DIGITAL ESTATE PLANNING INSTITUTE

depi.org

DEPI DIGITAL ESTATE CONTINUITY

BODY OF KNOWLEDGE AND STANDARD™

Draft Standard — Version 1.3

Open for Public Comment and Peer Review

May 2026

Voluntary Standard | Not a Legal or Regulatory Instrument

ABSTRACT

The Digital Estate Continuity Body of Knowledge and Standard™ defines the discipline, governance principles, domain architecture, process frameworks, normative requirements, and practitioner guidance governing the continuity of digital identity, digital assets, intellectual property, licensed digital products, tokenized representations, AI-augmented constructs, derivative economic rights, and continuity-critical systems across life, incapacity, and post-mortem transition.

This document serves three concurrent functions: a formal voluntary Standard with normative alignment requirements; a comprehensive Body of Knowledge from which all certifications, examinations, and course curricula are derived; and a practitioner reference providing actionable guidance, decision frameworks, checklists, and sample language for estate attorneys, fiduciaries, digital custodians, and platform operators.

It is designed to function as DEPI's governing reference — the document from which every certification exam question, every CLE module, every accreditation criterion, and every practitioner checklist can be traced.

HOW TO USE THIS DOCUMENT

This document is organized into twelve Parts and seventeen Appendices:

- Parts I–II: Foundations and Core Knowledge Domains — doctrine, principles, the discoverability problem, RUFADAA framework, access risk tiers, nine knowledge domains with normative requirements.
- Part III: Process Frameworks — seven canonical operational frameworks plus seven operational workflow specifications.
- Part IV: Normative Standard Requirements — consolidated alignment obligations.
- Part V: Accreditation and Certification Framework — professionalization governance.
- Part VI: Smart Contract and Blockchain Inheritance Framework — technical platform requirements.
- Part VII: Risk Management and Security Controls — security architecture and controls.
- Part VIII: Platform Accreditation Requirements — eight accreditation domains and process.

- Part IX: Regulatory and Compliance Alignment — USA (RUFADAA detail), EU, APAC, LATAM, blockchain, and AI compliance.
- Part X: Ethics, Dignity, and Post-Mortem Governance — consolidated ethical framework.
- Part XI: Future-State Continuity Systems — forward-looking guidance on emerging technologies.
- Part XII: Appendices A–Q — glossary, taxonomy, templates, checklists, schemas, advisory clauses, and reference models.
- Final Declaration — governing statement of purpose.

VERSION HISTORY SUMMARY

v1.0 (February 2026) — Initial published standard covering identity, asset taxonomy, lifecycle, workflows, smart contracts, security, accreditation, ethics, regulatory alignment, and future-state framework.

v1.1 (Working Draft) — Repositioned as Body of Knowledge and Standard. Added ten Knowledge Domains, seven Process Frameworks, Parts IV–VI, L1/L2/L3 risk classification, and legal boundary statements.

v1.2 (Draft Standard, May 2026) — Full synthesis of v1.0 and v1.1. Ethics consolidated into Part X. Regulatory moved to Part IX. Twelve parts, thirteen appendices (A–M).

v1.3 (Current Draft Standard, May 2026) — Added practitioner foundations layer (Sections 1.10–1.16): Discoverability Problem, Digital Orphans, Control vs. Ownership doctrine, RUFADAA three-tier priority structure, beneficiary access risk tiers with concrete examples, execution risk for beneficiaries and executors, attorney exposure, explicit authorization doctrine, structured discovery, and digital asset alignment guidance. Added Appendices N (DEP Schema), O (APMC Templates), P (Advisory Clause Library), Q (Jurisdictional Autonomy Statement). Added Final Declaration. Seventeen appendices (A–Q) total.

PART I — FOUNDATIONS OF DIGITAL ESTATE CONTINUITY

1.1 Definition of the Discipline

Digital Estate Continuity is the structured governance of digital identity, digital assets, intellectual property, licensed digital products, tokenized representations, AI-augmented constructs, and derivative economic rights such that authority, access, and continuity may transition lawfully and safely across life, incapacity, succession, and post-mortem administration.

Digital estate continuity is not synonymous with password storage, digital vaulting, or blockchain inheritance. It is an integrated discipline governing:

- authority assignment and verification
- lawful access and delegation
- ownership verification and classification
- transferability constraints and licensing
- beneficiary liability risk classification
- ethical stewardship of identity and AI-augmented assets
- audit integrity and evidence preservation
- cross-jurisdictional conflict management

1.2 Scope & Legal Non-Substitution Statement

> This Body of Knowledge and Standard does not replace governing estate law, probate authority, trust instruments, or statutory succession frameworks. It does not create independent legal rights, nor does it supersede wills, trusts, court orders, or statutory inheritance rules. DEPI does not provide legal advice. Licensed legal professionals remain solely responsible for legal advice and compliance with jurisdiction-specific law. Digital Execution Plans function as structured continuity annexes and documentation aids; they do not replace testamentary instruments.

1.3 Scope of Application

This Standard applies to:

- individuals and families
- estate planners, fiduciaries, trustees, and executors
- technology platforms and digital custodians
- SMBs and founder-led enterprises
- creators, inventors, engineers, and intellectual property holders
- cross-border estates
- blockchain-integrated systems
- AI-enabled systems and memory constructs
- regulators and legislative bodies seeking reference doctrine

1.4 Core Governing Principles

Principle	Statement
Legal Supremacy	Technical systems remain subordinate to governing law, probate authority, and court determination.
Access Is Not Ownership	Access rights do not automatically convey ownership, transferability, or commercialization rights.
Representation Is Not Title	Digitization, tokenization, minting, or blockchain anchoring does not automatically confer legal title or replace registries.
Beneficiary Protection Doctrine	Continuity systems shall prioritize protecting beneficiaries from civil, criminal, contractual, regulatory, or emotional harm resulting from access or misuse.
Structured Risk Governance	All digital assets must be classified and governed using an explicit risk model that includes beneficiary liability exposure.
Ethical Stewardship	Emotional and AI-augmented assets require dignity, consent, and harm-reduction safeguards.
Human Governance Over Automation	No automated system shall irreversibly execute inheritance without structured human oversight and override capability.
Technological Neutrality	The discipline remains adaptable to evolving technology without privileging any single implementation.

