LifeCounsel® Digital Asset Management & Access Guide

This guide provides an example of a secure, practical framework for organizing and transferring digital assets whose purpose is to provide individuals and families insight into how to ensure one's digital life is properly managed in the event of incapacity or death, in accordance with the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA).

Step 1: Inventory Your Digital Assets

Use the LifeCounsel® Digital Asset Inventory Form to list:

- Financial (Online banking, PayPal, crypto wallets)
- Social (Facebook, Instagram, Twitter)
- Media (iTunes, Spotify, YouTube)
- Storage (Google Drive, Dropbox, iCloud)
- Utilities/Accounts (Email, Amazon, rewards programs)
- Domain Names (Blogs or business sites)

Step 2: Choose and Set Up a Secure Password Manager

Recommended Apps:

- 1Password: Emergency access, document storage
- Bitwarden: Open-source, 2FA support
- Dashlane: VPN, dark web monitoring

Use it to store logins, notes, 2FA backup codes, and your Inventory Form.

Step 3: Configure Emergency Access

Enable the emergency access feature in your password manager. This allows your designated person to request access to your vault with your prior approval or a waiting period.

Step 4: Store a Physical Backup

- Record and store securely:
- Master password
- 2FA codes or USB backups
- Location of important digital assets
- Suggested storage: Fireproof safe or attorney's office.

LifeCounsel®

Step 5: Include Legal Authority in Your Living Trust Digital Asset Trustee (DAT)

Consider whether the Digital Assets Trustee should serve only after death, or during incapacity as well as after death.

The following clause may be used at your own risk in your Living Trust:

12. APPOINTMENT OF DIGITAL ASSETS TRUSTEE

12.1 Appointment and Authority

12.1. 1 The Settlor(s) hereby appoint(s) [ENTITY] as the Digital Assets Trustee ("DAT") to serve during the incapacity and after the death of the Settlor(s).

12.1. 2 The DAT shall have the power to access, use, control, modify, delete, and transfer the Settlor(s)' digital assets in accordance with this clause, Florida (insert your state here) law, and the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA) as adopted in Florida (insert your state here) or any other applicable jurisdiction.

12.2 Definition of Digital Assets

12.2. 1 For the purposes of this clause, "digital assets" shall include, but not be limited to:

(a) Email accounts and their contents;

(b) Digital music, photographs, and videos;

(c) Social network accounts;

(d) File-sharing accounts;

(e) Financial accounts accessible online;

(f) Domain registrations and web hosting accounts;

(g) Cryptocurrency wallets and accounts;

(h) Online gaming accounts and virtual assets;

(i) Loyalty program accounts (e.g., hotel points, airline miles);

(j) Software licenses and digital subscriptions;

(k) Any other digital items or electronically stored information, whether currently existing or developed in the future.

12.3 Powers and Responsibilities of the DAT

12.3. 1 The DAT shall have the following powers and responsibilities:

(a) To access and control all of the Settlor(s)' digital devices, including but not limited to computers, smartphones, tablets, and any future comparable devices;

(b) To access, modify, delete, control, and transfer any and all digital assets of the Settlor(s);

(c) To access the content of electronic communications sent or received by the Settlor(s);

(d) To access records and other information pertaining to the Settlor(s)' digital assets and accounts.

12.3. 2 This authorization shall be construed as broadly as possible and shall constitute the Settlor(s)' lawful consent under the Florida (insert your state here) Fiduciary Access to Digital Assets Act, the Electronic Communications Privacy Act of 1986 (as amended), the Computer Fraud and Abuse Act of 1986 (as amended), and any applicable federal or state data privacy laws.

12.4 Compliance with Terms of Service and Privacy Policies

12.4. 1 The DAT shall make reasonable efforts to comply with the terms of service agreements and privacy policies of digital asset providers, to the extent that such compliance does not conflict with the Settlor(s)' express wishes or the best interests of the beneficiaries.

12.5 Indemnification

12.5. 1 The trust shall indemnify and hold harmless the DAT and any digital asset provider that relies on the authority granted herein, from any claims, expenses, or liabilities arising from actions taken in good faith in accordance with this clause.

12.6 Succession of DAT

12.6. 1 If the appointed DAT is unable or unwilling to serve, a successor DAT shall be appointed in the following order: [ENTITY 1], [ENTITY 2], or as determined by a court of competent jurisdiction.

12.7 Termination of DAT's Authority

12.7. 1 The DAT's authority shall terminate upon the distribution of all digital assets in accordance with the terms of this trust or as otherwise directed by the Settlor(s) or a court of competent jurisdiction.

(Optional Provisions include, DAT working with other Trustees, Sentimental vs Valuable Digital Assets and Adherence to Security Protocols)

12.1 Cooperation with Other Fiduciaries

12.1. 1 The Digital Assets Trustee (DAT) shall work in conjunction with other fiduciaries appointed under this trust or by law, including but not limited to the executor, personal representative, or other trustees, to ensure coordinated management of the Settlor's estate.

