Betriebsregelung/Nutzungsregelung Mobile Device Management MDM
In den zentralen Organisationseinheiten ZHV, ZMI, UB
Zum Umgang mit mobilen dienstlichen Geräten an der FernUniversität in Hagen
Gerätetypen: iPhone und iPad von Apple

Die Nutzung dienstlicher Smartphones und Tablets erfordert einige Maßnahmen, um die Betriebssicherheit sowie den Schutz sensibler und personenbezogener Daten zu gewährleisten. Nicht allen Risiken ist mit technischen Maßnahmen zu begegnen.
Bei der Nutzung der mobilen Geräte sowohl zur dienstlichen als auch zulässigen privaten Nutzung soll eine Vermischung dienstlicher und privater Daten möglichst verhindert werden. Ziel dieser Betriebsregelung ist es trotz dieser schwer zu vereinbarenden Rechtsbereiche ein hohes Niveau sowohl der Informationssicherheit und als auch des Datenschutzes zu gewährleisten.

Die nachfolgenden Regelungen definieren daher einen angemessenen Umgang mit den ausgegebenen dienstlichen Geräten.
Alle Personen im MDM Umfeld werden aufgefordert diese Anweisungen zu beachten. Bei auftretenden Schwierigkeiten in der praktischen Umsetzung sollte der Helpdesk im ZMI informiert werden.
Diese Betriebsregelung kann nach Erforderlichkeit bezüglich der Informationssicherheit und des Datenschutzschutzes mit Rücksicht auf die praktische Nutzbarkeit mobiler Geräte für den dienstlichen Gebrauch angepasst werden.

I. Installation/Inbetriebnahme

A. Konfiguration durch das Mobile Device Management (MDM)

Das MDM Team im ZMI liefert das mobile Gerät mit den vorinstallierten Konfigurationsprofilen und voreingerichteten Sicherheits- und Datenschutzeinstellungen aus. Dazu gehören u.a.:

- Einrichtung des WLAN Netzwerkes *eduroam* (Benutzerkennung);
- Voreinrichtung des Exchange-Kontos mit allen Funktionen;
- Voreinstellung des VPN-Netzwerks (VPN-Verbindung zu FernUni);
- Bereitstellung der notwendigen digitalen Zertifikate der FernUni, DFN, Telekom;
- Sichern und Wiederherstellen der Gerätekonfiguration und der Profile;
- Konfiguration des MobileIron *Mobile@Work* Clients;
- Bereitstellung von Apps über den Enterprise App Store *Apps@Work;*

Diese Voreinstellungen sind beizubehalten!

Insbesondere sind folgende Aktionen zu unterlassen:

- Löschung des Konfigurationsprofils oder der *Mobile@Work* App
- Rückübertragung der Backup Version eines anderen Gerätes oder einer alten Betriebssystemversion (= Überschreibung des Konfigurationsprofils);
- Änderungen der E-Mail-Konto Einstellungen. Sollen zusätzliche E-Mail-Konten (z.B. Funktionskonto) angelegt werden, muss dies durch das MDM Team erfolgen. Zur Nutzung von privaten E-Mail-Konten kann die mobile Webseite des jeweiligen Anbieters genutzt werden.
- Löschung der bereitgestellten Profile mit den digitalen Zertifikaten;
- Nutzung eines öffentlichen oder unverschlüsselter WLAN Netze ohne manuell aktivierte VPN-Verbindung;

B. Einstellungen durch die Nutzer

1. Kennwörter auf dem Gerät und für FernUni Anwendungen

Nach der Geräteübergabe durch das MDM Team ist unter Beachtung der geltenden Passwortregeln die Codesperre (ein 6-stelliger Zahlencode) für den Sperrbildschirm einzugeben. Danach sind die persönlichen Kennwörter für das dienstliche E-Mail-Konto und für das WLAN-Netzwerk *eduroam* der FernUni Hagen einzugeben.
Der Code für die Einschränkungen auf dem Gerät soll nach der Übergabe nicht geändert werden, damit die Voreinstellungen bestehen bleiben.
Im Einstellungsbereich „*Datenschutz*" bei den „*Einschränkungen*" sind nur in Ausnahmefällen Änderungen vorzunehmen. Beispielsweise können dort die Kontakte oder der Kalender für Apps von Drittanbietern freigegeben werden, was gegen die Regelungen der Informationssicherheit und des Datenschutzes verstoßen würde.

2. Benutzeridentifikation, die Apple-ID

Die Nutzung der Geräte erfordert ein persönliches Benutzeridentifikationskonto bei der Firma Apple. Diese Apple-ID genannte Benutzer-ID zur dienstlichen Nutzung soll unter Angabe der dienstlichen E-Mail-Adresse und weiterer dienstlicher Adressdaten der FernUni Hagen angelegt werden.
Diese Apple-ID ist notwendig, um bestimmte Konfigurationen auf den Geräten festlegen zu können, um Apps über das Mobile Device Management MDM per Fernwartung zuzuweisen oder über den *Apps@Work* Store installieren zu können. Zum Anlegen einer Apple-ID ohne Kreditkartendateninformationen nutzen Sie bitte die Anleitung im Wiki.

