Anhang

Merkblatt IT-Sicherheit und Datenschutz

Beim mobilen Arbeiten ist ein verantwortungsvoller Umgang der Mitarbeitenden mit dienstlichen und personenbezogenen Daten besonders wichtig. Bei der Verarbeitung dieser Daten, müssen die Anforderungen des Datenschutzes und der IT-Sicherheit beachtet und eingehalten werden. Um das zu gewährleisten, enthält dieses Merkblatt verpflichtende Regelungen, die beim mobilen Arbeiten eingehalten werden müssen. Das Merkblatt konkretisiert die Anforderungen aus der Dienstvereinbarung zum Mobilen Arbeiten.

Aufgaben, bei denen die Sicherheit der Daten beim mobilen Arbeiten nicht gewährleistet werden kann, müssen in der Dienststelle erledigt werden.

Arbeiten mit dienstlichen Daten und Geräten

Die dienstlichen Daten, mit denen Sie täglich arbeiten, sind wichtig und schützenswert. Nehmen Sie deshalb nur Daten aus der Dienststelle mit in Ihren mobilen Arbeitsplatz, die Sie unbedingt benötigen. Mit vertraulichen oder sehr sensiblen Daten sollten Sie ausschließlich in der Dienststelle arbeiten.

Bitte stellen Sie sicher, dass:

- Sie Ihre dienstlichen Daten schützen, indem Sie andere Personen nicht auf Ihren Bildschirm schauen lassen, Sie Ihr dienstliches Gerät sperren, wenn Sie es (auch kurzzeitig) nicht benutzen und Sie Ihre dienstlichen Unterlagen sicher und verschlossen aufbewahren. Dies gilt sowohl zu Hause, als auch unterwegs. Verwenden Sie zum Beispiel Sichtschutzfolien um unbefugte Einblicke auf Ihren Monitor zu verhindern,
- Sie Ihre Daten möglichst auf Ihrem Netzlaufwerk und nicht lokal speichern,
- Sie für den Austausch von Daten die Dienste der Universität nutzen,
- Sie keine dienstlichen Dokumente auf privaten Druckern ausdrucken, sondern Ihre Druckaufträge an Drucker in der Dienststelle senden,
- Sie vertrauliche Unterlagen nicht über den Hausmüll oder unterwegs entsorgen, sondern datenschutzgerecht in der Dienststelle,
- andere Personen nicht Ihre dienstlichen Geräte verwenden,
- Sie Ihre dienstlichen Unterlagen nicht offen herumliegen lassen,
- Sie nicht mit Ihren privaten Geräten arbeiten, auch nicht über VPN,
- Sie keine dienstlichen Daten auf privaten Speichermedien wie USB-Sticks oder SD-Karten speichern,
- Sie private und dienstliche Unterlagen nicht vermischen, sondern getrennt aufbewahren,
- Sie Ihren mobilen Arbeitsplatz sichern, sobald Sie ihn verlassen (etwa in einem Hotelzimmer durch Schließen von Fenster und Türen).

Dienstliche Daten und Geräte transportieren

Schriftliche Notizen und Papierunterlagen müssen verschlossen transportiert und weggeschlossen werden, wenn Sie sie nicht verwenden. Lassen Sie Ihre Unterlagen und Geräte niemals unbeaufsichtigt. Melden Sie der Ihnen vorgesetzten Person umgehend den Verlust von Unterlagen oder Geräten.

Mit dem Uninetz und dem Internet verbinden

Nutzen Sie bitte vor allem bei öffentlichen WLANs wie in Zügen, Hotels oder Cafés eine VPN-Verbindung. Wenn Sie einen mit Opsi verwalteten Rechner verwenden, ist der VPN-Client AnyConnect bereits auf Ihrem Gerät installiert. Eine Anleitung zu VPN mit AnyConnect finden Sie auf den Webseiten des Hochschulrechenzentrums.

Bitte stellen Sie, wenn Sie von zu Hause aus arbeiten sicher, dass:

- Sie möglichst eine kabelgebundene LAN-Verbindung ins Internet nutzen,
- Sie die voreingestellten Zugangsdaten für das WLAN Ihres Routers sowie das Routerpasswort auf ein individuelles, mindestens 12-stelliges Passwort ändern (Hinweise zu starken Passwörtern finden Sie in der Passwortrichtlinie der UMR),
- für die Verschlüsselung des WLANs an Ihrem Router mindestens WPA2 eingestellt ist.

Dienstliche Geräte schützen

Installieren Sie auf Ihren Geräten Software-Patches für das Betriebssystem und die von Ihnen genutzten Programme so schnell wie möglich. Halten Sie Ihr Antivirenprogramm immer auf dem aktuellsten Stand. Nutzen Sie für Ihre tägliche Arbeit einen Benutzungs-Account ohne administrative Rechte. Nutzen Sie möglichst einen vom Hochschulrechenzentrum zentral gemanagten Rechner (Opsi).

Telefonieren und Besprechen

Auch bei Telefonaten und Webkonferenzen müssen Sie darauf achten, dass Unbefugte sensible Inhalte nicht mithören können. Insbesondere vertrauliche Inhalte sollten nicht in der Anwesenheit anderer Personen besprochen werden. Bitte

- nutzen Sie soweit möglich Telefonkonferenzen,
- nutzen Sie für Webkonferenzen die von der Philipps-Universität bereitgestellten Dienste,
- beachten Sie die Regelungen zur Nutzung von Webkonferenzen sowie die allgemeinen Hinweise zum Datenschutz,
- achten Sie darauf, ohne ausdrückliche Erlaubnis keine personenbezogenen Daten von anderen Personen preiszugeben, wenn Sie von Externen zu einer Webkonferenz eingeladen werden,
- nutzen Sie für E-Mail-Kommunikation ausschließlich Ihre dienstliche Adresse. Sie dürfen dienstliche E-Mails nicht an Ihre private E-Mail-Adresse (bei Google, GMX etc.) weiterleiten.

Bitte wenden Sie sich bei Fragen an

Informationssicherheitsbeauftragter: it-sicherheit@uni-marburg.de

Datenschutzbeauftragter: datenschutz@uni-marburg.de

Technischer Support: helpdesk@hrz.uni-marburg.de