RICHTLINIE für die Nutzung von FIRMENMOBILTELEFONEN

Version 2 (Stand 02.05.2018)

- Dem Mitarbeiter wird ein Firmenmobiltelefon in einem einwandfreien Zustand zur Verfügung gestellt. Der Mitarbeiter hat keinen Anspruch auf eine bestimmte Marke bzw. ein bestimmtes Modell. Das Firmenmobiltelefon kann daher jederzeit durch ein anderes Modell ersetzt werden.
- Der Mitarbeiter erhält einen PIN-Code zur Benutzung des Geräts, den er frei ändern kann. Der PIN-Code ist vom Mitarbeiter geheim zu halten. Generell ist die Nutzung des Firmenmobiltelefons für dienstliche Zwecke vorgesehen. Darüber hinaus wird dem Mitarbeiter eine private Nutzung des Geräts erlaubt, sofern dem Unternehmen dadurch keine Kosten entstehen, das heißt z.B. Telefonie in Netze, für die keine Gesprächsgebühren anfallen. Private Nutzung von kostenpflichtigen Diensten ist ausdrücklich untersagt, die so entstehenden Kosten werden im Anlassfall an den Mitarbeiter weiterberechnet. Die Auflistung der Dienste und Gebühren des aktuellen Handytarifs des Unternehmens können bei der Administration regelmäßig eingesehen werden.
- Bei Dienstreisen ins Ausland darf der Mitarbeiter auch private Telefonate vom Firmenmobiltelefon in angemessenem Ausmaß führen. Die Einräumung dieser Rechte ist jedoch freiwillig, auf diese Privatnutzung besteht daher selbst bei wiederholter langjähriger Gewährung weder dem Grunde, noch der Höhe nach ein Rechtsanspruch für die Zukunft. Die Privatnutzung ist daher unverbindlich und kann jederzeit vom Dienstgeber widerrufen werden. Schäden am Firmenmobiltelefon sind unverzüglich der IT-Administration bekannt zu geben sowie das schadhafte bzw. beschädigte Firmenmobiltelefon in der IT-Administration abzugeben.
- Bei Auslandsaufenthalten hat der Mitarbeiter zu beachten, dass die Datendienste im Roaming-Modus ein angemessenes Entgelt nicht übersteigen, da ansonsten hohe bzw höhere Kosten entstehen. Im Falle von Missachtung dieser Regelung kommt der Mitarbeiter für die entstandenen Mehrkosten auf.
- Der Verlust des Firmenmobiltelefons ist unverzüglich der IT-Administration bekannt zu geben, der Mitarbeiter haftet zur Gänze für das in Verlust geratene Firmenmobiltelefon. Der Diebstahl des Firmenmobiltelefons ist vom Mitarbeiter unverzüglich bei der Polizei anzuzeigen und ebenfalls unter Vorlage der Anzeige in der IT-Administration zu melden. Bei Beendigung des Dienstverhältnisses ist das Mobiltelefon samt Netzgerät, Zubehör sowie der entsprechenden PIN Codes der IT-Administration zurückzugeben.
- Der Mitarbeiter nimmt zur Kenntnis, dass auf dem Mobiltelefon interne Daten des Unternehmens gespeichert sind (z.B. Mails, Kontakte, Kalendereinträge) und dass er höchste Sorgfalt zum Schutz dieser Daten gegen den Zugriff Dritter anzuwenden hat.
- Kostenlose, öffentlich zugängliche WLAN-Netzwerke sind zu vermeiden, wenn Mobilgeräte für berufliche Zwecke eingesetzt werden. Unverschlüsselte Kommunikation über das Netzwerk kann problemlos abgehört werden. Im schlimmsten Fall können auch Daten auf dem Gerät ausgelesen werden.

- Private Cloud-Speicherdienst (Dropbox, iCloud, Google Drive) dürfen nicht für Unternehmensdaten verwendet werden. Fragt bei der zuständigen IT-Administration nach, welche Möglichkeiten bestehen, um Firmendokumente über das Internet sicher abzuspeichern.
- Mobilgeräte müssen ebenso wie PCs durch Passwörter oder PINs vor unbefugter Inbetriebnahme geschützt werden. Das Aufheben der automatischen Sperre nach Nichtbenutzung muss ebenfalls durch ein Passwort geschützt sein. Lasst eure Mobilgeräte nicht entsperrt liegen und gebt es nicht unbeaufsichtigt an Andere weiter.
- Im Idealfall sollten nur vorher geprüfte und als sicher eingestufte Apps installiert werden. In jedem Fall müssen die Benutzer aber auf ihre Auswahl achten und dürfen nur vertrauenswürdige Programme installieren.
- Auf manchen Systemen kann bei der Installation von Apps gewählt werden, auf welche Datenbestände das neue Programm zugreifen darf. Dabei sollten nur Zugriffe erlaubt werden, die unkritische Daten oder Funktionen umfassen.
- Das sogenannte „Jailbreaking“, d.h. das Aushebeln der vom Hersteller vorgesehenen Sicherheitsmaßnahmen, darf auf beruflich verwendeten Mobilgeräten keinesfalls ausgeführt werden. Es setzt die Geräte besonderen, zusätzlichen Sicherheitsgefährdungen aus.
- Wenn mobile IT-Geräte weitergegeben oder entsorgt werden, müssen alle darauf gespeicherten Daten und Einstellungen gelöscht werden. Dazu eignet sich am besten ein „Factory Reset“, d.h. das Zurücksetzen des Geräts in den Auslieferungszustand. Danach sollte noch manuell nachgeprüft werden, ob noch Informationen auf den Speichern verblieben sind.