Universität Marburg

Richtlinie zur Informationssicherheit auf Auslandsdienstreisen

Inhaltsverzeichnis

1 Ziele 2

2 Geltungsbereich 2

3 Allgemeine Regelungen 2

3.1 Maßnahmen vor Dienstreiseantritt 2

3.2 Besondere Bedingungen einzelner Reiseziele 2

4 Datensparsamkeit und Umgang mit Daten 3

5 Mitnahme von IT-Geräten 3

5.1 Gerätesperre 3

5.2 Verschlüsselung 3

5.3 Diebstahlsicherung 3

5.4 Sichtschutz 3

5.5 Mobile Datenträger 4

5.6 Klimatische Bedingungen 4

5.7 Prüfung nach der Dienstreise 4

6 Kommunikationsverbindungen 4

7 Verlustmeldung 4

1 Ziele

Um die Vertraulichkeit, Integrität und Verfügbarkeit der an der Philipps-Universität verarbeiteten Informationen zu gewährleisten, müssen bei Auslandsdienstreisen mitgeführte IT-Geräte und Datenträger angemessen geschützt werden. Diese Richtlinie definiert als Bestandteil des Informationssicherheitsmanagementsystems der Philipps-Universität Maßnahmen zum Schutz von Informationen auf Auslandsdienstreisen. Sie wurde auf Grundlage des IT-Grundschutzbausteins CON.7 ‚Informationssicherheit auf Auslandsdienstreisen' des Bundesamtes für Sicherheit in der Informationstechnik erstellt.

2 Geltungsbereich

Diese Richtlinie gilt für alle Beschäftigten der Philipps-Universität Marburg, die Auslandsdienstreisen durchführen und hierbei dienstliche IT-Geräte sowie Unterlagen mitführen.

3 Allgemeine Regelungen

Unabhängig von den Regelungen dieser Richtlinie müssen die vom Dezernat II festgelegten Regelungen zur Organisation von Dienstreisen[1] eingehalten werden. Weiterhin gelten auch bei Auslandsdienstreisen die Regelungen der Ordnung der Philipps-Universität für die Nutzung und den Betrieb der Informationstechnologie[2] und, sofern Sie das von Ihnen genutzte IT-Gerät selbst administrieren, die Richtlinie zur Administration von IT-Systemen und IT-Diensten im Netzwerk der Philipps-Universität[3].

3.1 Maßnahmen vor Dienstreiseantritt

Vor Reiseantritt sollten Sie prüfen, welche Daten während der Reise nicht unbedingt auf den IT-Systemen wie dem Notebook, Tablet oder Smartphone gebraucht werden. Ist es nicht notwendig, diese Daten auf den Geräten zu lassen, sollten diese gelöscht werden. Ist es nötig, dienstliche Daten mit auf die Reise zu nehmen, sollte dies nur in verschlüsselter Form erfolgen. Nutzen Sie alternativ für Daten mit einem normalen oder hohen Schutzbedarf[4] die Hessenbox mit einer VPN-Verbindung, um sicher auf Ihre Daten zuzugreifen. Achten sie dabei darauf, dass die Synchronisation über den Hessenbox-Client mit Ihrem mobilen Endgerät ausgeschaltet ist. Installieren Sie außerdem, sofern Sie Ihr IT-Gerät selbst administrieren, alle ausstehenden Updates für das Betriebssystem sowie für die auf dem IT-Gerät installierten Anwendungen. Führen Sie eine Datensicherung Ihres IT-Gerätes durch.

3.2 Besondere Bedingungen einzelner Reiseziele

Einzelne Reiseziele unterliegen besonderen gesetzlichen Regelungen des jeweiligen Reiselandes z. B. zur Benutzung von Verschlüsselungssoftware und VPN oder haben besondere Einreisebestimmungen zur Herausgabe von Geräten und/oder Passwörtern (bei der Ein- bzw. Ausreise). Der Dienstreisende informiert sich vor Beginn der Dienstreise auf den Webseiten des Auswärtigen Amts über die gesetzlichen Anforderungen des jeweiligen Reiseziels. Sofern im Zielland zu erwarten ist, dass besondere gesetzliche Regelungen gelten, darf der Dienstreisende keine regulär genutzten Dienstgeräte mitführen, sondern muss ausschließlich separate, gesicherte IT-Geräte (Laptops und

1 Siehe https://www.uni-marburg.de/de/universitaet/administration/verwaltung/dezernat2/dienstleistungen/allgemeine-informationen/dienstreisen.
2 Siehe https://www.uni-marburg.de/de/hrz/ueber-uns/it-management/it-nutzungsordnung
3 Siehe https://www.uni-marburg.de/de/universitaet/administration/recht/satzung/rl_2023-01-06_it_administration.pdf.
4 Entsprechend der unter https://hessenbox.uni-marburg.de/tos einsehbaren Nutzungsbedingungen.

