Inhoud

QM:Mobile Device Usage Policy

The use of mobile IT devices (notebooks, smartphones, tablet PCs) poses significant risks for the company: confidential company data is stored and used outside the company. Portable devices are an attractive, easily sold prey for thieves.

Workinstructie	
Instructions for employees regarding the use of mobile IT devices	
Toepassingsgebied	Company-wide
Versie	

If you use mobile IT devices, the following regulations must be observed.

Inhoud

1 Registration and Approval 3
2 Anti-theft storage and theft behavior 3
3 Use of security programs and installation of apps 3
4 Use of public networks and cloud services 3
5 Rules for disabling functionality 4
6 Disposal 4

Registration and Approval

- If you want to use your own smartphone or tablet for professional purposes: Check with your IT supervisor and supervisor first to see if this usage is allowed in your organization. Together, make sure that all necessary security measures have been implemented!
- If your company uses a Mobile Device Management solution: Use only the intended applications for professional purposes and do not process official data in private, unprotected areas!

Anti-theft storage and theft behavior

- Make sure your device is safe against theft. Do not store it in your vehicle. If this is unavoidable, cover the unit or lock it in the trunk.
- Do not leave the device unattended and do not leave it to others! Lock it during short breaks or turn it off. Set it so that it can only be operated after overcoming an access protection function (password, PIN, fingerprint, recognition pattern, ...).
- Report a theft or loss to the IT department immediately! Remote access to your company may need to be blocked or passwords changed to prevent unauthorized access. Immediate reporting of the incident can help prevent further security breaches.

Use of security programs and installation of apps

- There are several programs and services that allow you to remotely erase all data on a stolen or lost smartphone. Be sure to use these apps! The use of anti-virus programs for smartphones and tablets is also highly recommended.
- Encrypt hard disk contents or important files to prevent unauthorized access to company data. Activate file encryption on your smartphone or tablet or use an encryption app to store sensitive data!
- Only install apps that are known to you as trustworthy and secure! If in doubt, ask your IT staff or research on the Internet, if there are any known dangers.
- Many apps require access to various device functions during installation (WLAN, GPS receiver ...). Consider for yourself whether it is necessary that e.g. a game app gets access to your microphone or your address book. Only install apps whose access requirements you trust!

Use of public networks and cloud services

- Avoid free, publicly available Wi-Fi networks when using mobile devices for work: Unencrypted communication over the network can be easily intercepted. In the worst case, data can also be read out on your device.
- Apply a privacy screen when using the unit in public (such as at the airport) - preventing spying on company information.
- Do not use your private cloud storage service (Dropbox, iCloud, Google Drive) for corporate data! Ask your IT representative what options exist for securely storing company documents over the Internet.

Rules for disabling functionality

- Disable any device interfaces that are not required (USB, WLAN, Infrared, Bluetooth). If these interfaces are absolutely necessary (for example, WLAN for Internet connection), appropriate protective measures (personal firewall, anti-virus program, etc.) must be provided.
- Always turn off the GPS receiver on your smartphone when it is not needed.
- On smartphones or tablets you use for professional purposes, you must never override internal security mechanisms (such as "jailbreaks" or "roots")! These manipulations create additional sources of danger for the stored company data.
- Leave your smartphone during confidential meetings at your workstation or put it in flight mode!

Disposal

- Before you sell, pass on or dispose of a smartphone, you must ensure that all stored data has been deleted. This is best done via a "factory reset". After that, you have to check if any settings or data have been preserved.