Arbeitsrichtlinie
Mobile Endgeräte

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 21.0

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Arbeitsrichtlinie Mobile Endgeräte
Version	21.0
Geltungsbereich	Siehe Geltungsbereich Richtlinie Informationssicherheit
Erstmalige Freigabe	06.12.2019
Verabschiedet durch	Daniel Fürdauer (Informationssicherheitsbeauftragter)
Klassifikation	Intern
Verantwortlicher Verantwortliche Abteilung	Daniel Fürdauer Datenschutz und Informationssicherheit
Fachlicher Ansprechpartner	Daniel Fürdauer (daniel.fuerdauer@vav.at)
Letztes Review	November 2021

Dokumentenhistorie

Version	Datum	Beschreibung der Änderung	Ersteller
19.0	06.12.2019	Ersterstellung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 19.0.	Daniel Fürdauer
20.0	04.12.2020	Redaktionelle Änderungen und Änderungen in Anlehnungen an die entsprechende Arbeitsrichtlinie der VHV in der Version 20.0 (Sichtschutzfolien; mobile Endgeräte im Ausland)	Daniel Fürdauer
21.0	11.11.2021	Explizite Gültigkeit der Einleitung auch für externe Dienstleister ergänzt in Anlehnungen an die entsprechende Arbeitsrichtlinie der VHV in der Version 21.0	Daniel Fürdauer

Hinweis zur Schreibweise

Die verwendete männliche Sprachform dient der leichteren Lesbarkeit und meint immer alle Geschlechter (m/w/d). Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

INHALTSVERZEICHNIS

1. EINLEITUNG

Diese Richtlinie enthält Vorgaben für die Beschaffung und den sicheren Umgang mit mobilen Endgeräten. Unter mobilen Endgeräten im Sinne dieser Richtlinie sind alle mobilen Kommunikationsgeräte, die ortsungebunden zur Sprach- und Datenkommunikation eingesetzt werden können, zu verstehen. Unter den Begriff der mobilen Endgeräte fallen somit beispielsweise jegliche Arten von mobilen Computern, Mobiltelefone, Smartphones, Tabletcomputer, USB-Sticks und Speicherkarten.
Diese Richtlinie gilt ausschließlich für mobile Endgeräte, die von der VAV für Mitarbeiter und externe Dienstleister beschafft bzw. zur Verfügung gestellt werden.

2. PLANUNG UND BESCHAFFUNG

Die Beschaffung von mobilen Endgeräten erfolgt ausschließlich über den zentralen Beschaffungsprozess der VAV durch das Ressort IT/BO/FM. Bei der Beschaffung von mobilen Endgeräten müssen neben wirtschaftlichen und funktionalen Aspekten folgende sicherheitsrelevante Punkte berücksichtigt werden:

- Die mobilen Endgeräte müssen kompatibel zur bestehenden oder ggf. geplanten IT-Infrastruktur sein.
- Das Betriebssystem der mobilen Endgeräte sowie die Hardware selbst müssen mit angemessenen Zugriffs- / Zugangskontrollen ausgestattet sein.
- Das Betriebssystem der mobilen Endgeräte muss angemessene, dem Stand der Technik entsprechende, kryptographische Mechanismen für die Übermittlung von Daten von und zum Gerät bereitstellen.
- Es sollte die Möglichkeit bestehen, weitere Sicherheitsfunktionen nachzurüsten bzw. diese zu erweitern.

3. INVENTARISIERUNG

Alle mobilen Endgeräte sind als Eigentum der VAV zu kennzeichnen. Alle mobilen Endgeräte sind entsprechend der Vorgabe in der Konzernrichtlinie Informationssicherheit zu inventarisieren.

4. ÜBERGABE AN MITARBEITER

Sämtliche mobile Endgeräte müssen vor Übergabe an den Mitarbeiter im Rahmen eines Freigabeprozesses durch die Führungskraft beantragt werden. Erst nach Freigabe dürfen die Geräte an die Mitarbeiter ausgehändigt werden. Die Aushändigung und Entgegennahme sind zu dokumentieren.

