

# Wichtige Hinweise

- **Bewahren Sie Ihre Passwörter und ggf. privaten Schlüssel getrennt und sicher auf**, etwa in einem vertrauenswürdigen Passwortmanager oder in verschlüsselten Containern. Legen Sie zusätzlich eine offline gesicherte Kopie auf einem verschlüsselten Medium (zum Beispiel einem USB-Stick im Tresor) an, um im Notfall darauf zugreifen zu können.
- **Verlust von Passwörtern oder privaten Schlüsseln führt zum unwiederbringlichen Datenverlust!** Bereits verschlüsselte E-Mails lassen sich ohne den privaten Schlüssel oder die korrekte Passphrase nicht mehr entschlüsseln.
- **Löschen Sie niemals abgelaufene Zertifikate!** Auch abgelaufene Zertifikate werden zum Entschlüsseln älterer Nachrichten benötigt, bei Verlust ist eine Entschlüsselung nicht mehr möglich.
- **Richten Sie eine klare Backup- und Wiederherstellungsstrategie ein**, erstellen Sie regelmäßige, ebenfalls verschlüsselte Sicherungen von den verwendeten Passwörtern, privaten Schlüsseln und Zertifikaten und testen Sie die Wiederherstellung in festgelegten Abständen, um im Ernstfall vorbereitet zu sein.

---

Revision #2

Created 2026-06-08 09:32:39 UTC by Sandra Ulbrich

Updated 2026-06-08 09:44:42 UTC by Sandra Ulbrich