Wigington Security Group

Privacy consulting for individuals and families

Digital Estate Planning Guide

Ensuring your digital legacy is handled according to your wishes

What You'll Learn:

- Why digital estate planning is now essential
- Creating a comprehensive digital asset inventory
- Password inheritance and emergency access
- Social media legacy contacts and memorialization
- Financial account transfer procedures
- Cryptocurrency and digital asset recovery
- Legal framework and necessary documents
- Platform-by-platform legacy configuration

The Harsh Reality:

Without proper planning, your family faces:

- Locked accounts with no recovery method
- Lost cryptocurrency and digital assets
- Photos and memories permanently inaccessible
- Social media accounts as zombie profiles
- Identity theft targeting deceased accounts
- Legal battles for digital access
- Thousands in lost assets

February 2026 • 36 Pages • Free Download

wigingtonsecurity.com

Contents

1 Why Digital Estate Planning Matters

1.1 The Digital Assets You Don't Realize You Have

When people think "estate planning," they think wills, property, bank accounts. But your digital life has become equally valuable—and far more complex.

Your digital estate likely includes:

Category	Examples	Est. Value
Financial Accounts	Online banking, investment platforms, PayPal, Venmo	$10,000-$1,000,000+
Cryptocurrency	Bitcoin, Ethereum, NFTs, DeFi positions	$0-$1,000,000+
Digital Media	iTunes, Kindle books, Steam games, cloud storage	$1,000-$10,000
Photos & Memories	Google Photos, iCloud, Dropbox, phone storage	Priceless
Social Media	Facebook, Instagram, LinkedIn, Twitter/X	Varies
Domain Names	Personal websites, blogs, business domains	$10-$100,000+
Email Accounts	Gmail, Outlook, work email	Access to everything
Subscriptions	Netflix, Spotify, SaaS tools, recurring charges	$1,000-$5,000/year
Business Assets	Client lists, intellectual property, digital products	$0-$1,000,000+
Loyalty Points	Airlines, hotels, credit cards	$500-$50,000
Online Business Income	Affiliate sites, YouTube revenue, Etsy, eBay	$0-$100,000+/year

1.2 What Happens Without a Plan

CRITICAL

Real cases of digital estate disasters:

- **The locked Bitcoin:** Man dies with $200M in Bitcoin. No one has the private keys. Funds permanently lost.
- **The zombie Facebook:** Wife dies. Facebook refuses to give husband access. Memorial page created by strangers posts inappropriate content. Takes 2 years and lawyers to resolve.
- **The photo hostage:** Father dies. 30 years of family photos in Google account. No one knows the password. Google requires death certificate, court order, 6-month process. Some photos never recovered.
- **The business collapse:** Small business owner dies suddenly. All client data, passwords, financial records locked in his encrypted devices. Business dies with him. Family loses $500K/year income.
- **The identity theft:** Mother dies. Family doesn't deactivate social media for months. Scammers impersonate her, friend people she knew, run scams using her identity.

These are not rare. These happen every single day.

1.3 The Legal Complexity

Digital assets exist in a legal gray area:

- **Terms of Service:** Most platforms prohibit sharing passwords, even with family

- **CFAA:** Computer Fraud and Abuse Act makes "unauthorized access" a federal crime
- **State laws:** 47 states have passed some form of digital asset legislation
- **RUFADAA:** Revised Uniform Fiduciary Access to Digital Assets Act provides framework
- **Platform policies:** Each company has different procedures for deceased users
- **International accounts:** Different laws in different countries

The problem: Your executor has legal authority over your physical property. They do NOT automatically have authority over your digital accounts.

⚖ Legal Considerations

Legal authority hierarchy for digital assets:

1. **Platform's own tools** (legacy contacts, memorialization settings)
2. **Your explicit written instructions** (in legally valid documents)
3. **State law** (varies by state, often requires court order)
4. **Terms of Service** (what platform allows)
5. **Court order** (expensive, time-consuming, not guaranteed)

Best practice: Use platform tools + explicit legal documents + secure password sharing method.

1.4 Scope of This Guide

What we cover:

- Creating comprehensive digital asset inventory
- Platform-by-platform legacy configuration (Facebook, Google, Apple, etc.)
- Secure password and access inheritance methods
- Legal documents and necessary language
- Cryptocurrency and digital wallet succession
- Social media memorialization vs. deletion
- Business digital asset transfer
- Preventing digital identity theft after death

What we don't cover:

- Traditional estate planning (physical assets, real estate, traditional trusts)
- Specific tax implications (consult a CPA)

- Specific legal advice for your state (consult an estate attorney)
- Business succession planning beyond digital assets

Warning

This guide is not legal advice. We provide information and best practices for digital asset management. For legally binding estate planning, consult an attorney familiar with digital assets and your state's laws.
Recommendation: Use this guide to prepare, then work with an estate attorney to formalize your digital estate plan within your overall estate plan.

2 Creating Your Digital Asset Inventory

The first step is knowing what you have. Most people vastly underestimate their digital footprint.

2.1 Comprehensive Asset Categories

2.1.1 Financial Accounts

Action Checklist

List all financial accounts:

- ☐ Bank accounts (checking, savings)
- ☐ Investment accounts (brokerage, 401k, IRA)
- ☐ Credit cards
- ☐ Payment platforms (PayPal, Venmo, Cash App, Zelle)
- ☐ Cryptocurrency exchanges (Coinbase, Kraken, Binance)
- ☐ Peer-to-peer lending (LendingClub, Prosper)
- ☐ Robo-advisors (Betterment, Wealthfront)
- ☐ HSA / FSA accounts
- ☐ 529 college savings plans

For each account, document:

- Institution name and website
- Account number
- Login username/email
- Whether 2FA is enabled (and method)
- Approximate balance
- Beneficiary designation status
- Recovery email/phone

CRITICAL

Beneficiary designations trump wills:
For retirement accounts, life insurance, and many investment accounts, beneficiary designations override whatever your will says.
Action items:

- Review beneficiaries on ALL financial accounts
- Update after major life events (marriage, divorce, births, deaths)
- Keep beneficiaries current—many people have ex-spouses still listed
- Name contingent beneficiaries (in case primary predeceases you)
- Consider "Transfer on Death" (TOD) or "Payable on Death" (POD) designations

2.1.2 Cryptocurrency and Digital Assets

Action Checklist

Cryptocurrency holdings:

Exchange accounts (Coinbase, Kraken, Gemini, etc.)

