Emergency Sheet: Password Manager

Forgotten, lost, compromised · belongs to chapters 18 and 13 · Manager: [ ] KeePassXC [ ] Proton Pass · Preparation as of: _____

The password manager is the master key. That is exactly why the cluster risk deserves to be taken seriously: if it fails, every account hangs on it. A manager rarely fails because of hackers, though. It fails through three everyday cases: the master passphrase is forgotten, the file or the device is gone, the second factor is lost. Against all three only preparation helps, preparation that is done before the emergency. This sheet sorts both, the preparation at the top and the emergency at the bottom. It only holds up if part A was ticked off beforehand. The actual master passphrase never appears on this sheet. It is written by hand on the separate emergency sheet in the sealed envelope of the Disaster Kit (chapter 13).

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

Item	OK	Note
The master passphrase consists of six or more random words from the EFF list, rolled with dice or produced by the generator. It exists only in your head and once by hand on the emergency sheet in the Disaster Kit (chapter 18, rules 2 and 3). Here only the short code for the place.		Emergency sheet at: _____
No password is stored in the browser anymore. Everything was moved into the manager and the browser store was cleared. The browser is the attack surface, not the vault.		
The manager has been opened once from a second device (computer, spare device or smartphone). Otherwise the key to everything else is missing in an emergency.		Second device: _____
KeePassXC: the KDBX file is part of the 3-2-1 backup (three copies, two media, one off-site), the off-site copy encrypted before it leaves the house (chapter 13).		Last backup: _____
KeePassXC: key file and hardware token are secured. The key file is kept separate from the database. The hardware token (YubiKey) has a spare token programmed with the same secret, or the secret is on paper in the Disaster Kit. Without key file or token the database stays locked even with the passphrase.		Key file at: _____
Proton Pass: the recovery phrase of the Proton account has been generated and is on paper in the Disaster Kit. Only it restores password and data at once. A recovery email alone only resets the password, while the entries stay encrypted. The Proton account itself has a second factor. An encrypted export of the entries sits as an offline copy in the backup.		Recovery phrase at: _____
The recovery codes of the most important accounts are printed out in the Disaster Kit: main email first, then bank, Proton, Nostr key backup. Where a hardware key provides the second factor, a spare key is registered (chapter 18, rule 7).		Spare key at: _____
The restore test has been run: the backup was opened on a different device once after setup and annually since. A backup that has never been restored is only a hope.		Last test: _____
Your loved ones know that the Disaster Kit exists and where the emergency sheet is. For the copy in the safe-deposit box they hold banking power of attorney (chapter 13).		Informed: _____

B · IN AN EMERGENCY

No	Case and steps	Why	Done
1	**Master passphrase forgotten.** KeePassXC: there is no reset. The only way is the handwritten emergency sheet in the Disaster Kit. Proton Pass: reset the password with the recovery phrase from the Disaster Kit. Then set a new passphrase and renew the emergency sheet.	The encryption has no back door, not even for you. Without the emergency sheet the database is lost for good.	
2	**File damaged or device gone.** KeePassXC: fetch the backup from the 3-2-1 copies, plus key file and token, and open it on the second device. Proton Pass: sign in on the second device, then sign the lost device out of the account's active sessions.	The backup is the only way back to the data. An open session on a stranger's device otherwise remains a way in.	
3	**Second factor lost.** Sign in with the recovery codes from the Disaster Kit or the spare hardware key. Then register a new factor, remove the old one and replace the used codes with fresh ones.	In case of doubt a second factor locks you out as well. Used codes are no safety net anymore.	
4	**Suspected compromise** (malware, data breach, unknown session). From a clean device, first change the master passphrase, then the passwords in this order: main email, bank, Proton, then everything else. Sign out all sessions, check your addresses at haveibeenpwned, renew the second-factor tokens.	Almost every other password can be reset through the main email. Keeping to the order closes the door before the attacker uses it.	
5	**Permanent loss** (accident, death). Your loved ones open the Disaster Kit: emergency sheet, instructions and power of attorney are kept there together (chapter 13, digital estate).	No court can open encrypted data. What is not documented is lost to the heirs.	

Database backup kept at (short code): _____ · Emergency sheet kept at (short code): _____ · Second device: _____ · Spare token kept at (short code): _____

⚠ **No passphrase, no recovery code, no account name on this sheet**, not even "just in case". Places only as short codes that only you can read (for example "S2" for safe-deposit box 2, "FM" for the folder at a family member's). ⚠ **The handwritten emergency sheet with the passphrase is the only document that opens the manager.** It belongs in the sealed envelope, nowhere else, never in digital form.