12.1. 2 The DAT shall promptly share relevant information about digital assets with other fiduciaries as necessary for the proper administration of the Settlor's estate.

12.1. 3 In the event of any conflict between the DAT and other fiduciaries regarding the management or disposition of digital assets, the matter shall be resolved by mutual agreement or, if necessary, by seeking direction from a court of competent jurisdiction in Florida (insert your state here).

12.2 Regular Accountings

12.2. 1 The DAT shall provide regular accountings of digital asset management to the beneficiaries or their designated representatives at least annually, or more frequently if required by Florida (insert your state here) law.

12.2. 2 Such accountings shall include, but not be limited to:

(a) An inventory of all digital assets under the DAT's control;

(b) Actions taken with respect to these assets;

(c) Any income generated or expenses incurred in managing the digital assets;

(d) The current status and estimated value of the digital assets, where applicable.

12.2. 3 The DAT shall make these accountings available in a format that is reasonably accessible to the beneficiaries, taking into consideration the nature of the digital assets involved.

12.3 Handling of Sentimental vs. Monetary Digital Assets

12.3. 1 The DAT shall exercise discretion in distinguishing between digital assets with primarily sentimental value and those with monetary value.

12.3. 2 For digital assets with significant sentimental value, such as personal photographs, videos, or correspondence, the DAT shall:

(a) Prioritize preservation and appropriate distribution to beneficiaries as designated in the trust or will;

(b) Consult with beneficiaries to determine the most appropriate method of sharing or transferring such assets;

(c) Take reasonable steps to ensure the privacy and security of sensitive personal information contained in these assets.

12.3. 3 For digital assets with monetary value, such as cryptocurrency, domain names, or online business assets, the DAT shall:

(a) Prioritize the preservation of asset value;

(b) Manage these assets in accordance with prudent investment standards as required by Florida (insert your state here) law;

(c) Consult with financial advisors or relevant experts as necessary to maximize the value of these assets for the benefit of the trust.

12.3. 4 In cases where a digital asset has both sentimental and monetary value, the DAT shall strive to balance these considerations, consulting with beneficiaries and other fiduciaries as appropriate to determine the best course of action.

12.3. 5 The DAT's decisions regarding the classification and handling of digital assets shall be made in good faith and in the best interests of the beneficiaries, in accordance with the Settlor's expressed wishes and Florida (insert your state here) law.

13. HANDLING OF CONFIDENTIAL AND SENSITIVE DIGITAL ASSETS

13.1 Security Protocols for Confidential and Sensitive Information

13.1. 1 The Digital Assets Trustee (DAT) shall implement and maintain strict security protocols for handling confidential or sensitive information contained within the Settlor's digital assets, including but not limited to non-public personal information and information that could enable identity theft.

13.1. 2 These security protocols shall include, at a minimum:

(a) Encryption of all confidential and sensitive data using industry-standard encryption methods;

(b) Implementation of multi-factor authentication for accessing any systems or accounts containing confidential or sensitive information;

(c) Use of limited, non-delegated login credentials specific to the DAT's role.

13.2 Access and Storage

13.2. 1 The DAT shall store all confidential and sensitive digital assets on secure, encrypted servers or devices that meet or exceed industry standards for data protection.

13.2. 2 Access to confidential and sensitive digital assets shall be restricted to the DAT and any necessary professional advisors bound by confidentiality agreements.

13.3 Transmission of Confidential Information

13.3. 1 When transmitting confidential or sensitive information, the DAT shall use secure, encrypted channels and verify the identity and authorization of the recipient before transmission.

13.4 Regular Security Audits

13.4. 1 The DAT shall conduct or arrange for regular security audits of the systems and protocols used to handle confidential and sensitive digital assets, at least annually or more frequently as required by applicable Florida (insert your state here) law.

13.5 Breach Notification and Response

13.5. 1 In the event of a suspected or confirmed breach of confidential or sensitive information, the DAT shall:

(a) Immediately take steps to contain and mitigate the breach;

(b) Notify the beneficiaries and any affected parties as required by Florida (insert your state here) law;

(c) Cooperate fully with any investigation or legal proceedings related to the breach.

13.6 Compliance with Florida (insert your state here) Law

13.6. 1 The DAT shall ensure that all handling of confidential and sensitive digital assets complies with applicable Florida (insert your state here) laws, including but not limited to the Florida (insert your state here) Information Protection Act of 2014 and any subsequent amendments or relevant legislation.

13.7 Destruction of Confidential Information

13.7. 1 When no longer needed, the DAT shall securely destroy confidential and sensitive digital assets using methods that render the information unrecoverable, in accordance with Florida (insert your state here) law and industry best practices.

13.8 Liability and Indemnification

13.8. 1 The DAT shall be held to a standard of reasonable care in implementing and maintaining these security protocols. The trust shall indemnify the DAT for any claims arising from breaches that occur despite the DAT's good faith adherence to these protocols.