Hardware wallets (Ledger, Trezor)

- Location of physical device
- PIN/passphrase
- Recovery seed phrase (24 words)
- Location of seed phrase backup

Software wallets (MetaMask, Trust Wallet)

- Recovery seed phrase
- Private keys

DeFi positions (staking, liquidity pools, lending)

NFTs and digital collectibles

Smart contract holdings

For each crypto asset, document:

- Type of asset and amount
- Where held (exchange, wallet address, hardware wallet)
- Access method (keys, seed phrases, PINs)
- Current approximate value

Warning

Cryptocurrency is UNRECOVERABLE without keys:
Unlike a bank account where an executor can eventually gain access, cryptocurrency without the private key or seed phrase is **permanently lost**. There is no "password reset" for blockchain.
Critical requirements:

- Seed phrases (12-24 words) must be documented and secured
- Hardware wallet PINs must be documented
- Private keys must be backed up
- Location of hardware wallets must be known

Common failure: Person dies, family finds hardware wallet but doesn't have PIN or seed phrase. Crypto is lost forever.

2.1.3 Email Accounts

Action Checklist

Email accounts (all of them):

Primary personal email

Secondary/backup email

Work email (note: controlled by employer)

Old email addresses still in use

Email aliases and forwarding addresses

For each email account:

- Email address
- Provider (Gmail, Outlook, ProtonMail, etc.)
- Login credentials
- Recovery email and phone
- Whether Inactive Account Manager is configured (Google)
- Approximate number of important emails/attachments

Why email matters: Email is the "master key" to your digital life. Whoever controls your email can reset passwords on nearly every other account.

2.1.4 Social Media and Online Presence

Action Checklist

Social media accounts:

Facebook

- Legacy Contact designated?
- Memorialization preferences set?

Instagram

- Connected to Facebook for legacy access?

Twitter/X

LinkedIn

TikTok

Snapchat

Reddit

YouTube

- Channel monetization status?
- Google Inactive Account Manager configured?

Pinterest

Discord servers and accounts

For each account:

- Platform and username/handle
- Associated email
- Preference: Memorialize, Delete, or Give Access
- Legacy contact designated (if platform supports)
- Approximate followers/connections (may affect monetization)

2.1.5 Photos, Videos, and Digital Memories

Action Checklist

Media storage locations:

Google Photos

- Number of photos/videos
- Storage used
- Inactive Account Manager configured?

iCloud Photos

- Storage used
- Legacy Contact designated?
- Devices syncing to iCloud

Dropbox, OneDrive, Box

Amazon Photos (Prime members)

Phone local storage

Computer hard drives

External hard drives / NAS devices

- Physical location
- Encryption password (if encrypted)

Old USB drives, memory cards

CDs/DVDs with photos

Document:

- Where originals are stored
- Where backups exist
- Any encryption/passwords
- Whether family knows how to access

Critical consideration: Photos are often the most emotionally valuable digital asset. Ensure multiple backups and clear access instructions.

2.1.6 Subscriptions and Digital Purchases

Action Checklist

Paid subscriptions:

- Streaming services (Netflix, Hulu, Disney+, HBO, Spotify)
- Cloud storage (Google One, iCloud+, Dropbox)
- Software subscriptions (Adobe, Microsoft 365, etc.)
- News subscriptions
- Fitness/health apps
- Password manager subscription
- VPN service
- Web hosting and domain renewals
- Professional associations/memberships

Digital purchases:

- iTunes/Apple purchases (music, movies, apps)
- Kindle books
- Audible audiobooks
- Steam/gaming library
- In-game purchases and virtual items

For each subscription/purchase:

- Service name
- Monthly/annual cost
- Payment method on file
- Whether family should continue or cancel
- Account value (e.g., $2,000 worth of Kindle books)

Pro Tip

Why subscription inventory matters:
Family members need to know what's billing automatically after you're gone:

- Cancel unnecessary subscriptions to stop charges
- Continue valuable subscriptions (cloud storage with photos)
- Access purchased content before accounts are closed
- Prevent recurring charges from draining estate

Note: Most digital purchases (movies, books, games) are *licensed*, not owned. They cannot be transferred to heirs and will be lost when account closes.

2.1.7 Domain Names and Websites

Action Checklist

Domain registrations:

- [ ] Personal domain names
- [ ] Business domains
- [ ] Investment/parked domains
- [ ] Expired domains you still care about

Websites and hosting:

- [ ] Personal websites/blogs
- [ ] Business websites
- [ ] Hosting accounts (Bluehost, GoDaddy, etc.)
- [ ] Website builders (Squarespace, Wix, WordPress.com)
- [ ] Content Management System logins

For each domain/site:

- Domain name(s)
- Registrar (where domain is registered)
- Hosting provider (where site is hosted)
- Renewal dates
- Estimated value (if domain is valuable)
- FTP/SFTP credentials
- Database credentials
- Content Management System login
- Preference: Keep online, take offline, transfer to someone

Premium domains can be worth thousands or millions. Ensure family knows which domains are valuable and that they don't expire.

