-sicherheit/richtlinien/downloads/passwordpolicy.pdf
  - Die Vorgaben im IT-Grundschutzkatalog für Anwender der Universität Siegen https://www.uni-siegen.de/it-sicherheit/richtlinien/downloads/it-grundschutzkatalog_anwender.pdf (Link nur intern erreichbar)

Bei technischen Fragen wenden Sie sich gerne an das ZIMT unter support@zimt.uni-siegen.de. Bei weiteren Fragen können Sie sich gerne an das Team der Stabsstelle Informationssicherheit unter ciso-team@uni-siegen.de wenden.

Mit freundlichen Grüßen,
die Informationssicherheitsbeauftragte der Universität Siegen