Deutsche Universität für Verwaltungswissenschaften Speyer

RZ

Informationen zur IT Sicherheit und Datenschutz, insbesondere bei mobiler Arbeit

Allgemeine Regelungen zur Handhabung von dienstlichen Daten außerhalb des Campus

- Denken Sie bitte daran: Bearbeiten Sie dienstliche Daten ausschließlich im häuslichen Bereich und nicht in der Öffentlichkeit (z.B. in einem Café oder der Bahn).
- Die Ihnen bereits bekannten Dienste zur Speicherung bzw. Verarbeitung dienstlicher Daten stehen Ihnen auch weiterhin zur Verfügung. Dazu zählen beispielsweise die Nextcloud oder Seafile etc.
- Die Nutzung von Videokonferenzdiensten sollte mit Bedacht erfolgen. Es sollten keine Personaldaten, Gesundheitsdaten oder Dienstgeheimnisse übermittelt werden. Grundsätzlich sollte BigBlueButton verwendet werden.
- Bitte schützen Sie dienstliche Daten gegen unbefugten Zugriff. Dazu zählen auch Personen, die mit Ihnen in häuslicher Gemeinschaft leben. Maßnahmen sind insbesondere:
    - Keinen Einblick auf den Bildschirm
    - Sperrung des Gerätes bei Nichtgebrauch
    - Sichere Verwahrung von Unterlagen
    - Keine Speicherung von Passwörtern
- Wir möchten Sie und die Universität vor dem Verlust von vertraulichen, dienstlichen Daten schützen. Aus diesem Grund werden Festplatten der durch das Rechenzentrum ausgegebenen Laptops zukünftig verschlüsselt. Achten Sie insbesondere darauf, Datenträger (z.B. USB-Sticks) nur verschlüsselt zu transportieren.
- Klären Sie bitte mit Ihrer*m Vorgesetzten, welche Akten ggf. im häuslichen Bereich bearbeitet werden müssen und dokumentieren Sie deren Mitnahme. Akten, die vertrauliche Daten enthalten, sollten nur dann mitgenommen werden, wenn dies aus Gründen der Arbeitsorganisation unter den gegenwärtigen Bedingungen unbedingt erforderlich ist.

Allgemeine Regelungen für dienstliche IT-Geräte

- Eine Nutzung öffentlicher WLAN-Netze (z.B. in Cafés) ist nicht gestattet.
- Zur Speicherung Ihrer Daten stehen Ihnen wie gewohnt die Cloudspeicher der Universität zur Verfügung. Sollten diese aus technischen Gründen einmal nicht erreichbar sein, denken Sie bitte daran, lokal bearbeitete Daten umgehend auf den Campuslaufwerken abzulegen, sobald diese wieder verfügbar sind. Nur so sind Ihre Daten gegen einen Datenverlust gesichert.
- Verwenden Sie für dienstliche E-Mail-Kommunikation bitte ausschließlich die E-Mail-Adresse der Universität. Aus rechtlichen Gründen ist eine permanente Weiterleitung von dienstlichen E-Mails an private Anbieter wie Gmail, GMX, web.de etc. nicht gestattet.
- Mitarbeiter des RZ prüfen die Geräte regelmäßig auf die Einhaltung der genannten Regelungen.

Stand: 11/2023

Regelungen für die Nutzung privater IT-Geräte

- Es gibt Daten, die z.B. durch gesetzliche oder vertragliche Anforderungen besonders gut geschützt werden müssen und daher einen hohen Schutzbedarf haben. Dazu zählen beispielsweise Studierendendaten, Personalaktendaten, Gesundheitsdaten oder bestimmte wissenschaftliche Daten. Bitte beachten Sie, dass private Geräte aus Gründen des Datenschutzes und der Informationssicherheit nicht für eine Verarbeitung von Daten mit hohem Schutzbedarf geeignet sind.