1.5 Legal and Governance Hierarchy

Continuity systems shall defer to the following hierarchy, in descending order of authority:

1. Governing estate and succession law
2. Probate authority and judicial determinations
3. Intellectual property law
4. Contract and licensing law (including platform terms)
5. Data protection law and privacy rights
6. Regulatory mandates
7. User-level continuity configuration
8. Technical rules and automation (including smart contracts)

1.6 Valuation Boundary Doctrine

Digital Estate Continuity governs authority, classification, transferability, and risk — not asset valuation. While some digital assets may possess measurable financial value, others may possess emotional, intellectual, or relational significance that cannot be quantified in monetary terms.

This Body of Knowledge does not prescribe methodologies for fair market valuation, tax assessment, securities pricing, royalty discount modeling, or business enterprise valuation. Where financial valuation is required for probate, tax reporting, or commercial disposition, qualified valuation professionals and applicable legal standards shall govern.

Asset classification shall distinguish between economic value and continuity relevance. An asset of low financial value may carry high continuity significance, and vice versa.

1.7 Regulatory Evolution and Industry Stabilization Context

Digital estate continuity operates within a rapidly evolving regulatory environment. Digital identity systems, blockchain-based asset registration, AI-generated cognitive constructs, tokenized representations, licensed digital ecosystems, and platform-governed economic rights are developing faster than statutory frameworks in many jurisdictions.

Without a coherent reference framework, cross-border estates may face non-recognition of digital instruments; tokenized representations may conflict with statutory registries; executors may encounter inconsistent access rights across platforms; beneficiaries may incur

unintended legal exposure; and regulators may lack shared terminology and governance structure.

This Body of Knowledge is intended to serve as a stabilizing reference point. It does not replace governing law, prescribe statutory authority, or regulate practitioners. It provides structured doctrine and best practices that may inform professional practice, platform architecture, regulatory dialogue, legislative development, and cross-jurisdictional interoperability.

1.8 Normative Language Key

Term	Meaning
Shall / Must	Mandatory requirement under voluntary DEPI alignment claims.
Should	Recommended best practice.
May	Permissible action.
Prohibited	Not allowed under alignment or accreditation.

Shall and Must statements in this Standard apply only to voluntary DEPI alignment claims and do not override local law or controlling instruments. Where conflict exists between DEPI alignment and governing law, governing law prevails under the Legal Supremacy Doctrine defined in Section 1.5.

1.9 Relationship to Other Frameworks

This Standard is complementary to, and does not replace:

Framework	Domain
ISO/IEC 27001	Information security management
ISO Blockchain Framework	Blockchain and distributed ledger technology
NIST Digital Identity Guidelines (SP 800-63)	Digital identity assurance
NIST Cybersecurity Framework	Cybersecurity risk management
RUFADAA / UFADAA (USA)	Fiduciary access to digital assets

Framework	Domain
EU eIDAS 2.0	European digital identity and trust services
GDPR and analogous statutes	Data protection and privacy
International probate frameworks	Cross-border inheritance law

PART II — CORE KNOWLEDGE DOMAINS

Part II defines ten Knowledge Domains that constitute the body of knowledge for digital estate continuity practice. Each Domain includes a definition, key concepts, and embedded normative requirements for DEPI-aligned programs.

Domain 1 — Identity Continuity

2.1 Domain Definition

Identity Continuity governs lawful, secure transitions of authority across identity layers such that continuity may occur without impersonation, lockout, unauthorized escalation, or continuity failure. Identity is the gateway domain: without it, asset governance fails.

2.2 Identity Layers

Layer	Description
Legal Identity Layer	Government identity and legal authority documentation: powers of attorney, executor appointments, court orders.
Platform Identity Layer	Account credentials, authentication mechanisms, contractual access rights.
Cryptographic Identity Layer	Private/public key pairs, MPC/multi-sig constructs, decentralized identifiers (DIDs), verifiable credentials (VCs).
AI-Augmented Identity Layer	Memory models, personas, voice/likeness systems, behavioral representations trained on personal data.

2.3 Identity Risk Surfaces

- Executor impersonation
- Credential lockout and single-point-of-failure authentication
- Single-key cryptographic dependency
- Cross-border recognition conflict for legal authority
- AI post-mortem impersonation without consent
- Unauthorized delegated escalation
- Silent device-bound identity failure

2.4 Authorized Post-Mortem Communications (APMC)

APMC is a controlled, pre-authorized mechanism allowing certain communications after death or incapacity without creating unbounded impersonation risk.

Recognized APMC types include: pre-written obituary and final message posts (email/social); administrative notices (out-of-office, memorialization notice); and restricted notifications with defined audience and content scope.

Risk classification guidance: pre-written bounded messages are typically L1–L2; discretionary messaging that appears to originate from the decedent is L2–L3; messaging that can create financial commitments is L3 (restricted). See Domain 2 for the L1/L2/L3 classification model.

2.5 Normative Requirements — Domain 1

Aligned systems shall:

- Provide identity recovery pathways that do not create estate lockout.
- Prevent single-point cryptographic identity failure.
- Require verified authority before identity transitions.
- Log identity state transitions and revocations.
- Freeze AI identity layers upon verified death unless explicitly configured otherwise.
- Prohibit impersonation-by-default workflows.
- Support MFA continuity pathways including device-loss and biometric fallback.

Domain 2 — Digital Asset Taxonomy, Origination, and Rights

3.1 Domain Definition

This Domain defines how digital assets are classified based on origination, rights structure, and transferability, so that continuity governance is lawful, safe, and interpretable.

3.2 Asset Classification Categories

Category	Includes
Category 1: Financial Digital Assets	Online bank and investment accounts, payment platforms, loyalty programs, digital brokerage accounts, pension portals.