2.1.8 Business and Income-Generating Assets

Action Checklist

Online business assets:

- E-commerce stores (Shopify, Etsy, eBay, Amazon FBA)
- Affiliate marketing sites
- YouTube channels (monetized)
- Blogs with ad revenue
- Online courses and digital products
- Freelance platform accounts (Upwork, Fiverr)
- Stock photography portfolios
- App Store / Play Store apps
- SaaS products

For each business asset:

- Platform and account details
- Current revenue (monthly/annual)
- Customer/client lists location
- Outstanding orders or commitments
- Contractor/employee access
- Business value estimate
- Transfer/sale instructions or contacts

CRITICAL

Business continuity requires immediate access:
If you run an online business:

- Revenue stops immediately if no one has access
- Customer orders go unfulfilled
- Employees/contractors can't get paid
- Reputation damage from abandoned customers
- Business value evaporates quickly

Solution: Designate a trusted person with technical ability who can:

1. Access accounts immediately
2. Communicate with customers
3. Fulfill or refund orders
4. Either continue business or orderly shutdown
5. Transfer/sell business if desired

2.1.9 Loyalty Programs and Rewards

Action Checklist

Points and miles:

Airline frequent flyer programs

Hotel loyalty programs

Credit card reward points

Retail loyalty programs

For each program:

- Program name and member number
- Approximate points/miles balance
- Estimated cash value
- Transferability rules (many programs prohibit transfer)
- Whether points can be used by survivors before account closure

Reality check: Most loyalty programs expire or cancel points upon death. Act quickly to use valuable points before airline/hotel learns of death.

2.2 Digital Asset Inventory Template

Download our comprehensive spreadsheet template:

Columns to include:

- Asset Category
- Platform/Service Name
- Account ID / Username
- Email Associated
- Website / URL
- Approximate Value
- 2FA Method (if enabled)
- Recovery Email
- Recovery Phone
- Legacy Contact / Designated Person (if configured)
- Preference on Death (Memorialize / Delete / Transfer)
- Notes
- Last Updated

Storage location:

- **DO:** Keep in password manager secure notes
- **DO:** Print and store in safe/safety deposit box with will
- **DO:** Update quarterly
- **DON'T:** Email to yourself
- **DON'T:** Store unencrypted on computer
- **DON'T:** Put in cloud storage without encryption

3 Platform-by-Platform Legacy Configuration

Most major platforms now offer legacy features. Configure them *before* they're needed.

3.1 Google Accounts (Gmail, Photos, Drive, YouTube)

Google Inactive Account Manager

This is Google's solution for account inheritance.

Setup path: https://myaccount.google.com/inactive

Action Checklist

Configuration steps:

Set timeout period: 3, 6, 12, or 18 months of inactivity

- Recommended: 3-6 months (shorter if high-risk situation)

Add up to 10 trusted contacts

- These people get notified before timeout
- They can receive access to your data

Decide what to share:

- You can share all data or select specific services
- Gmail, Drive, Photos, Calendar, etc.
- Or share nothing and just have account deleted

Set notification preferences:

- Google sends warning before timeout (via email and SMS)
- Gives you chance to cancel if you're still alive

Choose what happens after data is shared:

- Delete account after sharing
- Or keep account memorialized

What trusted contacts receive:

- Email notification that account is inactive
- Link to download your data (if you enabled sharing)
- Access for 3 months to download data
- Data comes in Google Takeout format (archive files)

Pro Tip

Best practices:

- Use shorter timeout (3 months) if you want quick access for family
- Choose trusted contacts who are tech-savvy enough to download/use data
- Test the system: Have a trusted contact verify they have your correct email
- Update contacts if life circumstances change (divorce, death, estrangement)
- Include both local and remote contacts (in case of shared disaster)

Limitations:

- Requires you to be inactive (not helpful if you die suddenly but phone keeps auto-checking email)
- Contacts get download, not live account access
- Some Google services excluded (Payments, some business features)
- No inheritance of Google Play purchases or subscriptions

3.2 Apple / iCloud

Apple Legacy Contact

Introduced in iOS 15.2 / macOS 12.1.
Setup path: Settings → [Your Name] → Password & Security → Legacy Contact

Action Checklist

Configuration steps:

Add Legacy Contact:

- Choose from your contacts
- Or generate shareable code for someone not in contacts

Legacy Contact receives notification

- They must accept on their Apple device
- They receive an Access Key (save it!)

You can add multiple Legacy Contacts

Print Legacy Contact Access Key

- Contact needs this + your death certificate to gain access
- Store printed key with your will

What Legacy Contact can access after death:

- iCloud Photos

- Notes
- Files stored in iCloud Drive
- Messages backed up to iCloud
- Contacts
- Calendar
- Reminders
- Safari bookmarks
- Health data (if backed up)
- Home data

What Legacy Contact CANNOT access:

- iCloud Keychain (passwords)
- Payment information
- Licensed media (movies, music, books, apps)
- iCloud Mail

How Legacy Contact claims access:

1. Visit https://digital-legacy.apple.com
2. Provide Access Key
3. Upload death certificate
4. Apple reviews (can take days to weeks)
5. Once approved, access granted for 3 years
6. Data can be downloaded

Warning

Critical limitations:
Legacy Contact does NOT get:

- Your Apple ID password
- Access to your iTunes/App Store purchases
- Access to iCloud email
- Access to saved passwords

For complete access, you need both Legacy Contact *and* password inheritance (see Section 4).

3.3 Facebook

Facebook has two options: Legacy Contact or Account Deletion upon death.

Setup path: Settings & Privacy → Settings → Personal details → Account ownership and control → Memorialization settings

Reference: https://www.facebook.com/help/1506822589577997

3.3.1 Option 1: Legacy Contact

Action Checklist

Designating a Legacy Contact:

- Choose a Facebook friend as Legacy Contact
- Send them a message explaining your choice
- They receive notification of designation

What Legacy Contact can do after your death:

- Write a pinned post on your memorialized profile (like a tribute)
- Respond to new friend requests
- Update profile picture and cover photo
- Request removal of your account
- Download an archive of your posts, photos, videos, and profile info

What Legacy Contact CANNOT do:

- Log in as you
- Read your messages
- Remove or change past posts
- Remove friends
- See anything you posted privately to specific people

Memorialized account features:

- Word "Remembering" appears before your name
- No one can log into memorialized account
- Profile is visible according to your privacy settings
- Posts you shared (photos, videos, timeline posts) remain visible to audience they were shared with
- Account cannot be changed (except by Legacy Contact's limited permissions)
- Memorialized profiles don't appear in public spaces (suggestions, ads, birthday reminders)

3.3.2 Option 2: Account Deletion

Instead of memorialization, you can request account be deleted upon death.