Mindestanforderungen an ein privates IT-Gerät

- Verwenden Sie bitte ein aktuelles Betriebssystem mit allen relevanten Sicherheitsupdates. (Dazu zählen z.B. Windows 10 und 11, MacOS High Sierra und Mojave sowie viele Linux-Varianten.)
- Ein aktueller Virenscanner (bspw. Windows Defender) schützt Sie gegen schädliche Software.
- Ebenso ist eine aktuelle Software-Firewall notwendig (ist z.B. bei Windows 10 bereits integriert).
- Ihr IT-Gerät wird durch ein ausreichend sicheres Passwort geschützt, dass nur Ihnen bekannt ist.
- Zur Bearbeitung dienstlicher E-Mails nutzen Sie bitte den Uni-Webmailer („OWA“).
- Dienstliche Daten sollten, soweit technisch möglich, ausschließlich auf den Cloudlaufwerken der Universität bearbeitet werden.
- Achten Sie bitte darauf, bei Beendigung der dienstlichen Nutzung des Privatgerätes alle dienstlichen Daten vollständig von diesem zu löschen.
- Die Erfüllung der Anforderungen ist auf Anfrage nachzuweisen.

Unterweisungen/Schulungen

- Zweimal im Jahr werden Schulungen zum Thema IT-Sicherheit angeboten, eine Teilnahme an beiden Veranstaltungen ist verpflichtend.
- Ein online zu absolvierender Test bestätigt den Lernerfolg der genannten Schulungen.

Schutzbedarfsfeststellung/Risikoanalyse

- Gemeinsam mit der/dem Vorgesetzten erörtern:
  1. Welche Tätigkeiten möchte ich während mobiler Arbeit erledigen?
  2. Welche Daten sind von diesen Tätigkeiten betroffen?
  3. Welche Risiken können entstehen, wenn diese Daten missbräuchlich verwendet werden?
- Grundlage: Schutzstufenkonzept für den Datenschutz Niedersachsen (Schutzstufen A – E, siehe folgende Matrix[1]).
  - Je höher der Schutzbedarf der zu bearbeitenden Daten eingestuft wird, desto höher sind die zu ergreifenden Datensicherheitsmaßnahmen (bspw. Datenträgerverschlüsselung).
  - Ab Schutzstufe D sollte die Bearbeitung im Rahmen von mobiler Arbeit kritisch hinterfragt werden.

[1] Stufenkonzept der Landesbeauftragten für den Datenschutz Niedersachsen, Beispiele der Leibniz Universität Hannover

Schutzstufe	Personenbezogene Daten,	Beispiele	Risiko/Schadpotential
A	die von den Betroffenen frei zugänglich gemacht wurden.	• Kontaktangaben • Tätigkeitsbereiche • Publikationen • Vorlesungsverzeichnis • Vorlesungsmaterialien / Skripte • Übungsmaterialen	gering
B	deren unsachgemäße Handhabung zwar keine besondere Beeinträchtigung erwarten lässt, die aber von den Betroffenen nicht frei zugänglich gemacht wurden.	• Dienstliche Daten der Beschäftigten, die die interne Organisation betreffen (Geschäftsverteilungsplan, interne E-Mail-Verteiler, Zuständigkeiten) • Tätigkeitsbezogene Angaben in Protokollen von hochschulöffentlichen Gremiensitzungen • Kontaktinformationen Dritter (Vertragspartner, Drittmittelgeber, Behörden und ähnlich verbundenen Einrichtungen)	gering
C	deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen könnte („Ansehen")	• Vertragsunterlagen (zu Dritten) • Rechnungen • Reise- und Lohnabrechnungen • Drittmittelverträge • Einzelne Klausuren und einzelne Prüfungsergebnisse	überschaubar
D	deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen könnte („Existenz").	• Personalunterlagen und Personalakteninhalte • Leistungsinformationen über Studierende (z.B.Prüfungsakte, Leistungsübersicht, Abschluss) • Daten besonderer Kategorien nach Art. 9 DSGVO	substantiell
E	deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen könnte.	Daten über Personen, die mögliche Opfer einer strafbaren Handlung sein können, Zeugenschutzprogramm	groß