Category	Includes
Category 2: Communication and Social Identity Assets	Email accounts, messaging apps, social media profiles, contact lists, personal and professional communication history.
Category 3: Personal Data and Records	Photos, videos, cloud storage, educational and medical records, password managers, subscription accounts, digital purchases.
Category 3A: Emotional Digital Assets	Legacy letters, future-dated messages, AI-generated family memory models, video diaries, personal reflections for heirs, NFT-based emotional artifacts.
Category 4: AI-Generated Cognitive Assets	AI memory models, AI-generated personal writing/voice/likeness, AI personas, predictive behavioral models, cognitive datasets.
Category 5: Business and Operational Digital Assets	SMB cloud systems, CRM, operational software, vendor accounts, business identity credentials, key-person operational automations.
Category 6: Cryptographic and Blockchain Assets	Cryptocurrency wallets, on-chain tokens, NFTs, DIDs, smart-contract-bound assets, tokenized legal titles.
Category 7: Intellectual Property Assets	Code repositories, CAD files, patents, trade secrets, proprietary designs, model weights, open-source contributions.
Category 8: Representation and Derivative Rights	NIL-style rights, digital twin licensing, geospatial monetization rights, royalties, avatar-based appearances.
Category 9: Immersive and Spatial Digital Assets	AR/VR/XR environments, holographic recordings, volumetric spatial captures, AI-augmented immersive simulations.

3.3 Modes of Origination

Digital assets originate through: native digital creation; digitization of physical artifacts; tokenization of legal or physical instruments; platform-based publication; intellectual property authorship; representation or derivative rights creation; and emotional or intention-based origination. Origination mode influences legal status, rights boundaries, and risk.

3.4 Ownership, Transferability, and Licensing

Continuity governance shall treat ownership, transferability, and licensing as three separate governance dimensions. Key doctrine:

- Platform account ownership does not equal content ownership.
- NFT ownership does not equal copyright ownership.
- Tokenization does not equal legal title.
- Access does not equal ownership.
- Management rights do not equal commercialization rights.

Licensed digital products (music libraries, e-books, subscriptions) are non-transferable licenses and shall be classified explicitly as licensed-use assets and flagged in continuity plans to prevent beneficiary liability.

3.5 Intellectual Property and Trade Secrets

IP assets require: ownership verification (individual, corporate, or work-for-hire); review of license obligations (open source, CLAs); confidentiality preservation of trade secrets; application of export controls where applicable; and separation of access rights from commercialization rights.

3.6 Immersive and Spatial Digital Asset Governance

Spatial and immersive assets must preserve 3D rendering metadata, device capture details, and AI augmentation markers. Platforms shall support staged release, beneficiary-specific access, age gating for minors, and encrypted delivery. Immersive assets must not fabricate false memories, impersonate the deceased without authorization, or expose sensitive content inadvertently. Platforms must offer exportable formats (.usdz, .glb, .mp4 fallback) and cross-platform compatibility.

3.7 Beneficiary-Centric Risk Classification (L1/L2/L3)

Risk classification shall explicitly evaluate beneficiary liability exposure, not only asset value:

Tier	Definition and Examples
L1 — Minimal Exposure	No foreseeable regulatory, contractual, or criminal exposure. No significant third-party consent barriers. Examples: domestic Wi-Fi password shared with authorization; sentimental archives with no confidentiality issues; low-value inactive accounts.
L2 — Conditional/Contextual Exposure	Contractual constraints or ongoing obligations for beneficiaries. May contain IP with conditional

Tier	Definition and Examples
	transferability. Examples: licensed streaming accounts; email read-access; pre-written social message delivery; monetized social channels; digital art with royalty structures.
L3 — High-Impact Exposure	Regulatory, criminal, civil, reputational, or IP exposure likely. Examples: bank withdrawals without ownership; private key control; AI-trained identity artifacts; trade secret repositories; business operating accounts; material cryptocurrency portfolios; health or biometric data.

Risk classification governs verification thresholds and controls, not ownership. A single asset may be reclassified upon changes in context or jurisdiction.

3.8 Normative Requirements — Domain 2

Aligned systems shall:

- Classify assets by origination mode and rights structure.
- Flag licensed and non-transferable assets explicitly in continuity plans.
- Distinguish account ownership from content ownership.
- Apply beneficiary-centric L1/L2/L3 risk classification to all material assets.
- Preserve metadata necessary for executor interpretation.
- Include classification results in the Digital Execution Plan.
- Apply heightened governance to immersive, emotional, and AI-derived assets.

Domain 3 — Continuity Lifecycle and Execution Governance

4.1 Domain Definition

This Domain governs continuity across life phases by establishing lifecycle states and transitions for identity, assets, rights, and obligations.

4.2 Lifecycle Stages

- Origination and onboarding
- Classification and rights mapping
- Storage and protection

- Access governance and delegation
- Trigger verification
- Digital execution planning
- Inheritance execution
- Post-mortem governance
- Archival preservation
- Destruction protocols

4.3 Digital Execution Plan (DEP) Doctrine

A Digital Execution Plan is a structured continuity annex — not a testamentary instrument — that provides:

- Discoverability inventory with custody classification
- Rights structure and origination mode per asset
- Entitlement mapping (who gets what, when, and under what conditions)
- Risk sensitivity classification (L1/L2/L3)
- Delegation and authority mapping
- APMC instructions, if any
- License and IP constraints
- Audit identifiers and version history

A DEP is not a will, not a trust, not a dispositive instrument, and not self-executing legal authority. It is subordinate to legal documents and must be exportable, interpretable, and updatable.

4.4 Executor Authority Mapping

Executors and trustees shall receive authority proportional to legal documentation and asset risk classification. Systems shall prevent executor overreach into emotional assets not authorized, IP commercialization without right, non-transferable licensed products, and discretionary impersonation.

4.5 Normative Requirements — Domain 3

- Generate versioned DEPs upon material changes.
- Enforce legal hierarchy and executor authority mapping.
- Apply L3 controls to high-risk assets.
- Preserve audit traceability for all continuity actions.
- Support revocation and dispute holds.

- Prohibit DEPs from being represented as testamentary instruments.

Domain 4 — Cryptographic and Smart Contract Governance

5.1 Domain Definition

This Domain governs blockchain, wallets, smart contracts, tokens, NFTs, DIDs, and cryptographic continuity controls as assistive mechanisms that remain subordinate to legal authority.