Action Checklist

Settings → Memorialization settings

Select "Request that your account be deleted after you pass away"

Confirm your choice

What happens:

- After Facebook receives valid proof of death, account is permanently deleted
- All content is removed
- No one can access the account
- Family cannot request memorialization if you chose deletion

How Facebook learns of death:

- Family/friends submit request via https://www.facebook.com/help/contact/234739086860192
- Provide link to obituary or news article
- OR submit death certificate
- Facebook reviews and processes request

Pro Tip

Choosing between memorialization and deletion:
Choose memorialization if:

- You want profile to serve as memorial
- You have significant photos/posts family wants preserved
- You want timeline to remain accessible to friends/family
- You trust your Legacy Contact to manage it appropriately

Choose deletion if:

- You prefer no digital afterlife
- Privacy is paramount
- You don't want strangers posting on your wall after death
- You have limited Facebook presence anyway

Most people choose: Memorialization with trusted Legacy Contact.

3.4 Instagram

Instagram is owned by Meta (Facebook). Legacy options are more limited.

Reference: https://www.facebook.com/help/instagram/264154560391256

Two options:

1. **Memorialization:** Account turns into memorial, no one can log in
2. **Deletion:** Account permanently removed

Important: Instagram does NOT have a Legacy Contact feature like Facebook. If you've designated a Legacy Contact on Facebook, they do NOT automatically get Instagram access.

How to request memorialization or deletion (by family):

1. Visit: https://www.facebook.com/help/instagram/contact/452224988254813
2. Choose "Memorialize an account" or "Remove an account"
3. Provide:
   - Deceased person's Instagram username or URL
   - Proof of death (death certificate, obituary link, news article)
   - Your relationship to deceased
   - Your contact information
4. Instagram reviews and processes

Memorialized Instagram accounts:

- Word "Remembering" appears in profile
- No one can log in
- Existing posts and photos remain visible to followers
- Account will not appear in Explore, recommendations, or ads
- Direct messages remain private (no one can access them)
- Account cannot be modified

Planning ahead: Since Instagram has no Legacy Contact feature, if you want someone to access your account:

- You must share password with trusted person (see Section 4 on password inheritance)
- Designate someone in your will/digital estate plan to handle Instagram
- Consider downloading your Instagram data while alive (Settings → Your Activity → Download Your Information)

3.5 Twitter / X

Twitter does NOT have legacy contact or memorialization features.

Reference: https://help.twitter.com/en/rules-and-policies/contact-twitter-about-a-deceased-

Only option: Deactivation (deletion) of deceased user's account.

Process for family to deactivate account:

1. Email privacy@twitter.com with subject "Deceased User"
2. Provide:
   - Your full name
   - Contact information (email, phone)
   - Username of deceased person
   - Copy of death certificate
   - Copy of your valid ID showing you're authorized person
3. Twitter reviews (can take weeks)
4. If approved, account is deactivated

Account deactivation means:

- Account is suspended for 30 days
- After 30 days, permanently deleted
- All tweets, photos, followers removed
- Username may become available for others to claim
- No way to recover data after deletion

Planning ahead:

- Download your Twitter archive while alive (Settings → Your account → Download an archive)
- Consider whether you want account preserved or deleted
- If preservation important, share credentials with trusted person (risky, violates ToS)
- Or use third-party archiving service to preserve tweets
- Document your wishes in digital estate plan

Warning

Twitter/X has the worst digital legacy support of major platforms:

- No memorialization
- No legacy contacts
- No way to preserve account
- Deletion is only option
- Process is slow and frustrating for family

If your Twitter presence is important (public figure, business account, large following), plan ahead by:

1. Regularly downloading Twitter archive
2. Using third-party backup services
3. Sharing credentials via secure password inheritance method
4. Documenting wishes for account in estate plan

3.6 LinkedIn

LinkedIn removes profiles of deceased members.

Reference: https://www.linkedin.com/help/linkedin/answer/2842

Process:

1. Immediate family member or executor contacts LinkedIn
2. Use form: https://www.linkedin.com/help/linkedin/answer/2842
3. Provide:
   - Deceased member's profile URL
   - Proof of death (death certificate, obituary)
   - Relationship to deceased
   - Your contact information
4. LinkedIn closes account

What happens:

- Account is permanently closed
- Profile is removed from LinkedIn
- Connections are notified (optional)
- No memorialization option

- No data access for family

Planning ahead:

- Download your LinkedIn data (Settings → Data privacy → Get a copy of your data)
- Consider whether you want quick deletion or want account to remain briefly
- Professional connections may want to know of your passing—consider having someone post announcement before account closes

3.7 Other Platforms (Quick Reference)

Platform	Legacy Option	Process
TikTok	Deletion only	Family submits request with death certificate
Snapchat	Deletion only	Contact support with death certificate
Reddit	Deletion only	Email contact@reddit.com with death certificate
Discord	Deletion only	Contact support, provide proof of death
Pinterest	Memorialization or deletion	Submit request to help@pinterest.com
Spotify	Account closure	Contact support with death certificate
Netflix	Cancel subscription	Family can contact support to cancel
Amazon	Account closure	Call customer service with death certificate
PayPal	Account closure	Contact with death certificate, remaining funds can be withdrawn by estate
Venmo	Account closure	Contact support, provide documentation
Dropbox	Account closure after 90 days	No legacy features; download data before account closes
Microsoft/Outlook	Next of Kin Process	Submit request at https://support.microsoft.com, provide death certificate, get access or closure
Yahoo	Deceased User Account Termination	Submit form with death certificate, account will be closed (no data access)

4 Password Inheritance and Emergency Access

Platform legacy features are helpful but limited. Complete digital access requires password inheritance.

4.1 The Password Inheritance Dilemma

The problem:

- You need someone to access accounts if you die
- But giving someone your passwords while alive is a security risk
- Writing down passwords and storing them can lead to unauthorized access
- Not planning means family is locked out forever

The solution: Use secure emergency access features in password managers.

4.2 Password Manager Emergency Access

All major password managers now offer emergency access features.

4.2.1 1Password Emergency Kit

1Password uses "Emergency Kit" - a PDF with account info.

