

Digital Legacy Checklist

A 10-Step Guide to Organizing & Securing Your Digital Estate

1. Define Your Digital Assets

- Identify what you own: Financial (banking, crypto), Social (Facebook, LinkedIn), Sentimental (iCloud, Google Photos), and Professional (domains, blogs).

2. Create a Comprehensive Inventory

- List every account and the associated email/username. Important: Do not record raw passwords in this document.

3. Appoint a Digital Executor

- Choose a tech-savvy individual specifically to handle digital logins and data. Name them explicitly in your Will or a Codicil.

4. Utilize Platform Legacy Features

- Set up Google's Inactive Account Manager, Apple's Legacy Contact, and Facebook's Memorialization Settings.

5. Implement a Password Manager

- Use a service like 1Password or Bitwarden. Ensure your Digital Executor has the Master Key or has been added as an emergency contact.

6. Solve for Two-Factor Authentication (2FA)

- Document recovery codes for accounts using SMS or App-based 2FA. Store these in a secure physical location like a safe.

7. Specify the 'Fate' of Each Asset

- Clearly label accounts for Deletion (scrubbing data), Memorialization (archiving), or Transfer (passing ownership to heirs).

8. Formalize Legal Authorization

- Ensure your legal documents grant 'explicit consent' for executors to access the content of electronic communications to bypass privacy laws.

☐ 9. Secure Physical Hardware Gateways

- Provide PIN codes and passwords for laptops, phones, and external drives. Hardware is the primary gateway to the digital world.

☐ 10. Conduct an Annual Digital Audit

- The digital landscape changes quickly. Review and update your inventory, contacts, and permissions every 12 months.

PRO TIP: Keep your digital inventory private. Unlike a Will, which becomes public during probate, a separate 'Letter of Instruction' stays private between you and your executor.