5.2 Key Management Discipline

Aligned systems shall not rely on a single seed phrase or private key for continuity. High-risk cryptographic assets require MPC or multi-sig architecture and structured recovery pathways. Continuity must never depend on a single point of cryptographic failure.

5.3 Tokenization Discipline

Tokenization is representational unless jurisdictionally recognized as legal title. Systems shall disclose token legal status and prevent beneficiaries from assuming NFT ownership confers copyright ownership. Smart contracts and tokenized instruments are subordinate to statutory and judicial authority.

5.4 Smart Contract Governance

Inheritance smart contracts must be: audited; deterministic; capable of human override; upgradeable or migratable; and logged on-chain with linkage to off-chain authority verification. Inactivity-triggered inheritance is prohibited under DEPI alignment.

5.5 Blockchain-Specific Regulatory Considerations

Blockchain-based continuity must consider: jurisdictional recognition of tokenized assets; tax treatment of crypto inheritance; chain forks and governance changes; node location implications; and immutability versus right-to-erasure conflicts. Systems shall avoid storing personally identifiable information directly on-chain and shall maintain override pathways for legal compliance.

5.6 Normative Requirements — Domain 4

- Require multi-party governance for all L3 cryptographic actions.
- Provide human override mechanisms for smart contract execution.
- Ensure no PII is stored on-chain.
- Maintain structured audit linkage between on-chain and off-chain records.

- Disclose token legal status explicitly to users and beneficiaries.

Domain 5 — Risk and Security Governance

6.1 Domain Definition

This Domain governs risk assessment, security controls, monitoring, incident response, and audit integrity for digital continuity systems.

6.2 Beneficiary Protection as the Primary Risk Driver

Risk modeling shall explicitly include beneficiary civil, criminal, and regulatory exposure from: financial transactions without ownership; impersonation via email or social media; contract or ToS violations from licensed account use; trade secret disclosure; and regulatory breaches including data protection violations.

6.3 Core Control Areas

- Encryption at rest and in transit for all continuity-critical data
- Role-based access control (RBAC) and least-privilege design
- MFA continuity pathways to prevent estate lockout
- Anomaly detection and behavioral monitoring
- Incident response including fraudulent death claim procedures
- Vendor dependency risk evaluation
- Append-only, exportable audit logging with defined retention

6.4 Immutable Audit Doctrine

Audit integrity requires: structured event logging for identity, delegation, triggers, access, and releases; cross-linkage between on-chain and off-chain events; human-readable audit export capability; dispute resolution holds; and a defined minimum retention period.

6.5 Normative Requirements — Domain 5

- Maintain annual risk assessment covering all asset categories.
- Apply L3 safeguards to high-risk assets.
- Log all continuity-critical actions in append-only audit records.
- Maintain regulator-ready audit export capability.
- Implement incident response playbooks for continuity failures.

Domain 6 — Platform Architecture and Operational Continuity Governance

6A.1 Domain Definition

Platform Architecture and Operational Continuity Governance addresses the structural, infrastructural, and deployment-level requirements necessary to ensure that digital continuity systems remain secure, resilient, interoperable, exportable, recoverable, jurisdiction-aware, and vendor-neutral. Digital estate continuity is only as durable as the infrastructure that supports it.

6A.2 Deployment Models

DEPI recognizes multiple deployment models: cloud-hosted SaaS; hybrid architectures; on-premise enterprise systems; custodial cryptographic platforms; non-custodial cryptographic systems; self-hosted nodes; and federated identity architectures. The Standard does not privilege one model over another; each introduces distinct risk surfaces.

6A.3 Cloud-Based Platform Governance

Cloud-based platforms shall: maintain tenant isolation; segregate encryption keys; provide documented disaster recovery plans; maintain defined uptime SLAs; ensure continuity export in the event of service termination; document data residency locations; provide data portability mechanisms; and avoid vendor lock-in that prevents estate-level continuity. Platforms must disclose jurisdictional hosting locations where relevant to data protection law.

6A.4 Custodial vs. Non-Custodial Architectures

Where platforms control keys (custodial): key custody must be documented; multi-party governance is required for high-risk actions; recovery pathways must exist; and escrow and succession models must be defined. Where users control keys (non-custodial): single-seed dependency is prohibited for accreditation; recovery assistance must be structured; and executor onboarding must not require private key disclosure.

6A.5 Platform Survivability and Shutdown Risk

Platforms aligned with DEPI shall define: business continuity plans; data export procedures upon shutdown; asset portability mechanisms; smart contract migration pathways; and a communication plan for continuity events affecting the platform. Digital continuity must not collapse upon platform failure.

6A.6 Normative Requirements — Domain 6

- Document deployment model and infrastructure governance.
- Provide continuity export capability independent of platform status.
- Maintain disaster recovery procedures with defined RTO and RPO.
- Prevent single-point key dependency.
- Maintain operational logging.
- Support structured migration pathways.
- Disclose data residency and infrastructure governance to users.

Domain 7 — Regulatory and Jurisdictional Alignment

7.1 Domain Definition

The Regulatory and Jurisdictional Alignment Domain governs how Digital Estate Continuity operates within overlapping legal systems across national, regional, and local jurisdictions. Digital continuity is inherently cross-border: identity providers may operate in one country; data may be stored in another; blockchain nodes may be globally distributed; and beneficiaries may reside under different legal regimes.

7.2 Legal Precedence Model

Digital continuity systems shall operate within the governance hierarchy defined in Section 1.5. Technical architecture must not override this hierarchy. Smart contracts, tokenized instruments, and AI-generated outputs are subordinate to statutory and judicial authority.

7.3 Data Protection and Privacy Alignment

Digital continuity frequently intersects with: GDPR; CCPA; LGPD; PDPA; PIPA; HIPAA; local biometric data laws; and post-mortem data rights frameworks. Systems shall respect third-party privacy within inherited communications; distinguish catalogue data from content data; support executor-driven lawful data requests; allow deletion or redaction where legally required; and avoid storing PII on public blockchains. Beneficiary access must not override statutory privacy protections.

7.4 Intellectual Property and Regulatory Interface

IP-bound assets require alignment with: copyright law; patent law; trade secret law; open-source licensing frameworks; export control regulations; and cross-border commercialization restrictions. Continuity systems must not facilitate unlawful redistribution, automatically assign commercialization rights, expose trade secrets through executor misinterpretation, or assume that token ownership equals copyright transfer.

7.5 Financial and Securities Regulation Considerations

Digital financial assets may be governed by banking regulations, securities regulations, custodial requirements, AML/KYC frameworks, tokenized securities laws, and cross-border capital controls. Systems shall avoid enabling unauthorized withdrawal, require verification proportional to asset classification, and recognize that informational access differs from transactional authority. High-risk financial actions must remain L3-controlled.

7.6 AI Governance and Emerging Regulation

AI systems intersect with rapidly evolving regulatory frameworks including the EU AI Act and OECD AI principles. Continuity governance must prevent AI from issuing legal or financial instructions post-mortem; require labeling of AI-generated content; allow executor control over model freezing; avoid impersonation without explicit authorization; and respect cross-border AI compliance obligations. AI systems must not become de facto fiduciaries.

7.7 Normative Requirements — Domain 7

- Document legal constraints per asset category where feasible.
- Support lawful access request workflows consistent with applicable statute.
- Generate regulator-ready audit outputs.
- Prevent unlawful cross-border data export.
- Identify and document cross-border triggers for all material assets.

1.10 The Discoverability Problem

Physical assets are, by nature, discoverable. Real property is recorded in public registries. Bank accounts appear on tax returns. Vehicles have titles. The legal and fiduciary systems governing traditional estates were built on the assumption that assets can be found.

Digital assets invert this assumption entirely. They are credential-gated and non-public. A digital asset exists only if someone knows to look for it, knows where to look, and possesses or can obtain the credentials to access it. If the fiduciary does not know an asset exists, it cannot be governed, transferred, preserved, or included in the estate. It simply disappears.

This creates a structural asymmetry that governs every aspect of digital estate continuity practice:

Asset Type	Discoverability Characteristic
Physical Assets	Recorded and visible. Discoverable through public records, financial statements, and institutional notification.

Asset Type	Discoverability Characteristic
Digital Assets	Credential-gated and non-public. Discoverable only through proactive inventory, platform knowledge, and credential access.

The practitioner implication is direct: discovery is not a preliminary step in digital estate continuity — it is a foundational and ongoing governance obligation. An undiscovered asset is a failed continuity outcome regardless of how well everything else is governed.

1.11 Digital Asset Fragility and the Digital Orphan Problem

Physical assets have persistence. A deed, a stock certificate, a piece of jewelry — these do not disappear because their owner died. Digital assets are fundamentally more fragile. Without active management, they are subject to:

- Deletion — platforms may delete inactive accounts, unpaid subscriptions, or accounts flagged as abandoned.
- Lockout — security systems may permanently lock accounts upon detecting unusual access patterns, including estate administration activity.
- Subscription Drain — recurring charges may continue depleting the estate until accounts are discovered and cancelled.
- Storage Facilities Drain — cloud storage, hosting services, and data vaults may charge ongoing fees or delete content upon non-payment.

It is estimated that tens of millions of accounts are abandoned or become inaccessible each year. These are known as Digital Orphans — assets that existed, had value (financial, emotional, or operational), and were lost not because of legal complexity but because no one knew they existed or knew how to access them.

Digital Orphans represent a systemic failure of estate planning — and a direct indictment of the assumption that digital assets will somehow surface on their own. They will not. Structured discovery, documented inventory, and proactive continuity planning are the only remedies.

> Practitioner Principle: Mitigation starts with proper discovery and identification. An estate plan that does not address digital assets does not address the estate.

1.12 Control Is Not Ownership: The Foundational Digital Estate Distinction

The most consequential misunderstanding in digital estate practice is the conflation of credential control with legal ownership. In the physical world, these align: title creates ownership, which creates authority. In the digital world, they do not.

World	Control and Authority Chain
Physical World	Title → Ownership → Authority. Control of a physical asset derives from legal title. Ownership is documented, publicly registered, and legally enforceable.
Digital World	Credentials → Access → ≠ Authority. Possession of a username and password provides access. Access does not equal ownership. Ownership does not automatically equal authority to transfer, commercialize, or act on behalf of an estate.

This distinction has concrete legal consequences. A beneficiary who accesses a deceased family member's bank account using shared credentials may have committed unauthorized access regardless of intent. An executor who uses a decedent's email password to send notifications may have violated the Computer Fraud and Abuse Act, the Stored Communications Act, or both. Good intentions do not create legal authority.

Fiduciaries and practitioners must therefore govern three separate questions for every digital asset: Who has legal authority? What does that authority permit? How is that authority documented and exercised lawfully?

> Core Doctrine: Credentials ≠ Access. Access ≠ Ownership. Ownership ≠ Authority to act. Each must be established independently and documented.

1.13 The RUFADAA Priority Structure

The Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA) establishes the governing priority structure for fiduciary access to digital assets in states where enacted. Understanding this hierarchy is foundational to digital estate practice in the United States.

RUFADAA establishes a three-tier hierarchy of control, applied in descending order:

Priority	Type	Explanation
Tier 1	Platform Online Tools	Tools provided directly by the platform — such as Google's Inactive Account Manager, Apple's Digital Legacy Contact, Facebook's Legacy Contact, or crypto exchange beneficiary designations — that allow the user, while alive, to direct what happens to their account at death. These tools take priority over all other instruments, including wills and trusts.
Tier 2	Legal Documents	If no online tool governs, then the Will, Trust, or Power of Attorney becomes operative. However, these instruments can still be constrained by platform terms of service and applicable statute.
Tier 3	Terms of Service and Default Law	If neither online tools nor governing documents address the question, the platform's Terms of Service and applicable default statutory law control.

> Critical Practitioner Alert: Platform-provided online tools can and do override contrary estate language. If a client's Will says "all digital communications to my spouse" but their Facebook Legacy Contact designates their daughter, the Facebook designation controls — not the Will. This is not a technical quirk. It is the express structure of RUFADAA.

