InnoFly Company Family
Policy for the Use of Company Phones

1 Provision of a Company Phone

In certain cases, the employee will be provided with a company mobile phone in good working condition. The employee ***has no entitlement to a specific brand or model***. Therefore, the company mobile phone may be replaced by another model at any time.

The employee will receive a PIN code for using the device, which can be changed freely. The ***PIN code*** must be ***kept confidential*** by the employee. In general, the use of the company mobile phone is intended for business purposes. However, the employee is also allowed to ***use the device privately within reasonable limits***, provided that no costs are incurred by the company, meaning, for example, calls to networks for which no call charges apply. ***Private use of paid services is strictly prohibited***, and any resulting costs will be charged to the employee, as applicable. A list of services and fees for the current mobile plan can be reviewed regularly at the IFM-Office.

2 Business Trips Abroad with Company Phone

During business trips abroad, the employee may also ***make private calls from the company mobile phone within reasonable limits***. However, granting this privilege is voluntary, and no legal entitlement exists to this private use, either in principle or in terms of the amount, even after repeated long-term provision. Therefore, priv***ate use is non-binding and can be revoked by the employer at any time.***

Before traveling, the employee should inquire at the IFM-Office about international tariffs to minimize potential additional costs.

When traveling abroad, the employee must ensure that data services in ***roaming mode do not incur excessive charges***, as higher costs may result. If this regulation is violated, the employee will be responsible for the additional costs incurred.

3 Guidelines for the Use of the Company Phone

The employee acknowledges that company data (e.g., emails, contacts, calendar entries) are stored on the mobile phone and that the ***highest level of care must be taken to protect this data from unauthorized access.***

- → ***Activate automatic updates:*** Where possible, enable automatic updates for the operating system and apps. This ensures that updates are installed promptly without manual intervention.
- → ***Install updates promptly:*** For devices that do not support automatic updates, new updates should be installed immediately after receipt. Ignoring updates can open security vulnerabilities that attackers may exploit.
- → ***Check app updates:*** Regularly check the App Store or Google Play Store and install all available app updates. This protects against potential security risks and improves the functionality of the applications.
- → ***Take security warnings seriously:*** Pay attention to notifications or warnings regarding updates and address them promptly. These notifications often relate to critical security improvements or bug fixes.

→ ***Avoid using free, public Wi-Fi networks*** when mobile devices are used for business purposes. Unencrypted communication over such networks can easily be intercepted. In the worst-case scenario, data on the device may also be accessed.
→ Only enable interfaces like ***Bluetooth, Wi-Fi, or NFC when needed***, and ***disable*** them immediately ***after use***. These interfaces can be targets for cyberattacks. Additionally, this helps conserve battery life.
→ ***Private cloud storage services*** (e.g., Dropbox, iCloud, Google Drive) must ***not be used*** for company data. Inquire at the IFM Office about secure ways to store company documents over the internet.
→ Mobile devices, like PCs, must be ***protected from unauthorized activation*** by ***passwords, PINs, or biometric access***. The auto-lock feature after inactivity should also be secured with a password. Do not leave your mobile devices unlocked or unattended with others.
→ Ideally, only pre-vetted and secure apps should be installed. In any case, users must carefully select their apps and ***only install trusted programs***. On some systems, it is possible to choose which data the new app can access. Only allow access to non-sensitive data or functions.
→ "***Jailbreaking***" (i.e., bypassing the manufacturer's intended security measures) must ***never be performed*** on mobile devices used for work. It exposes the device to additional security risks.

4 Damage, Loss and Termination of Employment

→ Any damage to the company mobile phone must be ***reported immediately to the IFM-Office***, and the damaged or defective device must be returned to the IFM-Office.
→ In case of loss of the phone, immediate action must be taken:
1. Try calling the phone – you may have simply misplaced it.
2. If possible, locate and lock the phone. The lock and locate function varies by model.
3. Immediately notify your supervisor, the Compliance Officer, and the IFM Office.
4. Change your passwords on a secondary device.

→ When mobile IT devices are passed on or disposed of, all data and settings stored on them must be erased. The best method for this is a "***Factory Reset***," which ***resets the device to its original settings***. Afterward, manually verify that no data remains on the device.