- Alle Peripheriegeräte (auch ohne Netzzugriff) sowie sämtliches Zubehör müssen registriert und freigegeben werden. Zuständig hierfür ist der jeweilige IT-Manager der Einrichtung. Die Nutzung nicht freigegebener Geräte ist untersagt. Die Nutzung von privaten Peripheriegeräten und Zubehör ist untersagt. Dies gilt auch für USB Geräte sowie USB Sticks oder USB Festplatten.

5. Datenträger

- Mitarbeiter sind für die sichere, sachgerechte Nutzung und Lagerung der von ihnen genutzten Datenträger verantwortlich.
- Vor der Weitergabe eines Datenträgers ist sicherzustellen (z.B. durch vorheriges Entfernen der Daten, ohne Wiederherstellungsmöglichkeit), dass dieser nur die zur Weitergabe bestimmten Daten enthält.
- Jeder Mitarbeiter ist dafür verantwortlich, dass die von ihm weitergeleiteten Informationen nur an berechtigte Empfänger weitergegeben werden.
- Datenträger sind vor dem Versand grundsätzlich auf Viren zu prüfen. Der Versender des Datenträgers ist für die Virenfreiheit desselben verantwortlich.
- Alle elektronischen Dokumente, deren weitere Verarbeitung nicht gewünscht bzw. beabsichtigt ist, dürfen nur im PDF-Format mit Veränderungs- und ggf. Kopierschutz nach außen gegeben werden.

6. Passwörter

- Es gilt die Passwortrichtlinie des DLR in der gültigen Fassung.
- Ein Passwort sollte mindestens 10 Zeichen lang und nicht leicht zu erraten sein, aus Groß- und Kleinbuchstaben bestehen sowie mindestens eine Zahl bzw. ein Sonderzeichen enthalten.

7. Dienstreisen

- Bei der Dienstreise ins Ausland beachten Sie bitte das "Merkblatt für Dienstreisende ins Ausland"
- Melden Sie etwaige Kontrollen unmittelbar nach Ihrer Rückkehr dem IT-Sicherheitsbeauftragten des DLR sowie Ihrer Institutsleitung.

Ich habe die genannten IT-Sicherheitsmaßnahmen zur Kenntnis genommen.

Institut

SHRIYA HAZRA
Mitarbeiter Name

Shriya
Datum / Unterschrift