5. BETRIEB

Beim Betrieb von mobilen Endgeräten sind die nachfolgenden Punkte zu beachten.

5.1. Installation und Konfiguration

Installationen und Konfigurationen dürfen grundsätzlich nur durch die dafür verantwortlichen Mitarbeiter des IT Supports durchgeführt werden. Nicht von dem IT Support autorisierte Installationen und Konfigurationsänderungen durch die Benutzer sind unzulässig. Je nach Art des mobilen Endgeräts gelten im Rahmen der Installation und Konfiguration folgende ergänzenden Anforderungen:

5.1.1. Mobile Computer

- Jeder mobile Computer ist mit dem von dem IT Support bereitgestellten aktuellen Betriebssystem auszustatten und aktuell zu halten.
- Die installierte Hard- und Softwarekonfiguration darf vom Anwender nicht verändert, manipuliert oder erweitert werden.
- Nach Vorgaben der Arbeitsrichtlinie Schutz vor Schadsoftware ist ein Virenschutz lokal zu installieren. Updates der Anti-Virensoftware sollten automatisch installiert werden, um diese stets auf dem aktuellen Stand zu halten.
- Die Festplatten sind nach Vorgaben der Arbeitsrichtlinie Kryptographie komplett zu verschlüsseln.
- Wird der mobile Computer regelmäßig außerhalb der VAV-Gebäude verwendet, sollte das Display mit einer Sichtschutzfolie versehen werden, oder vergleichbare Maßnahmen gesetzt werden.

5.1.2. Smartphones und Tablets

Anforderungen für den **dienstlichen Bereich**:

- Zusätzliche Installationen durch Benutzer auf den Geräten werden blockiert (ausgenommen ist der nicht dienstliche Bereich).
- Smartphones dürfen nur mit IT-Systemen der VAV kommunizieren. Ausnahmen: Bluetooth Freisprecheinrichtungen und private Computer zum Synchronisieren nicht-dienstlicher Daten.
- Der dienstliche Bereich, oder das gesamte Gerät, ist mit einem Kennwort zu schützen. Die Anforderungen richten sich nach der Arbeitsrichtlinie Kennwörter.
- Programmaktualisierungen (neue App-Versionen, Sicherheitsupdates) werden durch die Hersteller bereitgestellt und müssen regelmäßig vom Anwender selbst aktualisiert werden. Für die Verbindung zur VAV können auch WLANs (private, öffentliche) genutzt werden, da eine ausreichende Verschlüsselung vorliegt.
- Bei Verlust des Smartphones erfolgt eine Löschung des Geräts. Hiervon ist auch der nicht dienstliche Bereich, zum Schutz vor unbefugtem Zugriff durch nicht berechtigte Personen, betroffen. Wenn es wahrscheinlich ist, das Smartphone zurückzuerlangen, ohne dass der Schutz vor unbefugtem Zugriff durch nicht berechtigte Personen beeinträchtigt wird, kann die Löschung solange verzögert werden.

Regelungen für den **nicht dienstlichen Bereich**:

- Die Installation von Software und Apps im nicht dienstlichen (privaten) Bereich erfolgt auf eigene Verantwortung des Nutzers. Ein Support durch die IT erfolgt nicht.

- Es ist verboten, Daten aus dem dienstlichen Bereich in den nicht dienstlichen Bereich zu übertragen.

5.1.3. Datenträger, Digitalkameras und sonstige Speichermedien

Mobile Datenträger, insbesondere USB-Sticks und digitale Kameras dürfen nur über freigeschaltete Schnittstellen betrieben werden. Der Freigabeprozess wird über die IT initiiert.
Auf digitalen Kameras dürfen nur die mit der Kamera erstellten Aufnahmen gespeichert werden. Die Nutzung als Datenspeicher / -transportmedium für weitere Daten ist unzulässig.
Weitere mobile Datenträger, wie beispielsweise Datensicherungsmedien, dürfen nur von der IT im Rahmen der Datensicherung oder Installation / Wartung eingesetzt werden.