Auf den Dienstgeräten darf nur die dienstliche FernUni Apple-ID verwendet werden. Die Nutzung einer privaten Apple-ID für dienstliche Zwecke ist unzulässig.

Im Benutzerkonto der FernUni Apple-ID dürfen keine Kreditkarten Informationen hinterlegt werden. Bei Zahlungsvorgängen sollen Gutscheinkarten verwendet werden.

II. Sicherheitsvorgaben im Betrieb

A. Gesicherte Internetverbindung mit VPN

Die Nutzer sollen dafür sorgen, dass eine gesicherte Internetverbindung beim Abruf von Daten und dem Zugriff auf Ressourcen der FernUni Hagen genutzt wird. Die voreingestellte VPN Verbindung (Virtuelles Private Netzwerk) soll für folgende Anwendungen manuell aktiviert werden.
Für alle Zugriffe auf Anwendungen und Dienste der FernUniversität (Netzlaufwerke, BSCW-Server, Sharepoint-Server, etc.) bei der Nutzung:

- eines öffentlichen WLAN-Netzes
- eines privaten WLAN-Netzes
- der Mobilfunk-Netze (GSM, UMTS, LTE)

Kein Zugriff auf SAP-Anwendungen FiBu, HCM, etc. sowie SSH Zugriff auf Server/Clients!

B. Nutzung und Installation von Apps

1. Enterprise App Store *Apps@Work*

Die FernUni Hagen stellt auf den mobilen Endgeräten einen eigenen Enterprise App Store (*Apps@Work*) bereit. Nur über diesen App Store sind verwaltete Apps zu beziehen - der App Store von Apple steht nicht mehr zur Verfügung. Über den Enterprise App Store sind ebenfalls App-Updates zu beziehen, sobald diese durch das ZMI freigegeben werden.

2. Finanzierung und Lizensierung der Apps

Die FernUni Hagen finanziert und lizenziert alle über das MDM bereitgestellten Apps. Die FernUni Hagen übernimmt keine Verantwortung für diese Apps, diese liegt beim Unternehmen Apple als Plattformbetreiber und den Herstellern der Apps. Die Installation nicht verwalteter Apps für den dienstlichen und privaten Gebrauch ist durch die Sperrung des Apple App Stores nicht mehr möglich.
Die FernUni Hagen erhebt keinen Anspruch auf die in der Vergangenheit für private Zwecke erworbenen Apps. Diese können jedoch nicht mehr auf den dienstlichen Geräten genutzt werden, da wie oben bereits erwähnt die Installation von nicht verwalteten Apps untersagt ist.

3. Verbot der Nutzung von Drittanbieterdiensten

Durch das Betriebssystem erhält der Nutzer die Möglichkeit, Drittanbieterdienste zu aktivieren, welche nicht Datenschutzkonform sind. Da sich diese Dienste jedoch durch die MDM-Konfiguration nicht ohne andere Beeinträchtigungen deaktivieren lassen, müssen die Nutzer darauf achten, diese Dienste nicht zu nutzen. Das sind insbesondere:
Twitter, Facebook, Flickr, Vimeo, iCloud.

C. Rücksetzung auf Werkszustand, (Fern)-Löschung von Daten, Datensicherung

1. Rücksetzung auf Werkszustand; Fernlöschung

Das Gerät darf über die Einstellungen am Gerät nicht auf den ursprünglichen Werkszustand zurückgesetzt werden. Ein zurückgesetztes Gerät darf dienstlich nicht mehr genutzt werden und ist unverzüglich dem MDM Team zur Neukonfiguration auszuhändigen.
Die Fernlöschung eines Gerätes aus Datenschutz- und Sicherheitsgründen im Falle von Verlust oder Diebstahl obliegt einzig der Administration des MDM im ZMI. Der Helpdesk ist zu informieren. Nur in absoluten Ausnahmefällen (Helpdesk ist am Wochenende nicht erreichbar) dürfen die Nutzer aus Sicherheitsgründen die Fernlöschung oder Rücksetzung durchführen.

2. Datensicherung

Die Sicherung der Daten auf dem Gerät (Backup) wird vom ZMI nicht zentral unterstützt. Eine Sicherung der Daten auf dem Gerät (Dokumente, Bilder, Einstellungen, etc.) kann von den Nutzern selbst vorgenommen werden. Die Sicherung mit Hilfe des Programms iTunes darf jedoch nur auf dienstlichen Geräten wie Arbeitsplatz PC oder Notebook vorgenommen werden.