What it contains:

- Your account email
- Secret Key (unique to your account)
- QR code for quick setup
- Space to write master password (on printed copy only)

Setup:

Action Checklist

- [ ] Download Emergency Kit PDF when setting up account
- [ ] Print two copies
- [ ] Write your master password on printed copies (NOT digital PDF)
- [ ] Store in two separate secure locations:
  - Copy 1: Home safe or locked drawer
  - Copy 2: Safety deposit box or with estate attorney
- [ ] Delete digital PDF (security risk if unencrypted)
- [ ] Tell executor/trusted person where Emergency Kits are stored
- [ ] Update Emergency Kits if you change master password

Family recovery process:

1. After your death, trusted person retrieves Emergency Kit
2. Uses Emergency Kit + master password to log into your 1Password
3. Gains access to all your passwords and secure notes
4. Can access all your accounts

Pros:

- Simple, no special configuration needed
- Works immediately
- Complete access to all passwords

Cons:

- Master password is written down (physical security risk)
- No time delay or notification if someone uses it
- Requires physical access to Emergency Kit

4.2.2 Bitwarden Emergency Access

Bitwarden has dedicated emergency access feature (Premium feature).

Setup path: Settings → Emergency Access

Action Checklist

Configuration:

Add trusted emergency contact (email required)

They receive invitation and must accept

Set wait time: 0 days, 1 day, 2 days, 7 days, 14 days, 30 days, 90 days

- Recommended: 7-30 days for balance of access and security

Choose access level:

- View: They can view passwords but not change them
- Takeover: They can reset your master password and take full control

Can add multiple emergency contacts with different wait times

How it works:

1. Emergency contact initiates emergency access request
2. You receive email and in-app notification

3. Wait time countdown begins
4. If you don't reject during wait time, access is granted
5. If you're deceased, wait time expires and contact gets access
6. If you're alive but don't respond, you can reject even during wait time

Pros:

- No passwords written down
- Notification if someone requests access (prevents abuse while alive)
- Can set appropriate wait time based on circumstances
- Contact doesn't need death certificate or legal documents
- Works across all devices

Cons:

- Requires Premium subscription ($10/year)
- Emergency contact must have Bitwarden account
- Assumes you'll be unable to reject request (if incapacitated but alive, could grant unintended access)

4.2.3 LastPass Emergency Access

Similar to Bitwarden.

Setup path: Account Settings → Emergency Access

☑ Action Checklist

- Add trusted contact (email required)
- Contact must have LastPass account (free is fine)
- Set wait time (1-30 days or instant)
- Choose: View access or Full access

Process is same as Bitwarden—request, wait period, automatic grant if not rejected.

4.2.4 KeePassXC Manual Method

KeePassXC doesn't have built-in emergency access (it's offline-only).

Options:

1. **Database + Master Password method:**
   - Store KeePassXC database file in accessible location (Dropbox, Google Drive, USB drive)
   - Write master password on paper, store in safe/with will

- Tell trusted person where database and password are

2. **Shared Secret Method:**
   - Use Shamir's Secret Sharing to split master password
   - Requires multiple people to reconstruct password
   - Complex but very secure
3. **Key File Method:**
   - KeePassXC can use key file + password
   - Store key file separately from password
   - Trusted person needs both to access

4.3 Secure Password Documentation Methods

If not using password manager emergency access, you need secure documentation method.

4.3.1 The Sealed Envelope Method

Action Checklist

Traditional approach:

Write critical passwords on paper

Include:

- Email account passwords
- Password manager master password
- Phone/computer unlock codes
- Cryptocurrency seed phrases

Seal in envelope

Sign across seal (so you can detect if opened)

Store in safety deposit box or with attorney

Include in will: "Password envelope is in safety deposit box at [bank]"

Pros:

- No technology required
- Survives digital disasters
- Attorney can verify envelope is sealed
- Clear chain of custody

Cons:

- Must update whenever passwords change
- Risk of envelope being opened (curious attorney, bank employee)
- Fire/flood can destroy
- Requires physical access

4.3.2 The Split Knowledge Method

Action Checklist

Divide information among multiple people:

Person A gets: List of accounts + usernames

Person B gets: Passwords for those accounts

Both must collaborate to access accounts

Neither person alone has complete access

Variation: Three-person split

- Person A: Account list
- Person B: Passwords
- Person C: 2FA backup codes
- Requires all three to fully access accounts

Pros:

- No single point of failure
- Prevents unauthorized access by one person
- Checks and balances

Cons:

- Complex coordination required
- If one person unavailable, access delayed/impossible
- Requires multiple trusted people

4.4 What Passwords Family Absolutely Needs

Prioritize which passwords to make accessible:

Action Checklist

Critical - Must Have:

- Primary email account
- Password manager master password
- Phone unlock code
- Computer login password

Important - Should Have:

- Bank account logins
- Investment account logins
- Cryptocurrency wallet keys/seed phrases
- Cloud storage (Google Drive, iCloud, Dropbox)
- PayPal/payment platforms

Nice to Have:

- Social media accounts
- Subscription services
- Shopping accounts

Strategy: Focus on master password + email. With those two, family can reset most other passwords.

5 Cryptocurrency and Digital Wallet Succession

Cryptocurrency requires special attention. It's the 1 digital asset that's permanently lost.

5.1 The Cryptocurrency Succession Problem

Key facts:

- Cryptocurrency is controlled by private keys, not institutions
- No "password reset" for blockchain
- No customer service to call if you lose access
- If private key is lost, cryptocurrency is **permanently, irretrievably gone**
- Estimated $140 billion in Bitcoin alone is lost forever (2026 estimate)
- Most losses are from death or incapacitation without key backup

CRITICAL

Without proper planning, your cryptocurrency will be lost forever:
Common scenarios:

1. Person dies with Bitcoin on hardware wallet. Family finds wallet but doesn't have PIN or seed phrase. Bitcoin lost forever.
2. Person has seed phrase written down, but family doesn't know what it is or where it's stored. Found years later, too late.
3. Seed phrase stored digitally in encrypted file. Family doesn't have password to decrypt. Bitcoin lost.
4. Person uses complex multi-signature wallet. Family doesn't understand how to access. Bitcoin lost.
5. Person dies with crypto on exchange. Exchange requires death certificate, ID, legal documents. After months of process, account is frozen indefinitely due to "security concerns." Family never gets access.