1.13.1 Structural Limits of RUFADAA

Even with valid RUFADAA authority, fiduciaries face structural constraints that the statute does not override:

- Custodians retain discretion under their Terms of Service — platforms may still decline requests or impose additional verification requirements.
- Access may be limited to content disclosure rather than full account control — viewing is not the same as managing or transferring.
- Electronic communications require explicit consent under the Stored Communications Act — access to email content requires specific authorization.
- Transferability may still be restricted — RUFADAA provides access, not transferability. Licensing constraints and platform non-transferability clauses remain operative.

RUFADAA creates a framework for access — but execution still depends on the platform. Having legal authority and obtaining practical access are two different problems.

1.13.2 State Variation

RUFADAA adoption is broad but uniformity is not complete. Most states have enacted versions of RUFADAA; some have modified the statutory language; a few have not adopted it. Interpretation and enforcement vary. Digital assets are governed by similar statutes, but those statutes are applied differently across jurisdictions.

As statutory interpretation evolves and courts encounter digital estate disputes with increasing frequency, structured standards and continuing education become increasingly important. A practitioner who treated RUFADAA as a complete solution in 2018 may find that the platform relationships and ToS constraints have rendered that analysis incomplete today.

1.13.3 RUFADAA Practical Checklist

Practitioners advising clients on digital estate planning should address all four of the following:

Action	Guidance
1. Inventory Platform Online Tools Explicitly	Ask: Has the client set up Google Inactive Account Manager? Have they designated a Facebook Legacy Contact? Have they set Apple Digital Legacy? Are crypto exchange beneficiary designations in place? Have they set TOD/POD designations on financial accounts? Has the client affirmatively declined any platform legacy tools?

Action	Guidance
2. Align Online Tools with Estate Intent	If the Will says one thing and a platform designation says another, there is a structural conflict. Either update the platform setting or revise the estate language — do not leave them misaligned. The platform designation will win.
3. Avoid Contradictory Instructions	If a client has strong privacy preferences (e.g., delete all emails), that may require explicit consent language in estate documents AND alignment with platform deletion settings. Otherwise, fiduciaries may be blocked or exposed.
4. Document the Client's Platform Elections	Record: whether online tools are used; who is designated; whether those designations are intended to control; and whether they were reviewed in connection with estate planning.

Digital estate planning requires coordination between legal documents and platform control systems. One without the other is incomplete.

1.14 Beneficiary Access Risk: A Tiered Framework

Not all digital asset access creates the same risk. Risk scales with the nature of the account, the actions that access enables, and the clarity of the legal authority supporting those actions. Without clear authorization and defined scope, access may create unintended liability — even when the intent was entirely benign. Good intentions can create liability. This is the most important practical insight in digital estate administration.

1.14.1 The Three Access Risk Tiers

Tier	Description and Examples
Tier 1 — Administrative	Limited legal exposure. Examples: streaming accounts; food delivery apps; WiFi routers; low-value subscriptions. ToS violations are possible but practical consequence is low.
Tier 2 — Contractual and Operational	Moderate contractual and operational implications. Examples: cloud storage; small business tools; insurance

Tier	Description and Examples
	portals; professional accounts. May trigger ToS violations, account lockouts, or scope disputes.
Tier 3 — Identity and Financial Control	High legal exposure and liability potential. Examples: email (controls password resets for all other accounts); banking and investment portals; government portals; accounts with transactional capability. Access without documented authority creates serious risk.

Clear, documented authority can reduce liability — but it may not eliminate all platform constraints. See Appendix K for the full Risk-Tier Decision Reference Matrix with additional asset examples.

1.14.2 Execution Risks for Beneficiaries

Beneficiaries acting without clear documented authority — even with the best intentions — may:

- Access accounts without documented legal authority, creating CFAA and SCA exposure.
- Transact without authority, creating unauthorized transfer claims.
- Transfer assets prematurely before probate authority is established.
- Violate Terms of Service, triggering permanent account lockouts that harm the estate.
- Trigger security resets that lock out the authorized executor.
- Disrupt probate sequencing or tax reporting integrity through premature access.

Good intentions do not create legal authority. Practitioners must counsel clients and their families on this explicitly.

1.14.3 Risk to Executors

Even a formally appointed executor may act beyond scope, prematurely access accounts before letters testamentary are issued, trigger security resets that complicate estate access, or disrupt probate sequencing through premature digital actions. Digital estates require staged engagement — the appropriate posture at each stage must be explicitly planned and documented.

1.14.4 Evolving Exposure for Attorneys

Estate planning counsel faces a growing exposure landscape. Direct credential custody creates independent liability. Attorneys also face advisory scope gaps, undisclosed digital exposure, client expectation shifts, and reputational risk from estates where digital assets were lost despite a completed estate plan. Digital literacy is increasingly inseparable from the fiduciary core skill set.

1.15 Explicit Authorization Doctrine

The foundation of defensible digital estate administration is explicit, documented authorization. Intent is not authorization. Family expectation is not authorization. Prior permission during the decedent's lifetime is not authorization for post-mortem access.

Even when beneficiaries are "intended" to act:

- They may lack legally sufficient documented authorization.
- They may not be able to prove the scope of any permission granted.
- Platforms may deny access absent documentation that meets their requirements.
- Actions may exceed the scope of whatever authorization exists.

Intent without documented authority creates friction at best and liability at worst. Authorization should be explicit and defensible. This requires that it be written, scoped, and connected to the legal instruments that grant the underlying authority.

1.15.1 Scope of Authority — Four Required Dimensions

Clients and their advisors should explicitly define four dimensions of authority for digital assets:

Dimension	Guidance
Who May Access Which Accounts	Named individuals tied to specific account categories — not blanket grants to "my executor" without asset-specific mapping.
Whether Access Includes Action or View-Only	Reading email differs from sending email. Viewing account balances differs from making transactions. Scope must be stated.
Timing of Access	Pre-death delegation differs from post-death executor authority. Emergency access differs from full estate administration authority. Timing must be specified.

Dimension	Guidance
Authority to Communicate on Their Behalf	Out-of-office messages, final notifications, and social media posts require specific authorization. Communication authority must be explicitly granted, not assumed.

Reducing ambiguity reduces risk. This is the central practitioner principle of digital estate governance.

