JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN

# Empfehlungen für die Nutzung von dienstlichen Smartphones und Tablets an der JLU Gießen

Herausgeber: Dr. Matthias Stenke, IT-Sicherheitsbeauftragter der JLU

Dieses Informationsblatt enthält Empfehlungen für alle Personen an der JLU, die dienstliche Smartphones und Tablets einsetzen. Es soll zur Sensibilisierung gegenüber potenziellen Risiken beitragen und die Nutzerinnen und Nutzer mit entsprechenden Handlungsempfehlungen unterstützen. Die hier gegebenen Empfehlungen gelten sinngemäß auch für dienstlich genutzte Privatgeräte, wenn diese mit Diensten der Universität wie z.B. E-Mail verbunden werden.

## Einleitung

Smartphones und Tablets sind mobile Endgeräte mit zahlreichen Zusatzfunktionen und einer Vielzahl eingebauter Sensoren bis hin zur genauen Positionsbestimmung per GPS. Nutzerinnen und Nutzer können mit Smartphones nicht nur telefonieren, sondern auch im Internet surfen sowie Medien wie Audio, Fotos und Videos wiedergeben und aufnehmen. Mit den Geräten lassen sich E-Mails bearbeiten und Terminkalender und Adressbücher mit den E-Mail-Servern der JLU Gießen synchronisieren. Bei vielen Geräten sind bereits im Auslieferungszustand Clients für soziale Netzwerke und Blogdienste sowie Navigation integriert. Darüber hinaus kann der Funktionsumfang mithilfe von Apps nahezu unbegrenzt erweitert werden.

Durch die aufgrund der vielfältigen Funktionen auf Smartphones und Tablets automatisch erfassten und gespeicherten Daten sind diese Geräte höchst attraktive Angriffsziele. Risiken gehen auch von Apps auf den Geräten aus, die auf dem Gerät gespeicherte Daten oder Positionsdaten ungewollt an Dritte übertragen.

## Empfehlungen

Bitte beachten Sie die folgenden Empfehlungen bei der Einrichtung und Nutzung Ihres Smartphones oder Tablets, um die mit der Nutzung verbundenen Risiken zu verringern.

### Nehmen Sie grundlegende Sicherheitseinstellungen vor und schützen Sie das Gerät gegen unbefugten Zugriff

- **Automatische Sperre:** Richten Sie eine automatische Bildschirmsperre per PIN, Muster oder mit biometrischen Verfahren wie Fingerabdruck ein. Achten Sie darauf, dass diese stets aktiviert ist. Ob PIN oder Muster: Sorgen Sie für einen Sichtschutz bei der Eingabe, damit niemand Ihre Kombination ausspähen kann. Reinigen Sie regelmäßig das Display, um Wisch- und Berührungsspuren zu beseitigen, mit denen die Kombination erraten werden könnte.
- **Geräteverschlüsselung:** Um die auf dem Gerät gespeicherten Daten zu schützen, sollten Apps mit Zugriff auf dienstliche Daten wie z.B. E-Mail nur bei aktiver Geräteverschlüsselung verwendet werden. Bei Apple IOS ist die Verschlüsselung standardmäßig aktiv, bei Android-Geräten muss diese ggfs. in den Einstellungen aktiviert werden.
- **Schnittstellen:** Deaktivieren Sie Drahtlosschnittstellen wie Bluetooth, WLAN oder NFC, wenn Sie diese nicht benötigen. Für die USB-Schnittstelle gilt: schließen Sie Ihr Gerät nur an vertrauenswürdige Rechner an, denn auch auf diesem Weg kann Schadsoftware übertragen werden oder es können auf dem Gerät gespeicherte Daten abgezogen werden.
- **Zugriffschutz:** Halten Sie das Gerät stets sicher verwahrt und geben Sie es vor allem im entsperrten Zustand nicht unbeaufsichtigt an andere Personen weiter.

