Password & Access Plan

This is the single most impactful thing you can do for your survivors. Without access credentials, your loved ones face an uphill battle with every single account -- often requiring death certificates, court orders, and weeks of waiting per account.

2.1 -- Password Manager Setup

- [ ] Choose and set up a password manager (1Password, Bitwarden, Dashlane, LastPass, Keeper)
- [ ] Migrate existing passwords from browsers, sticky notes, and memory into the password manager
- [ ] Ensure every account has a unique, strong password
- [ ] Set up the password manager's emergency access or family sharing feature

Emergency Access Features by Manager

- [ ] 1Password: Family/Teams account; share a vault; store Emergency Kit in physical safe
- [ ] Bitwarden: Emergency Access feature with trusted contact and waiting period
- [ ] Dashlane: Emergency Contact feature
- [ ] LastPass: Emergency Access feature with trusted contact and waiting period
- [ ] Keeper: Emergency Access (KeeperChat) feature

Password manager chosen and emergency access details:

2.2 -- Two-Factor Authentication (2FA) Planning

2FA protects your accounts while you are alive, but it can lock everyone out after you die if not planned for.

- [ ] Document which accounts have 2FA enabled
- [ ] Store 2FA backup/recovery codes in password manager AND physical location
- [ ] Document which authenticator app you use and what device it is on
- [ ] Consider Authy (multi-device sync) instead of Google Authenticator (device-bound)
- [ ] If you use a hardware security key (YubiKey, Titan), document its physical location and register backups
- [ ] Store your phone's passcode/PIN securely
- [ ] Document your phone carrier's account PIN/password (needed for SIM transfers)

2FA details and recovery code storage locations:

2.3 -- Device Access

- [ ] Document passcode/PIN/password for every device: phones, tablets, laptops, desktops
- [ ] Document biometric backup methods (backup PINs for Face ID / fingerprint)
- [ ] Document Apple ID or Google account password tied to each device
- [ ] Note any encrypted drives or volumes and their decryption passwords
- [ ] Record location of recovery keys for disk encryption (FileVault, BitLocker)
- [ ] If you have a NAS or home server, document its admin credentials

Device access notes:

2.4 -- Physical Storage of Access Information

- [ ] Store master password and emergency kit in fireproof safe, safe deposit box, or with attorney
- [ ] Consider splitting sensitive info (master password in one location, emergency kit in another)
- [ ] Let your executor/trusted person know WHERE this information is stored
- [ ] Review and update this information at least annually

Storage locations and trusted persons: