Christian.paulsen@vw.hcu-hamburg.de
InSiBe und DSB
040 428 27 4359

HafenCity Universität Hamburg

HCU-Richtlinie
„Informationsschutz auf Reisen“

Autor: Christian Paulsen (InSiBe / DSB) Stand: 21.07.2020

Version: 1.1

Vertraulichkeit: Öffentlich

1 Einleitung

Die Bedeutung berufsbedingt oder forschungsbedingt notwendiger Reisetätigkeiten hat in den letzten Jahren durch die Globalisierung und die dadurch zunehmende internationale Vernetzung von Hochschulen, Behörden und Unternehmen stetig zugenommen. Um auch außerhalb des regulären Arbeitsumfeldes arbeiten zu können, ist es zumeist unabdingbar geworden, neben Unterlagen in Papierform auch Informationstechnik mitzuführen, sei es z. B. Notebook, Smartphone, Tablet, Wechselfestplatte oder USB-Stick. Bei allen Reisen, vor allem bei Auslandsreisen, ist eine Vielzahl an Bedrohungen und Risiken für die Informationssicherheit zu beachten, die im normalen Geschäftsbetrieb nicht existiert:

- Abhören und Ausspähen von Informationen/Wirtschaftsspionage
- Offenlegung und Missbrauch schützenswerter Informationen
- Unbemerkter Zugriff auf mobile Endgeräte
- Verstoß gegen lokale Gesetze und Regelungen
- Nötigung, Erpressung
- Diebstahl und Verlust von Dokumenten und Datenträgern

Das Ziel dieser Richtlinie ist daher der Schutz aller Informationen, die auf Auslandsreisen sowohl in elektronischer als auch physischer Form mitgeführt werden, in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit. Bitte beachten Sie dazu auch die gültige HCU-IT-Benutzungsordnung.

2 Empfehlungen zur Reisevorbereitung

- Vertrauliche oder sensible Unterlagen gehören möglichst nicht ins Reisegepäck.
- So wenig technische Geräte mitnehmen wie möglich – damit Sie den Überblick behalten!
- Falls möglich Reise-Laptops nutzen – ausschließlich mit Daten, die Sie für die Reise benötigen!
- Geschäftliches von Privatem trennen! Auf private Geräte gehört nichts Geschäftliches – und umgekehrt
- Es gibt Länder, die eine Entschlüsselung bei der Einreisekontrolle verlangen können (z. B. USA) oder wo eine Einfuhr von Verschlüsselungssoftware – auch auf Datenträgern – generell verboten ist (z. B. China, Russland). Bitte erkundigen Sie sich vor der Reise diesbezüglich über die individuellen Einreisebestimmungen des jeweiligen Landes.

3 Ausstattung und Verschlüsselung

Die folgenden Empfehlungen zur Ausstattung und Verschlüsselung Ihrer IT-Geräte gilt sowohl für ihre selbstadministrierten Geräte als auch für IT-Systeme, die von der HCU-IT verwaltet werden.

- Notebooks vor Reiseantritt immer mit der aktuellen Version eines Virenschutzprogramms ausstatten! Alle Programm-Updates vor Reisebeginn installieren!
- Mitgeführte Laptops (unter Beachtung der Einreisebestimmungen bei Auslandsreisen) unter Beachtung der HCU-Richtlinie „Mobiles Arbeiten und Homeoffice“ verschlüsseln, um Daten bei Verlust der Hardware zu schützen!
- Smartphones ebenfalls (unter Beachtung der Einreisebestimmungen und unter Beachtung der HCU-Richtlinie „Mobiles Arbeiten und Homeoffice“) verschlüsseln, sperren und die Option der Fernlöschung einstellen!
- Zum Schutz vor Diebstahl: Nutzen Sie mechanische Diebstahlsicherungen (können in der Geräteausgabe zur Verfügung gestellt werden)!

4 Sicherer Umgang mit IT-Geräten auf Reisen

- Bluetooth und W-LAN bei Nichtgebrauch abschalten (Einfallswege von Hackern)!
- Zum Schutz vor fremdem Zugriff und Diebstahl: vor dem Verlassen des Laptops die Bildschirmsperre aktivieren bzw. den Rechner ausschalten, eine Diebstahlsicherung verwenden oder die Geräte nicht unbeaufsichtigt lassen!
- Öffentliche W-LAN-Netze nur im Notfall nutzen!
- Wenn immer möglich, Internet und E-Mail über eine VPN-Verbindung nutzen!
- Auf Reisen niemals vertrauliche Details und Unterlagen per E-Mail versenden!
- Grundsätzlich besteht auf Reisen ein höheres Risiko, dass eine Korrespondenz (wie auch immer geführt: E-Mail, Firmen-Plattformen, Soziale Netzwerke, Business Netzwerke wie Xing und LinkedIn usw.) von Dritten mitgelesen werden kann.
- Weder auf Reisen noch nach der Rückkehr USB-Sticks oder ähnliche externe Speichermedien nutzen, die Ihnen Dritte/Fremde angeboten haben!
- Achten Sie darauf, dass auf Ihren elektronischen Endgeräten (Smartphone, Tablet, Notebook) im Ausland keine kritischen (anzügliche, pornografische, religiöse, politische) Inhalte in Form von Texten oder Bildern vorhanden sind. Dies kann Ihnen u. U. erhebliche Probleme bereiten und/oder auch zur Konfiszierung der Geräte führen!

5 Verhalten im öffentlichen Raum

- Keine geschäftlichen Gespräche, ob per Telefon oder persönlich, im öffentlichen Raum führen – selbst vermeintlich Belangloses kann schädigend sein.
- Unterlagen nie offen liegenlassen! Bereits ein Titel kann zu viel offenbaren.
- Unterlagen/Laptops/Taschen etc. nie unbeaufsichtigt zurücklassen! Auch nicht für den kurzen Moment, wenn Sie bspw. für ein persönliches kurzes Gespräch aus dem Raum gebeten werden.
- Nicht mehr benötigte sensible Unterlagen so vernichten, dass Informationen nicht mehr zu erkennen sind.
- Das Hotelzimmer ist kein privater Raum: Unterlagen und elektronische Geräte nicht unbeaufsichtigt im Hotelzimmer lassen!
- Zimmer-/Hotelsafe an der Rezeption bieten keinen echten Schutz – Angestellte haben die Möglichkeit, mit einem Generalschlüssel oder -code Zugang zu erlangen.

- Vertrauliche und sensible Gespräche nicht im Hotelzimmer führen: weder persönlich Face-to-Face noch über Mobiltelefon/Hoteltelefon. In manchen Ländern werden versteckte Aufzeichnungen von allen Aktivitäten in Hotelzimmern angefertigt.

6 Nach der Reise

- Elektronische Endgeräte nach der Reise auf Unversehrtheit prüfen
- Bei auffälligen Vorkommnissen die Vorgesetzten / Informationssicherheitsbeauftragten informieren
- Den Verlust von Informationen, IT-Systemen oder Datenträgern zeitnah dem Vorgesetzten, der HCU-IT und dem Datenschutzbeauftragten melden