## Halten Sie das Gerät und die installierten Apps stets auf aktuellem Softwarestand und installieren Sie nur Apps aus vertrauenswürdigen Quellen

- **Betriebssystem aktuell halten:** Überprüfen Sie regelmäßig, ob vom Hersteller eine aktuellere Android- bzw. IOS-Version bereitgestellt wurde. Richten Sie Ihr Gerät am besten so ein, dass Ihnen das Vorliegen einer neuen Version automatisch gemeldet wird. Installieren Sie neue Versionen zeitnah, damit Sicherheitslücken möglichst rasch geschlossen werden.
- **Apps aktuell halten:** Auch die auf dem Gerät installierten Apps müssen aktuell gehalten werden. Richten Sie Ihr Gerät am besten so ein, dass Aktualisierungen von Apps automatisch aus Google Play (Android) bzw. dem App Store (IOS) heruntergeladen und installiert werden.
- **Einsatz veralteter Geräte vermeiden:** Seitens der Hersteller werden die Geräte nur für eine gewisse Zeit mit Aktualisierungen des Betriebssystems Android bzw. IOS versorgt. Wenn es für ein Gerät keine Aktualisierungen mehr gibt, werden neu entdeckte Sicherheitslücken nicht mehr geschlossen und das Risiko für ein Ausnutzen einer Sicherheitslücke steigt. Solch ein veraltetes Gerät sollte nicht mehr für dienstliche Zwecke eingesetzt werden, sondern durch ein neues Gerät ersetzt werden.
- Installieren Sie **Apps nur aus den offiziellen App Stores**: Google Play für Android und App Store für IOS.
- Nehmen Sie **kein Rooting** (Android) **oder Jailbreak** (IOS) des Geräts vor.

## Beachten Sie den Grundsatz der Datensparsamkeit

Wichtigster Grundsatz zur Vermeidung von Risiken ist die Datensparsamkeit. Daten, die nicht auf dem Gerät vorhanden sind, können bei einem unberechtigten Zugriff nicht in falsche Hände geraten.

- Speichern Sie möglichst wenige dienstliche Daten auf dem Gerät.
- Installieren und verwenden Sie **nur Apps, die für die dienstlichen Zwecke notwendig sind**. Apps mit privatem Charakter wie z.B. Spiele gehören nicht auf ein dienstliches Gerät.
- **Prüfen Sie** bei der Installation von Apps die **Nutzungsbedingungen** und die benötigten **Zugriffsberechtigungen**, insbesondere wenn eine App Zugriff auf die im Gerät gespeicherten Daten wie dem Adressbuch erfordert.
- **Bedenkliche Apps vermeiden**: Vermeiden Sie den Einsatz von Apps, die auf dem Gerät gespeicherte Daten auslesen und diese an externe Stellen oder in eine Cloud übertragen.
  **Dazu gehören:**
  - **WhatsApp** liest regelmäßig die Telefonnummern aus dem Adressbuch aus und überträgt diese an den Anbieter in USA. Hierfür ist eine Einwilligung **aller** Betroffenen erforderlich, die normalerweise nicht vorliegt.
  - Die **Outlook-App** überträgt Benutzerkennungen und Passwörter an fremde Server. Sie ist deshalb für den Zugriff auf die Exchange-Server der JLU gesperrt.
  - **Prüfen Sie Apps kritisch, die den Zugriff auf Ortungsdienste (GPS) verlangen**

  **Ausdrücklich gewarnt wird vor dem Einsatz der App WeChat** – hier fehlt es z.B. an einer Ende-zu-Ende Verschlüsselung und es muss angesichts der Hinweise in der Datenschutzrichtlinie von WeChat davon ausgegangen werden, dass chinesische Behörden Zugriff auf sämtliche Daten haben, die von WeChat erfasst oder übertragen werden.

- **Cloud-Dienste vermeiden:** Prüfen Sie vor dem Einsatz einer App genau, wo diese Daten speichert und wofür diese evtl. genutzt werden. Insbesondere bei kostenlosen Apps „zahlen“ Sie meist mit der Nutzung Ihrer Daten durch den Anbieter.