5.2. Authentifizierung und Verschlüsselung

Der nicht autorisierte Zugang zu mobilen Endgeräten ist mit angemessenen Authentifizierungsmechanismen zu verhindern. Jedes tragbare Endgerät sollte daher zumindest mit einem Kennwortschutz versehen werden, das verhindert, dass das Endgerät unberechtigt benutzt werden kann (siehe auch Arbeitsrichtlinie Kennwörter).
Die mobilen Endgeräte sollen weiterhin möglichst über Funktionen verfügen, die die mobilen Endgeräte automatisch bei nicht autorisiertem Gebrauch oder Verlust deaktivieren, alle Daten auf diesen löschen, oder alternativ manuell aus der Ferne löschbar sind.

- Ist ein mobiles Endgerät und / oder Datenträger nicht durch eine Kennwortroutine beziehungsweise einer Verschlüsselung geschützt, ist die Speicherung von vertraulichen und streng vertraulichen Daten verboten.
- Vertrauliche und streng vertrauliche Daten dürfen nur in verschlüsselter Form transportiert werden. Weitere Details können der Arbeitsrichtlinie Informationsklassifizierung entnommen werden.
- Die Planung und technische Realisierung der Verschlüsselung wird durch die IT in Zusammenarbeit mit der Stabstelle Datenschutz und Informationssicherheit vorgenommen (siehe Arbeitsrichtlinie Kryptographie). Ausnahmeregelungen hiervon sind nur nach ausdrücklicher Genehmigung durch die Stabstelle Datenschutz und Informationssicherheit möglich.

5.3. Datensicherung

Die Mitarbeiter sind dazu verpflichtet, solche Daten, die beispielsweise bei fehlender Verbindung zur VAV nicht auf Netzlaufwerken gesichert werden können, später zu sichern. Daten, die lediglich als Kopie auf mobilen Endgeräten vorhanden sind, müssen nicht gesichert werden.

5.4. Wartung und Defekte

Die Wartung (z.B. Reparatur, Softwareupdates, Austausch) mobiler Endgeräte erfolgt über den IT Support.
Im Falle eines Defekts eines mobilen Endgeräts sind die darauf befindlichen Daten vor der Rückgabe sicher zu löschen. Es gelten die Regelungen der Arbeitsrichtlinie Entsorgung von Datenträgern.

5.5. Diebstahl und Verlust

Ein Diebstahl oder Verlust von mobilen Endgeräten ist unverzüglich durch den Nutzer dem IT Support zu melden. Von dort aus werden dann die notwendigen nachgelagerten Aktivitäten gesteuert. Im Anschluss ist das Meldeformular Datenschutz & Informationssicherheit auszufüllen und an die Stabstelle Datenschutz und Informationssicherheit zu senden.

5.6. Verwendung von mobilen Endgeräten im Ausland

Sollten staatliche Stellen (z. B. der Zoll) die Herausgabe eines mobilen Endgeräts verlangen, ist dieser Weisung Folge zu leisten. Wird das mobile Endgerät außer Sichtweite (z. B. in einem anderen Raum) von der staatlichen Stelle untersucht und könnte Schadsoftware / Spionagesoftware installiert worden sein, darf das Gerät bis auf weiteres nicht mit dem Netzwerk der VAV verbunden werden. Der Vorfall ist unverzüglich telefonisch dem IT Support unter

+43.1.716 07-666

zu melden. Der IT Support veranlasst in Abstimmung mit der Stabstelle Datenschutz und Informationssicherheit etwaige notwendige Maßnahmen.

6. RÜCKGABE

Mobile Endgeräte sind bei Ausscheiden oder Wegfall des Nutzungszwecks durch den Mitarbeiter an den IT Support zurückzugeben.
Im Falle der Rückgabe von mobilen Endgeräten sind die gespeicherten Daten ausreichend sicher zu löschen. Insoweit gelten die Regelungen in der Arbeitsrichtlinie Entsorgung von Datenträgern. Die Rückgabe von mobilen Endgeräten ist zu dokumentieren.