1.16 Structured Discovery: The Practitioner Process

Discovery is the foundational activity of digital estate continuity practice. It cannot be delegated to the client alone, and it cannot be completed once and considered done. Digital accounts and credentials change continuously.

A structured discovery process includes:

- Inventory digital accounts and platforms — systematically, by category, not from memory.
- Identify devices and credential recovery pathways — the phone, the laptop, the hardware key, the recovery email.
- Map recurring financial and contractual obligations — subscriptions, storage fees, automated payments, ongoing licensing.
- Develop a plan to maintain the information as digital accounts and credentials grow and change.

Mitigation starts with proper discovery and identification. The estate plan cannot govern what the plan does not know exists.

1.16.1 Structured Guidance on Digital Asset Alignment

After identifying and categorizing digital assets, practitioners should guide clients to take the following alignment steps where appropriate:

- Clarify whether beneficiaries should receive ownership, administrative access, or view-only rights — and document that decision per asset.
- Align account titling with estate intent — joint ownership, TOD/POD designations, and co-owner designations should reflect the estate plan.
- Add authorized users or co-owners where appropriate and legally permissible.

- Establish payable-on-death or transfer-on-death designations for financial accounts where available.
- Document the scope of permitted actions for any non-owner access granted.

The governing principle: align legal ownership, platform access, and estate intent before death — not after. Post-death remediation is significantly more difficult, more expensive, and frequently incomplete.

Domain 9 — Dispute Resolution, Enforcement, and Institutional Interfaces

9.0 Purpose and Structural Context

Digital estate continuity does not conclude at planning or administration. It is tested under contest. Domain 9 establishes the doctrinal and operational framework for resolving disputes arising within digital estates and for interfacing with courts, regulators, platforms, and cross-border authorities.

Unlike traditional probate disputes, digital estate conflicts are complicated by platform-governed contractual environments, cross-border data storage, encryption and decentralized control, algorithmic identity persistence, and conflicts between statutory authority and technical capability. This Domain recognizes that digital continuity lacks legitimacy unless enforceable. Planning without enforceability collapses into aspiration.

9.1 The Nature of Digital Estate Disputes

Digital estate disputes differ from traditional probate conflicts in three structural ways.

First, control is often technical rather than legal. Possession of credentials or private keys may allow unilateral action independent of legal authority. This creates asymmetry between lawful entitlement and technical control. Dispute governance must reconcile these two realities.

Second, platforms function as quasi-jurisdictions. Platforms establish internal rules governing account transferability, memorialization, deletion, and access thresholds. These contractual regimes may conflict with probate law. Disputes frequently arise not between beneficiaries alone, but between estates and platform governance systems.

Third, digital assets cross borders instantly. Digital records may reside across multiple jurisdictions simultaneously, implicating probate court authority, data protection regulators, consumer protection bodies, and foreign judicial systems. The dispute is rarely geographically contained.

9.2 Dispute Typology

For governance clarity, disputes shall be categorized according to structural nature:

- Authority Conflicts — competing claims to digital fiduciary power.
- Access-Ownership Distinctions — beneficiaries asserting ownership based on granted access.
- Platform Refusal Conflicts — platforms declining estate requests despite probate authority.
- Cryptographic Custody Disputes — control of private keys without documented entitlement.
- AI Continuation and Identity Misrepresentation Disputes — unauthorized synthetic simulation or commercial use.
- Privacy and Disclosure Disputes — tension between confidentiality and beneficiary demand.
- Cross-Border Enforcement Disputes — jurisdictional collision affecting data access.

Each category requires doctrinally distinct analysis.

9.3 Governing Instrument Hierarchy Doctrine

Dispute analysis shall begin with structured instrument hierarchy review: express digital continuity directives; testamentary instruments; powers of attorney for incapacity; statutory digital access provisions; platform contractual terms; and default inheritance rules. Conflicts shall not be assumed resolved by chronology alone.

Platform terms cannot automatically override statutory fiduciary rights where law provides representative access. Conversely, statutory authority may not compel violation of foreign data protection law. Hierarchy analysis must be documented.

9.4 Preservation and Non-Destruction Doctrine

Upon identification of dispute: destructive actions shall be suspended; asset transfers shall be paused; audit logs shall be secured; and key redistribution shall cease. Digital disputes are uniquely vulnerable to irreversible action. Preservation is therefore a primary duty. Failure to preserve may constitute breach of fiduciary obligation and may expose practitioners to liability.

9.5 Evidentiary Integrity in Digital Context

Digital evidence must meet institutional-grade standards. Required documentation may include: verified death certificate; letters testamentary or court appointment; authority

documentation; credential access logs; blockchain transaction verification; and forensic metadata. Screenshots, informal messages, and verbal confirmations are insufficient in contested matters. Chain-of-custody principles apply to digital evidence. Where cryptographic assets are involved, independent expert verification may be required.

9.6 Platform-State Friction Doctrine

Digital estate disputes frequently reveal tension between public law (probate authority) and private contract (terms of service). Platforms may assert non-transferability, privacy restrictions, or internal policy limitations. Courts may assert estate representative authority and statutory override rights. Governance must navigate this friction without unlawful circumvention.

Unauthorized credential bypassing, hacking, or terms violation is inconsistent with institutional legitimacy. Dispute resolution must occur through formal engagement or judicial order.

9.7 Cryptographic Enforcement Limitations

Decentralized systems introduce structural enforcement constraints: irreversible transactions, absence of centralized reversal authority, public ledger transparency, and pseudonymous ownership. In such systems, court authority may not guarantee technical recovery. Doctrine must therefore recognize enforcement asymmetry.

Dispute governance shall include pre-transfer verification, forensic blockchain analysis, asset tracing, and custodial exchange freeze requests where applicable. Irreversibility elevates the importance of preventive governance.

9.8 AI and Identity Litigation Interface

AI continuation disputes may implicate false endorsement claims, emotional distress, moral rights, commercial exploitation, and personality rights. Courts may be asked to determine whether consent existed, whether representation is deceptive, and whether continuation violates public policy. Pending judicial clarity, governance doctrine defaults to transparency, suspension under dispute, and a non-commercial posture absent express authorization.