All of these are real cases. All resulted in permanent loss of hundreds of thousands to millions of dollars.

5.2 Types of Cryptocurrency Storage

5.2.1 Exchange Accounts (Coinbase, Kraken, Binance, etc.)

What it is: Cryptocurrency stored in account on centralized exchange (like a bank).
Access method: Username + password + 2FA
Succession planning:

Action Checklist

- [ ] Include exchange logins in password manager
- [ ] Document 2FA method (authenticator app, SMS, hardware key)
- [ ] Save 2FA backup codes in secure location
- [ ] Check exchange's policy on deceased accounts:
  - Coinbase: Has specific process for estate claims
  - Kraken: Requires legal documentation
  - Binance: Varies by jurisdiction
- [ ] Include exchange accounts in will/estate plan
- [ ] Consider moving to personal wallet for full control

Pros:

- Exchange may have estate recovery process
- Similar to traditional financial account
- Can potentially recover with legal documents

Cons:

- Exchange can freeze/seize assets
- Recovery process is slow and uncertain
- Exchange bankruptcy could wipe out holdings
- "Not your keys, not your crypto"

5.2.2 Hardware Wallets (Ledger, Trezor)

What it is: Physical device that stores private keys offline. Most secure storage method.
Access method: Physical device + PIN + seed phrase (24 words)
Succession planning:

Action Checklist

Document location of hardware wallet device

- Exact location: "In safe, top drawer, under passports"
- Include photo of device so family knows what to look for

Document wallet PIN

- Store separately from device (not with the wallet!)
- Include in password manager or sealed envelope with attorney

CRITICAL: Document 24-word seed phrase

- This is the master key to all cryptocurrency
- Must be exact words in exact order
- Store in multiple secure locations
- NEVER store digitally (photo, cloud, email)

Document which cryptocurrencies are on wallet

Document approximate amounts (for estate valuation)

Include instructions for accessing:

- "Connect device to computer"
- "Enter PIN: [see password manager]"
- "OR restore from seed phrase: [see safety deposit box]"

Seed phrase storage methods:

1. **Metal backup plate:** Stamp or engrave words onto metal
   - Fireproof, waterproof, extremely durable
   - Products: Cryptosteel, Billfodl
   - Store in safe or safety deposit box
2. **Paper backup (multiple copies):**
   - Write seed phrase on acid-free paper
   - Laminate for water protection
   - Store in fireproof safe
   - Keep copy in safety deposit box
   - Keep copy with estate attorney
3. **Shamir Backup (advanced):**
   - Split seed into multiple shares (e.g., 3 of 5 required)
   - Give different shares to different trusted people

- Requires any 3 shares to reconstruct seed
- Supported by Trezor Model T

Warning

Seed phrase security is paramount:
DO:

- Write on paper or stamp on metal
- Store in multiple physical locations
- Keep separate from hardware wallet itself
- Check annually that you can read/access it

NEVER:

- Take photo of seed phrase
- Store in cloud (iCloud, Google Drive, Dropbox)
- Email to yourself
- Save as digital file on computer
- Store in password manager (controversial—some argue encrypted password manager is OK)

Anyone with your seed phrase can steal all your cryptocurrency. But without seed phrase, it's lost forever. This is the dilemma.

5.2.3 Software Wallets (MetaMask, Trust Wallet, Exodus)

What it is: App on phone or computer that stores private keys.
Access method: App password + seed phrase
Succession planning:

Action Checklist

- [ ] Document which wallet app (MetaMask, Trust Wallet, etc.)
- [ ] Document app password/PIN
- [ ] Document 12 or 24-word seed phrase (most critical)
- [ ] Document which phone/computer wallet is installed on
- [ ] Export and save private keys (if wallet allows)
- [ ] List wallet addresses (for verification)
- [ ] List which cryptocurrencies and amounts

Additional considerations:

- Software wallets are less secure than hardware wallets
- If phone/computer dies, only way to recover is seed phrase
- Emphasize seed phrase storage even more than hardware wallets

5.2.4 Multi-Signature Wallets

What it is: Wallet requiring multiple signatures to move funds (e.g., 2 of 3 keys required).
Common use: Business accounts, large holdings, inheritance planning
Succession planning:

☑ Action Checklist

- Document multi-sig structure (e.g., "2 of 3 required")
- List all key holders
- Document where each key is stored
- Ensure at least [threshold] keys are accessible to heirs
  - For 2 of 3: At least 2 keys must be recoverable
- Document recovery process (which software, which blockchain)
- Test recovery process while alive

Advantage: Can structure for inheritance (you hold 1 key, trusted person holds 1 key, backup key in safe)

5.3 Cryptocurrency Succession Best Practices

Action Checklist

Do this for all cryptocurrency holdings:

Create comprehensive inventory:

- Which cryptocurrencies you own
- Approximate amounts
- Where stored (exchange, hardware wallet, software wallet)
- Wallet addresses
- Access methods for each

Secure seed phrases:

- Metal backup or multiple paper copies
- Multiple secure physical locations
- Never digital unless encrypted in password manager

Document everything:

- Step-by-step instructions for accessing each wallet
- Screenshots if helpful
- Simple language (assume family has no crypto knowledge)

Designate crypto-savvy person:

- Choose someone who understands cryptocurrency
- Give them your crypto documentation in estate plan
- Consider paying them percentage to help family recover funds

Test recovery process:

- Set up test wallet with small amount
- Walk trusted person through recovery process
- Verify they can actually access it
- Do this annually

Update documentation:

- When you acquire new cryptocurrency
- When you move between wallets/exchanges
- When balances change significantly
- At least annually

Include in legal documents:

- Will mentions "cryptocurrency holdings as documented in [secure location]"
- Executor is authorized to access digital assets
- Designate specific person to handle crypto if executor isn't tech-savvy

Pro Tip

The inheritance wallet approach:
Some cryptocurrency holders set up dedicated "inheritance wallet":

1. Create new hardware wallet
2. Transfer inheritance amount to it (10%, 25%, 50%)
3. Seal seed phrase in envelope with attorney
4. Keep hardware wallet itself with executor
5. Neither can access alone, but together they can
6. Main holdings remain in your secure wallet
7. Inheritance portion is clearly designated and recoverable

This provides clean separation between active trading and inheritance amounts.

