Goethe University recommendations and best practices for using mobile devices

The following recommendations apply to all members of Goethe University Frankfurt. They regulate the use of mobile devices. Goethe University regulations and statutes, in particular IT security regulations, IT security guidelines and the IuK use regulation[1], are not affected by these recommendations.

These days, mobile devices with internet access are the equivalent of small computers that are used to work, communicate and save confidential data. This means they have at least the same security requirements as stationary computers.

Security is even more crucial in this case, since the possibility of having these devices with you everywhere and at all times and to be constantly connected with the Internet carries additional risks. The official use of private devices is quite practical, but it means that additional requirements are necessary for the secure use of these devices.

Goethe University's Security Management Team (SMT) recommends the following measures regarding information security for mobile devices:

1) When **purchasing** a mobile device, make sure the operating system is up to date and that **updates are available**.

2) Make sure you have **basic protection** and carry out security updates regularly.

   - Keep the operating system and all installed software and apps up to date with security updates. Many attacks are aimed at known vulnerabilities that can only be closed by an update from the manufacturer. For this reason, activate the **automatic update function** so that security updates are installed right after they are released.

3) Only install apps from **trusted sources** and check the access authorisations.

   - Before installing an app, get information about it if you are not familiar with the provider. A quick Internet search is usually sufficient to inform yourself. Remove **outdated applications** as well as ones you no longer us. Every additional app is a potential security gap.

[1] Allgemeine Nutzungsordnung für die Informationsverarbeitungs- und Kommunikationsinfrastruktur der Goethe-Universität Frankfurt – General use regulations for information processing and communication infrastructure at Goethe University Frankfurt

- Many apps grant themselves wide-ranging rights for no recognisable reason. It is not necessary, for example, that every app has access to location, address book or telephone status. Critically review whether the **access rights** are necessary for carrying out the function.

4) Use **lock codes** and **passwords**.

   - Access to mobile devices and their applications must be protected through measures such as a password or PIN.

5) Only activate interfaces as needed and secure them.

   - Deactivate wireless interfaces such as B**luetooth or NFC** when you are not using them. This makes your device less vulnerable to cyber attacks.

6) Only connect your mobile device with **trusted computers**.

7) Use extra care with public hotspots.

   - Public WIFI hotspots should not be used without heedlessly, as they do not always provide a secure, encrypted connection. In particular when using sensitive data (e.g., online banking, shopping, etc.), **an encrypted connection** is essential.

   - It is best to use a VPN connection. The University Computing Centre (HRZ) provides a free VPN connection for all university members. You can find more information at: https://www.rz.uni-frankfurt.de/vpn

8) Never let your device out of your sight.

   - To protect your device from unauthorised access and manipulation, **never leave it unwatched and never lend it** to someone else. Lost or stolen official mobile phones must be reported to your IT support officer.

9) Use common sense when surfing.

   - Maintain a healthy amount of scepticism when it comes to following recommendations for apps on what you install, from where and on what you click. Not everything is as good as its promise, and empty promises are a popular vehicle for installing malware on a device.

10) Protect your data.

   - Use the functions for data encryption where available, or encrypt sensitive data yourself using encryption software.

   - Create **back-up copies** regularly.

11) Check unknown numbers before returning calls.

   - Current information on the improper use of telephone numbers can be found in German on the internet site of the Bundesnetzagentur (Federal Network Agency). If necessary, you can have unwanted numbers blocked by your network provider as a value-added service.

     https://www.bundesnetzagentur.de/Rufnummernmissbrauch

12) Delete your entire storage before selling or disposing of your device.

   - If you do not want your stored data to fall into the wrong hands when you sell or dispose of your device, all data storage (**internal storage and SD cards**) should be securely deleted. The SIM card and if necessary the SD cards should be removed and – if you no longer wish to use them – destroyed.

13) Please contact your IT support or your IT security officer if you have any questions.

Further information:

- Bundesamt für Sicherheit in der Informationstechnik (BSI) - (Federal Office for Information Security)
  https://www.bsi-fuer-buerger.de

- DFN Computer Emergency Response Team (DFN-CERT)
  https://www.dfn-cert.de

- IT-Sicherheitsmanagement-Team (SMT) - Goethe-University IT Security Management Team
  https://www.uni-frankfurt.de/smt

- Goethe University Computer Emergency Response Team (GU-CERT)
  https://www.rz.uni-frankfurt.de/gu-cert

- Hochschulrechenzentrum (HRZ) – Goethe University Computing Centre
  https://www.uni-frankfurt.de/hrz/it-sicherheit