- Bedenken Sie, dass die **Spracherkennung der Geräte** („Hey, Siri“ oder „OK, Google“) die aufgenommene Sprache zur Analyse in die **Cloud des Herstellers** überträgt.
- **Backup in der Cloud vermeiden:** Insbesondere bei Android ist ein Backup des Geräts in der Google-Cloud unverschlüsselt. Nehmen Sie stattdessen ein Backup des Geräts möglichst mit einem vom Hersteller bereitgestellten Tool vor, das eine Speicherung der Daten auf einem JLU-internen System (z.B. PC, Fileserver) erlaubt.
- **Vorsicht an öffentlichen Hotspots:** Hier ist die Übertragung der Daten über das Netzwerk meist unverschlüsselt. Nutzen Sie hier nur verschlüsselte Übertragungen (https).

## Nutzung von JLU-Diensten mit dem Gerät

- Für den Zugriff auf E-Mail, Kalender und Adressbuch sollten Sie ein **Exchange E-Mail-Konto verwenden**. Hiermit werden grundlegende Sicherheitseinstellungen wie die Bildschirmsperre des Geräts umgesetzt und Sie haben bei einem Verlust die **Möglichkeit das Gerät aus der Ferne zu löschen.**
- Für den VPN-Zugriff ins Netz der JLU können Sie die **Cisco Anyconnect App** verwenden.
- Für die Speicherung und den Austausch von Dateien steht Ihnen die **JLUbox** zur Verfügung.

## Was tun bei Verlust?

Bei einem Verlust des Geräts nehmen Sie bitte folgende Schritte in dieser Reihenfolge vor:

- Falls Sie Ihr Exchange E-Mail-Konto auf dem Gerät eingerichtet haben, **löschen Sie möglichst zeitnah alle Daten auf dem Gerät aus der Ferne** mit Hilfe von Outlook Web Access https://owa.uni-giessen.de Nach der Anmeldung mit Ihrer Benutzerkennung und Passwort finden Sie unter „Einstellungen → Optionen → mobile Geräte“ eine Liste aller mobilen Geräte, die mit Ihrem E-Mail-Konto verbunden sind. Dort wählen Sie das verlorene Gerät aus und dann die Option „Alle Daten zurücksetzen“. Sofern das Gerät noch im Mobilfunknetz oder WLAN-Netz aktiv ist, wird es damit auf die Werkseinstellungen zurückgesetzt. **Vorsicht: Das Zurücksetzen kann nicht rückgängig gemacht werden!**
- Anschließend lassen Sie bitte ggfs. die **SIM-Karte** von der Nachrichtentechnik im HRZ **umgehend sperren**. Wenden Sie sich dazu telefonisch an Herrn Christian Bell (Tel. 13077) oder Frau Sigrun Merte (Tel. 13060) bzw. per E-Mail an nt@hrz.uni-giessen.de.
- **Melden Sie den Verlust** unter Mitteilung der näheren Verlustumstände **im Dezernat B**, Abteilung B2 bei Frau Katrin Amling (Tel. 12280), Herrn Mario Kahl (Tel. 12281) oder Frau Carolin Wurmb (Tel. 12282) bzw. per E-Mail an schadensfall@admin.uni-giessen.de

## Entsorgung

Am Ende der Nutzungsdauer setzen Sie das Gerät bitte sofern möglich auf **Werkseinstellungen** zurück. Defekte und ausgemusterte Geräte geben Sie bitte im HRZ-Shop zur datenschutzgerechten Entsorgung ab.

## Sie benötigen Unterstützung oder haben Fragen?

Unterstützung bei der Einrichtung Ihres Smartphones oder Tablets bekommen Sie

- an der Servicetheke im Hochschulrechenzentrum
- beim Helpdesk des Hochschulrechenzentrums telefonisch unter 0641 99-13050 oder per E-Mail an support@hrz.uni-giessen.de

Für weitergehende Fragen zur IT-Sicherheit steht Ihnen der IT-Sicherheitsbeauftrage der JLU telefonisch unter 0641 99-13050 oder per E-Mail an itsicherheit@uni-giessen.de gerne zur Verfügung.