5.4 Tax Considerations

Legal Considerations

Cryptocurrency is property for tax purposes:

- Estate must report cryptocurrency holdings for estate tax purposes
- Heirs receive "step-up in basis" (cost basis = value on date of death)
- Future sales by heirs only taxed on gains after inheritance
- Executor needs cost basis information (what you paid) for tax reporting

Document for taxes:

- Purchase dates and prices (cost basis)
- Current holdings and values
- Transaction history if possible
- Exchange reports (Coinbase sends tax forms)

Consult a CPA specializing in cryptocurrency for specific guidance.

6 Legal Framework and Documents

Digital assets need to be addressed in your estate planning documents.

6.1 Why Standard Wills Are Not Enough

Traditional wills were written before the digital age. They typically say:

- "I leave all my property to..."
- "My executor shall have authority over my estate..."

The problem:

- "Property" isn't defined to clearly include digital assets
- Executor authority is ambiguous for online accounts
- Terms of Service may prohibit access by third parties
- Computer Fraud and Abuse Act makes "unauthorized access" potentially criminal
- Some states require explicit authorization for digital asset access

Result: Executor may have no legal authority to access your email, social media, cloud storage, or cryptocurrency.

6.2 Essential Legal Documents

6.2.1 Digital Asset Addendum to Will

What it is: Separate section in will or standalone document that specifically addresses digital assets.

Recommended language to include:

⚖ Legal Considerations

Sample Digital Asset Provision:
"I hereby authorize my executor to access, manage, distribute, and dispose of my digital assets and electronic communications, including but not limited to:

- *Email accounts and all messages therein*
- *Social media accounts and content*
- *Cloud storage accounts and all stored data*
- *Cryptocurrency and digital currency holdings*
- *Domain names and websites*
- *Digital media purchases and subscriptions*
- *Online financial accounts*
- *Any other digital content or accounts*

My executor shall have full legal authority to access these assets, including the right to obtain usernames, passwords, and any other authentication credentials necessary for access. This authorization complies with the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA) and any applicable state laws.
Specific instructions for digital assets are maintained in a separate document titled 'Digital Estate Plan' stored with my estate attorney and in [location]."

Why this matters: Explicit authorization overcomes Terms of Service restrictions and CFAA concerns. It gives executor clear legal authority.

6.2.2 Digital Estate Plan Document

Separate from will, this is the detailed instruction manual.

Should include:

Action Checklist

Digital Estate Plan Contents:

Asset Inventory (from Section 2)

- Complete list of all digital assets
- Account names, websites, usernames
- Approximate values

Access Information

- Location of password manager
- Master password (or reference to where it's stored)
- Recovery codes and 2FA backup codes
- Seed phrases for cryptocurrency

Disposition Instructions

- Which accounts to close
- Which to memorialize
- Which to transfer
- Specific wishes for social media

Key Contacts

- Legacy contacts already designated
- Cryptocurrency expert to assist
- Web hosting support contacts
- Important online business contacts

Priority Actions

- "First, access email to prevent password resets"
- "Second, secure cryptocurrency holdings"
- "Third, download photos from Google Photos"
- Etc.

Business Continuity (if applicable)

- How to handle ongoing business
- Client communication templates
- Refund/closure procedures

Storage locations:

- Original: With estate attorney

- Copy 1: In home safe or secure location
- Copy 2: With executor
- Digital copy: Encrypted in password manager secure notes

Update schedule: Review and update every 6-12 months or after major life changes.

6.2.3 Power of Attorney for Digital Assets

What it is: Legal document granting someone authority over your digital assets while you're incapacitated (but not yet deceased).

Why it matters:

- If you're in coma, vegetative state, severe dementia
- Someone needs to manage your accounts
- Standard power of attorney may not cover digital assets

Recommended: Include digital asset authority in your Durable Power of Attorney.

Sample language:

⚖ Legal Considerations

"My agent is authorized to access, manage, and control my digital assets and electronic communications, with the same authority I would have, including but not limited to email accounts, social media, online financial accounts, cryptocurrency holdings, and cloud storage. This includes authority to obtain passwords and authentication credentials as necessary."

6.3 State-Specific Laws

6.3.1 RUFADAA States

47 states have adopted some version of the Revised Uniform Fiduciary Access to Digital Assets Act.

What RUFADAA does:

- Gives executors default authority over digital assets
- BUT platform tools override (legacy contacts take precedence)
- Prioritizes user's expressed wishes
- Provides legal framework for fiduciary access

Hierarchy under RUFADAA:

1. User's online tool designation (legacy contact, inactive account manager)
2. User's will or trust directive
3. Terms of service (if no user directive)

Best practice: Use both platform tools AND will provisions for redundancy.

6.3.2 Non-RUFADAA States

As of 2026, only a few states haven't adopted RUFADAA:

- Oklahoma
- Louisiana (has its own unique law)
- Massachusetts (pending)

If you live in non-RUFADAA state: Even more important to have explicit will provisions and platform legacy tools configured.

6.4 Working with an Estate Attorney

Action Checklist

Questions to ask your estate attorney:

Are you familiar with digital asset planning?

Have you drafted digital asset provisions before?

Does my current will include digital asset authority?

How does our state's RUFADAA adoption affect this?

Should digital asset plan be in will or separate document?

Where should I store password information legally?

How do we handle cryptocurrency specifically?

What about business digital assets vs. personal?

If attorney isn't familiar with digital assets:

- Provide them with this guide
- Ask them to research RUFADAA in your state
- Consider finding attorney who specializes in technology and estates
- Or use their services for traditional estate planning + add digital provisions yourself

Cost: Adding digital asset provisions to existing estate plan typically costs $200-$500. Full estate plan with digital assets: $1,000-$3,000.

7 Ongoing Management and Maintenance

Creating your digital estate plan is step one. Maintaining it is just as critical.