Smartphones) mitführen, die über die IT-Administration der Fachbereiche und Einrichtungen in Zusammenarbeit mit dem Hochschulrechenzentrum zur Verfügung gestellt werden. Die Anfrage und Ausgabe dieser Geräte erfolgt über die IT-Administration der Fachbereiche und Einrichtungen[5].

4 Datensparsamkeit und Umgang mit Daten

Es sollten so wenige Daten wie möglich auf einem mitgeführten IT-Gerät gespeichert sein und bevorzugt über eine VPN-Verbindung auf Daten beispielsweise in der Hessenbox oder auf Netzlaufwerken des Hochschulrechenzentrums zugegriffen werden. Das Gebot der Datensparsamkeit gilt analog für Daten, die auf Papier oder auf andere Weise mitgeführt werden.

Dokumente, Datenträger und Geräte dürfen im Ausland nicht entsorgt werden, um keine Kenntnisnahme Dritter zu ermöglichen. Sie sind bis zur Rückkehr aufzubewahren, um sie anschließend angemessen zu vernichten.

Im Ausland ist eine besondere Aufmerksamkeit erforderlich. Mit Nichtbefugten darf nicht über dienstliche Daten, den Zweck der Reise und/oder den Arbeitgeber bzw. die Dienststelle gesprochen werden. Grundsätzliche und allgemeine Informationen hierzu dürfen im Zuge der Einreisemodalitäten genannt werden.

5 Mitnahme von IT-Geräten

5.1 Gerätesperre

Die auf allen IT-Geräten verfügbare Bildschirm-/Passwort-Sperre muss genutzt werden. Das IT-Gerät muss unmittelbar nach der Benutzung aktiv gesperrt werden und darf nur nach Eingabe eines Passwortes wieder benutzbar sein. Darüber hinaus ist besonders auf die Geheimhaltung des Passwortes zu achten. Bei Verdacht der Ausspähung des Passwortes muss dieses unverzüglich geändert werden.

Auf mitgeführten IT-Geräten muss sich nach maximal 15 Minuten der Inaktivitat eine automatische Bildschirmsperre aktivieren. Diese darf durch die nutzende Person nicht deaktiviert werden.

5.2 Verschlüsselung

Alle IT-Geräte und mobile digitale Datenträger (bspw. USB-Sticks oder Festplatten), die im Rahmen einer Auslandsdienstreise verwendet werden, müssen verschlüsselt werden. Der oder die Informationssicherheitsbeauftragte kann Dienstreisende über die Möglichkeiten von Verschlüsselungen beraten und ggf. Auskunft über die landesspezifischen Regelungen des Ziellandes geben. Grundsätzlich sollten dabei etablierte Verschlüsselungsverfahren wie PKI, Bitlocker und ähnliche Verschlüsselungsmethoden zum Einsatz kommen.

5.3 Diebstahlsicherung

IT-Geräte sollen dürfen während der gesamten Dienstreise nicht unbeaufsichtigt bleiben und müssen jederzeit vor Diebstahl und Manipulation geschützt werden. Ungenutzte IT-Geräte müssen ausgeschaltet und dürfen nicht im Stand-by oder Ruhemodus belassen werden. Bei Flugreisen dürfen IT-Geräte nicht als Fluggepäck aufgegeben werden, sondern sind direkt von der/dem Reisenden (als Handgepäck) mitzuführen.

Die/der Dienstreisende sollte, je nach IT-System, eine Diebstahl-Sicherung mitführen und diese bei Bedarf nutzen.

5.4 Sichtschutz

Um den unerwünschten Einblick in die am Bildschirm angezeigten Inhalte, insbesondere in öffentlichen Räumen, zu erschweren, müssen alle Dienstreisenden Sichtschutzfolien für alle eingesetzten

5 Siehe https://www.uni-marburg.de/de/hrz/hilfe-beratung/anlaufstellen/admins-der-fachbereiche-und-einrichtungen

IT-Geräte (Notebook, Tablet und Smartphone) verwenden. Die Sichtschutzfolien können in Zusammenarbeit mit den IT-Administrationen der Fachbereiche und Einrichtungen oder dem Hochschulrechenzentrum beschafft werden. Die Beschaffung erfolgt als Einzelverfahren und hängt von den Gegebenheiten des Fachbereichs bzw. der Einrichtung ab.