D. Einschränkung von Funktionen und Apps auf dem Gerät

1. Gesperrte Funktionen oder Apps

In der Voreinstellung sind bestimmte Funktionen im Bereich „Einschränkungen" vorgenommen worden. Einige dieser Einschränkungen wurden durch die MDM Profilkonfiguration gesperrt, so dass sie nicht genutzt werden können, z.B. der Sprachassistenzdienst Siri, AirDrop, etc.

2. Aktivierbare Funktionen oder Apps

Andere Funktionen wie Bluetooth, Mikrofon, Ortungsdienste, Kalender, Kontakte, Fotos, Erinnerungen, etc. sind per Voreinstellung zwar deaktiviert, lassen sich durch den Nutzer jedoch wieder aktivieren. Es wird darauf hingewiesen, dass die nachträgliche Aktivierung einiger dieser Funktionen oder Apps zur Verletzung der Informationssicherheit dienstlicher Daten oder des Persönlichkeitsschutzes des Nutzers und anderer dritter Personen auf dem Gerät führen kann.

Beispiel 1: Die Ortungsdienste des Gerätes über GPS, WLAN oder Mobilfunk sind zunächst deaktiviert. Zur Nutzung bestimmter Dienste (z.B. zur Navigation, Fahrplansuche, etc.) ist eine **temporäre Änderung** der „Einschränkungen" zulässig. Es gibt jedoch auch Systemdienste wie Werbung (iAds), „*Häufige Orte*", „*In der Nähe beliebt*", etc. bei denen eine nicht erwünschte Datenübertragung aktiviert werden könnte.
Beispiel 2: Die Sperrung der Fotos bewirkt beispielsweise, dass Apps nicht auf die Fotos auf dem Gerät zugreifen dürfen.
Die Nutzer sollen dafür sorgen, dass diese Einschränkungen im Regelfall deaktiviert bleiben oder nach der temporären Nutzung wieder deaktiviert werden.

3. Hinweise zur Nutzung weiterer Funktionen oder Apps

Kamera
Der Gebrauch der Kamera ist freigeschaltet. Eine Trennung von dienstlichen und privaten Fotos in den Apps Fotos und Videos ist nicht möglich. Die Nutzer sollen beim dienstlichen Gebrauch auf die Erforderlichkeit der Bilder und den Persönlichkeitsschutz von Personen achten.

Mikrofon
Das Mikrofon ist deaktiviert. Die Nutzung des Mikrofons sollte ebenfalls sehr sorgfältig ausgewählt werden. Das verdeckte Aufzeichnen von Gesprächen ist nicht erlaubt. Installierte Apps könnten das Mikrofon zur Aufzeichnung der Umgebungsgeräusche nutzen, z.T. auch ohne Kenntnis des Nutzers.

Nutzung von Drittanbieterkonten
Auch von uns verwaltete sowie System-Apps können mit sog. Drittanbieterkonten genutzt werden. Eine Registrierung oder Anmeldung mit der dienstlichen E-Mail-Adresse über das mobile Endgeräte ist derzeit unzulässig. Auch private Konten dürfen mit den dienstlich verwalteten Apps nicht genutzt werden.

Apps von Apple: Health App und Apple Watch. Nutzung nicht erlaubt.
Mit den Updates des iOS Betriebssystems für iPhones seit der Version 8.0 sind neue Programme wie die **Health App** und die **Apple Watch** hinzugekommen. Diese sind fest mit dem Betriebssystem von Apple verknüpft und lassen sich deshalb weder löschen noch deaktivieren. Die Funktionen dieser Apps sind mit den Zielen der FernUniversität Hagen für mobile Gerätenutzung und Bereitstellung mobiler digitaler Dienste nicht kompatibel. Sie dürfen deswegen nicht genutzt werden. Die Verbindung des iPhones mit einer iWatch von Apple ist untersagt. Dies gilt auch für sonstige mobiler Geräte mit denen z.B. Daten mit Sensoren erfasst werden oder auf die Daten des iPhones zur Ansicht und Verarbeitung übertragen werden.
Der Tracker des iPhone zur Bewegungs- und Schrittzählung wird durch das MDM Team manuell deaktiviert. (Einstellungen -> Datenschutz -> Bewegung & Fitness -> Fitnessprotokoll -> deaktivieren). Eine Reaktivierung dieser Funktion ist zu unterlassen.

III. Dienstliche und private Nutzung des Mobilfunks

Regelungen für die Nutzung der von der FernUni Hagen zur Verfügung gestellten SIM Karten zu dienstlichen und privaten Zwecken werden an anderer Stelle beschrieben.

IV. Abschließender Hinweis

Die bisher geltenden Sicherheits- und Datenschutzvorgaben für die dienstliche Nutzung von IT-Geräten (Arbeitsplatzrechner, Laptop, etc.) sind auch für Smartphones und Tablets zu beachten. Dies betrifft z.B. den Umgang mit Passwörtern, den Schutz der Daten vor Unbefugten, sowie die Nichtverwendung von als sicherheitskritisch einzustufenden Diensten und Anwendungen.