7.1 Update Triggers

Update your digital estate plan when:

☑ Action Checklist

You acquire significant new digital assets

- New cryptocurrency holdings
- Online business launched
- Large investment in digital media

You change password managers

You designate or change legacy contacts

Life events:

- Marriage or divorce
- Birth of children
- Death of designated legacy contact
- Major health diagnosis

You close or open significant accounts

Your master passwords change

Cryptocurrency seed phrases change

Annually (scheduled review)

7.2 Annual Review Process

Schedule: Set calendar reminder for same date each year (birthday, January 1st, etc.)

Action Checklist

Annual digital estate review tasks:

Review and update digital asset inventory

- Add new accounts
- Remove closed accounts
- Update valuations

Verify all legacy contacts are still appropriate

- Are they still alive and capable?
- Is your relationship still strong?
- Do they still have your current contact info?

Test password manager emergency access

- If using Bitwarden, have trusted person initiate test request (then cancel)
- Verify you receive notification

Verify seed phrase storage

- Can you physically access all copies?
- Are they still readable?
- Are they in secure locations?

Update documentation

- New accounts added
- Closed accounts removed
- Changed passwords noted
- New instructions for new platforms

Review platform legacy settings

- Google Inactive Account Manager still configured?
- Facebook Legacy Contact still designated?
- Apple Legacy Contact still valid?

Verify executor still has current information

- Do they know where documents are?
- Do they have updated contact info for you?

7.3 Communicating with Your Executor/Family

They need to know:

Action Checklist

That you have a digital estate plan

Where the plan is stored

Basic overview of your digital assets

- Don't need to know passwords now
- But should know "I have cryptocurrency" or "I have online business"

Who to contact for help (crypto expert, tech-savvy friend)

How to access the plan (safety deposit box key, attorney contact)

That you keep it updated

Sample conversation:

> *"I want you to know that I've created a digital estate plan. It covers all my online accounts, passwords, cryptocurrency, and digital assets. The plan is stored with my estate attorney [Name] and in my safety deposit box at [Bank]. You're designated as my executor, and you'll have full authority to access these assets if something happens to me. I keep it updated annually, so it will reflect my current situation. If you need help with technical stuff, I've designated [Tech-Savvy Friend] to assist. Do you have any questions about this?"*

Don't overshare: They don't need passwords now. They just need to know the plan exists and how to access it when needed.

7.4 Testing Your Plan

The ultimate test: Can someone actually follow your instructions?

Action Checklist

Test procedure (every 2-3 years):

Give your executor/trusted person access to digital estate plan

Ask them to:

- Read through it
- Identify anything confusing
- Try to locate password manager (without opening it)
- Verify they understand process

Update plan based on their feedback

Simplify instructions where they struggled

Add clarifying details where needed

Red flags during test:

- "I have no idea what this means"
- "Where would I even start?"
- "I couldn't find the password manager"
- "What's a seed phrase?"

Fix: Rewrite instructions at simpler level. Add screenshots. Provide glossary.

8 Conclusion and Action Plan

8.1 The Stakes

Digital estate planning isn't about being morbid. It's about:

- **Protecting your family** from losing valuable assets
- **Preserving memories** (photos, messages, content)
- **Preventing identity theft** of deceased accounts
- **Honoring your wishes** for digital afterlife
- **Making a difficult time easier** for those you leave behind

The cost of inaction:

- Millions in lost cryptocurrency (happening daily)
- Decades of family photos permanently inaccessible
- Businesses that collapse because no one has access
- Identity theft targeting deceased persons
- Zombie social media accounts posting inappropriate content
- Families fighting platforms for years to get access

8.2 Your Action Plan

This month:

☑ Action Checklist

Week 1: Create digital asset inventory

Week 2: Configure platform legacy features

- Google Inactive Account Manager
- Apple Legacy Contact
- Facebook Legacy Contact

Week 3: Set up password manager emergency access

Week 4: Secure cryptocurrency access information

Next quarter:

Action Checklist

- [ ] Schedule consultation with estate attorney
- [ ] Add digital asset provisions to will
- [ ] Create formal Digital Estate Plan document
- [ ] Store documents in secure locations
- [ ] Communicate plan to executor/family

Ongoing:

Action Checklist

- [ ] Update plan after major life events
- [ ] Annual review and update
- [ ] Test plan every 2-3 years
- [ ] Keep executor informed of changes

8.3 Final Thoughts

Digital estate planning is now essential, not optional.

The average person has:

- $50,000-$200,000+ in digital assets
- 10-20 years of irreplaceable photos
- Critical financial and personal information
- Online businesses or income streams
- Social connections and legacy

Without a plan, all of this can be lost in an instant.

The time to plan is now, while you're healthy and capable. Don't leave your family struggling to piece together your digital life while they're grieving.

CRITICAL

Start today. Your family will thank you.
Pick one task from the action plan and do it today:

- Set up Google Inactive Account Manager (15 minutes)
- Designate Apple Legacy Contact (5 minutes)
- Enable password manager emergency access (10 minutes)
- Start your digital asset inventory (30 minutes)

One small step today prevents a crisis tomorrow.

8.4 Additional Resources

WigSec Services:

- Digital Estate Planning Consultation ($200)
- Complete Digital Estate Plan Creation ($500)
- Annual Digital Estate Review ($150)
- Executor Support Services ($100/hour)

Download our other guides:

- Password Manager Setup Guide
- Complete Data Broker Removal Guide
- Phone & Device Hardening Guide
- Social Media Privacy Configuration
- Breach Response Playbook

All free at: https://wigingtonsecurity.com/guides

Need Help With Digital Estate Planning?

We specialize in comprehensive digital estate planning for individuals, families, and businesses.

Services:

- Digital Asset Inventory Creation
- Platform Legacy Configuration
- Legal Document Preparation
- Cryptocurrency Succession Planning
- Executor Training and Support

Contact: https://wigingtonsecurity.com/contact
Schedule: https://wigingtonsecurity.com/services

Protect your digital legacy. Secure your family's future.

Document Version 1.0 • February 2026

https://wigingtonsecurity.com