5.5 Mobile Datenträger

Die auf der Dienstreise nicht benötigten Daten auf mobilen Datenträgern müssen vor der Dienstreise sicher (durch Überschreiben) gelöscht werden. Die Datenträger müssen vor Benutzung auf Schadsoftware geprüft werden. Nach ihrer Benutzung müssen die Datenträger ebenfalls durch Überschreiben gelöscht werden. Hierbei kann die IT-Administration der Fachbereiche und Einrichtungen oder das Hochschulrechenzentrum unterstützen.

Mobile Datenträger (wie z. B. USB-Sticks, Powerbanks, Mäuse oder Tastaturen), die Dienstreisende als Geschenke erhalten, dürfen nicht an die dienstliche Hardware angeschlossen werden.

5.6 Klimatische Bedingungen

Die/Der Dienstreisende sollte sich vor Antritt der Dienstreise über die klimatischen Bedingungen am Zielort zu informieren und für die mitgeführten IT-Geräte entsprechende Schutzmaßnahme treffen. Es ist z. B. darauf zu achten, dass sich verschiedene IT-Geräte bei einer Überhitzung automatisiert abschalten und dann vorübergehend nicht zur Verfügung stehen.

5.7 Prüfung nach der Dienstreise

Nach Beendigung der Dienstreise müssen die oder der Dienstreisende, wenn während der Reise die Möglichkeit zur Manipulation am Gerät bestand, ihre mitgenommenen IT-Geräte visuell auf physische Unversehrtheit (z. B. ob Schrauben geöffnet oder Siegel entfernt wurden) und auf Virenbefall (Scan durch eine Software zum Endgeräteschutz) prüfen. Bei Auffälligkeiten muss die oder der Datenschutzbeauftragte sowie die oder der Informationssicherheitsbeauftragte informiert werden. Das Gerät darf bei Verdacht auf Manipulation nicht wieder genutzt werden.

6 Kommunikationsverbindungen

Nutzen Sie für Zugriffe auf öffentlich zugängliche Dienste der Philipps-Universität sowie das universitäre Netzwerk ausschließlich verschlüsselte Zugriffswege via VPN. Nutzen Sie auf Auslandsdienstreisen ausschließlich die VPN-Gruppe ‚unimr-vpn-staff-ft-Passwort+2FA‘.

Für die Benutzung öffentlicher WLANs z. B. in Hotels gelten die folgenden Regelungen:

- Schalten Sie die WLAN-Funktion Ihres Gerätes nur ein, wenn Sie diese wirklich benötigen.
- Vermeiden Sie, vertrauliche Daten unverschlüsselt über ein fremdes WLAN-Netzwerk abzurufen. Nutzen Sie hierfür immer VPN oder SSL-gesicherte Verbindungen.
- Achten Sie beim Zugriff auf Webseiten auf gesicherte HTTPS-Verbindungen.
- Deaktivieren Sie Dienste, die einen Zugriff auf Ihr IT-Gerät erlauben wie beispielsweise Laufwerk-, Druck-, Datei- oder Verzeichnisfreigaben, Remote Desktop (RDP) oder SSH.

7 Verlustmeldung

Bei Verlust eines IT-Gerätes oder von Daten oder dem Verdacht der Ausspähung von Kennworten oder PINs im Ausland informiert die/der Dienstreisende unverzüglich die Stabsstelle Informationssicherheit telefonisch unter der Rufnummer +49 6421 2828281 oder per E-Mail an it-sicherheit@uni-marburg.de.

Wenn ein verschwundenes IT-Gerät wieder auftaucht, sollte es während der Dienstreise nicht wieder in Betrieb genommen werden und nach Rückkehr auf eventuelle Manipulationen untersucht werden, z. B. ob Schrauben geöffnet oder Siegel entfernt wurden. Das Gerät ist bei Verdacht auf Manipulation nicht wieder in Betrieb zu nehmen und auszutauschen.

Ein Diebstahl von IT-Geräten muss unverzüglich über das Formular unter https://www.uni-marburg.de/de/universitaet/administration/verwaltung/stabsstellen/recht/dokumente/anzeige-diebstahl-einbruch-schaden-2022.pdf der Stabsstelle Recht gemeldet werden.

Die Richtlinie zur Informationssicherheit auf Auslandsdienstreisen wurde am 08.10.2024 vom Präsidium der Philipps-Universität beschlossen und tritt mit Veröffentlichung in den Amtlichen Mitteilungen in Kraft.