

Sicherheitsrichtlinien für den mobilen Arbeitsplatz

Die Zielgruppe dieses Dokuments sind Mitarbeiter der Hochschule Harz mit einem mobilen und wechselnden Arbeitsplatz. In solchen Umgebungen kann nicht die infrastrukturelle Sicherheit der Hochschule Harz vorausgesetzt werden. Daher sind Sicherheitsmaßnahmen zu ergreifen, mit denen sich eine vergleichbare Sicherheitssituation erreichen lässt.

herausgegeben vom Rechenzentrum Hochschule Harz
Erreichbar unter E-Mail: rz@hs-harz.de
 Tel.: 03943 / 659-919
Version IT-Grundschutzkonzeption „Sicherheitsrichtlinie mobiler Arbeitsplatz“; Version 1.0
 vom 02.11.2008

Regelungen bei der Mitnahme von IT-Geräte

Außerhalb der Hochschulinfrastruktur sind die Nutzer verantwortlich für die mobile IT. Auf die zu ergreifenden Vorsichtsmaßnahmen wird hingewiesen:

- IT-Geräte müssen stets sicher aufbewahrt werden.
- Mobile IT-Geräte sollten nicht unbeaufsichtigt bleiben bzw. das IT-Gerät sollte von außen nicht sichtbar sein sofern es zurückgelassen werden muss, z.B. Verschießen im Schrank. Alle Passwort- oder PIN-mechanismen sollten jetzt aktiviert sein. Insbesondere sollten sie nicht in Fahrzeugen zurückgelassen werden.
- IT-Geräte und deren Anwendungen sollten durch Passwörter oder PINs abgesichert werden.
- Sensitive Daten auf den IT-Systemen sollten möglichst komplett verschlüsselt werden.

Nutzung eines mobilen Arbeitsplatzes

Jeder Nutzer eines mobilen Arbeitsplatzes ist angehalten zu prüfen, ob die jeweilige Umgebung als Arbeitsplatz genutzt werden kann. Aspekte die hierbei beachtet werden sollten sind:

- Es ist ein stabiler Arbeitsplatz vorhanden.
- Die Umgebung ist nicht zu laut.
- Die Umgebung ist ausreichend beleuchtet.
- Die IT-Geräte können so aufgestellt werden, dass Dritte keine Einsicht haben.
- Es sind eine Stromversorgung und eine Netzwerkanbindung vorhanden.
- Die Umgebung hat notwendige Bedingungen, um vor Diebstahl zu schützen, z.B. so sollten nach Möglichkeit Fenster und Türen bei Verlassen des Raumes geschlossen werden.
- Die Sicherheitsregelungen der besuchten Organisation oder Einrichtung müssen beachtet werden.

Sicherheitsregelungen zum Schutz der Informationen

- Vertrauliche Informationen dürfen unterwegs nicht mit fremden Personen ausgetauscht werden. Es dürfen vertrauliche Informationen auch nicht in Hör- oder Sichtweite von Dritten diskutiert oder weitergegeben werden.
- Mitarbeiter sind verpflichtet sich über die Sicherheitslage und Gesetze des Reiselandes zu informieren.
- Auf Reisen sollten keine sensiblen Informationen mitgeführt werden. Falls doch sensitive Informationen mitgenommen werden müssen, sind diese im Handgepäck mitzuführen.
- Sensible Informationen nicht unbeaufsichtigt liegen lassen.
- Für die Kommunikation mit Institutionen und Partnern nur gesicherte Verbindungen nutzen. Vorsicht auch bei fremden Faxanschlüssen, da zu übertragene Dokumente gespeichert und später ausgedruckt werden können.
- Die Entsorgung von Datenträgern und Dokumenten unterwegs ist wenn möglich zu vermeiden. Auch Akten- und Datenvernichter in fremden Organisationen sind zu meiden, da hier nicht ersichtlich ist wie und wer die Entsorgung durchführt.

Bei Nutzung eines mobilen Datendienstes, wie UMTS oder HDSPA im Ausland, melden Sie sich bitte 14 Tage vor Antritt der Reise im Rechenzentrum