# Emergency Sheet: Phone Gone

Lost, stolen, seized · belongs to chapters 5 and 17 · Device: _____ · Preparation as of: _____

**Accounts first, then the device.** A stolen GrapheneOS device with a strong password and Auto reboot is a brick to the thief: after the reboot no keys remain in memory, storage stays fully encrypted, and the secure element slows failed unlock attempts down to a standstill, with a hard stop after twenty failed attempts. The real risk is not the device but everything attached to it: the SIM that receives codes, the email account that resets passwords, the two-factor tokens, the bank. This sheet sorts the emergency so that the accounts come first. It only holds up if the upper half was done beforehand.

## A · BEFORE, SO THE SHEET HOLDS UP IN AN EMERGENCY

| Item | OK | Note |
|---|---|---|
| **The backup runs regularly** and has been restored once as a test. It is encrypted before it leaves the device, so the target may even be storage you do not control (chapter 5). | | Schedule: _____ |
| **The recovery code is on paper** in a place you can reach in an emergency. Without it the backup is worthless. Enter only a short code for the place here. | | Kept at: _____ |
| **The two-factor vault (Aegis) has a backup outside the device**, updated after every new token, for example on a USB stick kept physically separate and in an encrypted cloud. Vault password and backup password are secured independently of it, in the password manager and on paper (chapter 17). | | Backup at: _____ |
| **The password manager is reachable from a second device.** Master password memorized, login on the computer or second device tried once. Otherwise the key to everything else is missing in an emergency. | | |
| **IMEI and proof of purchase are at home.** The IMEI is the device identifier tied to the hardware, no SIM swap changes it (chapter 6). Police and carrier will ask for it. | | Kept at: _____ |
| **Carrier hotline for blocking the SIM noted** (in the field below). In Germany, Austria and Switzerland the SIM is tied to your identity, and so to your contracts and costs. | | |
| **A second device or a computer is ready for the emergency**, one you can reach accounts with and set up a replacement device from. | | Located at: _____ |
| **Auto reboot and a strong password are active.** That is the real theft protection: not a remote service but a device that gives away nothing without you (chapter 5). | | Interval: _____ |

## B · IN AN EMERGENCY, IN THIS ORDER

| No | Step | Why | Done |
|---|---|---|---|
| 1 | **Have the SIM blocked.** Call the carrier, block the number, order a replacement SIM or eSIM profile. | No SMS codes or calls into a stranger's hands, no foreign charges on your contract. | |
| 2 | **Secure the password manager and main email** from another device: change the password, sign out all sessions, check the recovery paths. | Almost every other password can be reset through the main email. It is the master key. | |
| 3 | **Messengers:** sign the device out of the accounts where possible, otherwise re-register and inform your contacts. A Nostr key that lived only on the phone counts as compromised. | Otherwise a stranger keeps reading or writing in your name. | |
| 4 | **Inform bank and payment services**, block cards and banking apps, set up approval methods again on the replacement device. | Approval apps and cards in the wallet are money in a stranger's hands once an account falls. | |
| 5 | **Restore two-factor from the Aegis backup on the replacement device.** You need the backup file and the backup password for that. | Without tokens you lock yourself out of the very accounts you are protecting. | |
| 6 | **Bitcoin:** keys on the hardware wallet (BitBox02) are not affected, they never left that device. A wallet that lived only on the phone counts as compromised: move the funds from a clean device to a new wallet with a new seed. | An attacker who does crack the password would otherwise have time on his side. | |
| 7 | **File a police report with the IMEI**, inform the carrier about the theft, note the case number. | Report and IMEI are needed for insurance, the carrier and the case that the device turns up. | |
| 8 | **Restore the new device from the backup**, with the recovery code from the paper. Then tick off the items in part A again. | The backup is the only way back to your data. The code is the only key to it. | |
| 9 | **If the device comes back:** treat it as compromised. Do not keep using it, reinstall GrapheneOS, restore from the backup (chapter 19). | Tampering takes little time and is not readily detectable. | |

Carrier hotline: _____ · Bank blocking number: _____ · Second device located at (short code): _____ · Who gets informed: _____

⚠ **No remote locate, no remote wipe.** GrapheneOS ships no Google service for locating or wiping the device remotely and, according to its FAQ, deliberately leaves out factory reset protection because it is theft deterrence, not a security feature. A thief can therefore reset the device and keep using it. He does not get to your data as long as password and Auto reboot are active. The preparation in part A replaces both. ⚠ **No passwords, PINs or recovery codes on this sheet.** It may be found without giving anything away. Places only as short codes.