9.9 Cross-Border Enforcement Doctrine

Digital estates frequently implicate multiple jurisdictions. Structured analysis shall include: primary probate jurisdiction; location of beneficiaries; platform incorporation state; data storage location where known; and applicable data protection regimes. Enforcement feasibility must be assessed realistically. Where conflict exists between jurisdictions,

escalation to cross-border counsel may be required, mutual legal assistance frameworks may apply, and data transfer compliance must be reviewed. Practitioners shall disclose enforcement uncertainty.

9.10 Regulatory Interface

Disputes may intersect with data protection authorities, financial regulators, consumer protection agencies, and intellectual property offices. Institutional governance requires clarity on when a dispute escalates beyond probate court. Escalation to regulatory bodies must be documented, justified, and proportionate.

9.11 Beneficiary Standing Doctrine

Not all claimants possess equal standing in digital estate disputes. Standing may derive from economic interest, instrument designation, identity protection claim, or privacy exposure. Governance shall distinguish between lawful fiduciary authority and emotional objection without legal basis. This distinction reduces unnecessary escalation.

9.12 Liability Allocation and Professional Exposure

Digital disputes may generate liability exposure for fiduciaries, advisors, custodians, and platforms. Allocation analysis must evaluate scope of duty, documentation sufficiency, compliance with this Standard, and reasonableness of actions taken. Adherence to structured governance principles mitigates liability exposure.

9.13 Institutional Harmonization Imperative

Digital estate disputes will increase in frequency as digital identity persistence expands. Absent harmonized standards, courts may reach inconsistent conclusions, platforms may adopt unilateral policy dominance, and cross-border fragmentation may deepen. Domain 9 provides doctrinal scaffolding for institutional coherence. It does not displace judicial authority; it informs it.

9.14 Normative Requirements — Domain 9

Aligned systems and practitioners shall:

- Suspend destructive actions immediately upon identification of dispute.
- Produce instrument hierarchy analysis prior to dispute escalation.
- Preserve evidence logs in secure, court-ready form.
- Document enforcement feasibility for all cross-border assets.
- Apply L3 procedural posture to any asset where dispute risk is identified.

- Escalate contested AI continuation decisions pending legal determination.
- Maintain dispute records suitable for retrospective expert review.

Domain 10 — Professional Standards, Certification, and Continuing Competence

10.0 Purpose and Structural Role

Digital estate continuity is not a single-discipline practice. It intersects law, cybersecurity, data governance, fiduciary administration, AI ethics, cross-border regulation, and cryptographic custody. Domain 10 establishes the professional doctrine governing those who operate within this field.

Without structured professional standards: planning becomes inconsistent; enforcement becomes unreliable; ethical governance becomes discretionary; courts lack reference architecture; and certification becomes marketing rather than credential. This Domain defines professional identity, competency thresholds, ethical obligations, documentation standards, continuing competence requirements, certification governance principles, and institutional accountability.

10.1 Professional Identity Doctrine

Digital estate continuity constitutes a distinct professional field characterized by cross-disciplinary knowledge requirements, technology-aware fiduciary practice, jurisdictional sensitivity, and ethical governance obligations beyond statutory minimums. Practitioners in this Domain are not defined solely by licensure. They are defined by demonstrated competence in digital continuity governance.

Professional identity in this field requires: recognition of technological asymmetry between legal authority and technical control; understanding of AI and identity persistence implications; ability to assess cross-border enforcement feasibility; and structured risk disclosure capability. Digital estate governance shall not be treated as an ancillary checkbox within traditional estate planning.

10.2 Competency Architecture

Competence within digital estate continuity requires structured mastery across interlocking domains including:

- Digital Asset Classification and Risk Mapping
- Authority and Authorization Architecture

- Custody and Control Distinctions
- Cross-Border Legal Interface
- AI and Synthetic Identity Governance
- Post-Mortem Ethical Doctrine
- Dispute Resolution and Enforcement Mechanisms
- Platform-State Interaction
- Documentation and Audit Standards

Competence is not established through theoretical familiarity alone. It requires applied analytical capability. Practitioners shall recognize when escalation to technical or legal specialists is required.

10.3 Standard of Care in Digital Estate Continuity

The professional standard of care in this Domain shall include: structured risk identification; jurisdiction-aware analysis; disclosure of enforcement uncertainty; avoidance of overbroad access recommendations; avoidance of unlawful credential-sharing advice; transparency regarding platform limitations; and a conservative posture in AI continuation ambiguity.

Failure to account for technological irreversibility — such as blockchain transfers — may constitute breach of duty. The standard of care evolves as technological and regulatory conditions evolve.

10.4 Scope of Engagement Doctrine

Digital estate professionals must clearly define engagement boundaries. Engagement may include advisory planning, documentation drafting, fiduciary administration, platform coordination, cross-border advisory, and technical custody coordination. Practitioners shall disclose where services do not extend to tax planning in foreign jurisdictions, securities compliance, cybersecurity engineering, or AI model architecture review. Scope clarity reduces liability and preserves professional integrity.

10.5 Disclosure and Transparency Obligations

Professional integrity requires explicit disclosure of: cross-border enforcement uncertainty; platform refusal risk; cryptographic irreversibility; AI continuation ambiguity; and regulatory fragmentation. Clients must understand that digital continuity planning cannot guarantee universal enforceability. Disclosure shall be documented in writing.

10.6 Conflict of Interest Governance

Digital estate professionals may encounter conflicts including vendor affiliations, custodial partnerships, referral compensation, and platform accreditation incentives. Conflicts must be disclosed clearly. Professional advice shall remain technology-neutral and vendor-neutral. Certification frameworks shall prohibit credential use as platform endorsement absent explicit, transparent criteria.

10.7 Documentation and Recordkeeping Doctrine

Professional documentation shall include: digital asset inventory summaries; authority analysis memoranda; risk disclosure records; AI continuation briefing notes; cross-border analysis summaries; and platform engagement records. Documentation must be securely stored, accessible for audit, and retained according to jurisdictional requirements. Oral advisement without documentation is inconsistent with institutional-grade governance.

10.8 Continuing Competence Imperative

Digital infrastructure evolves rapidly. Professional competence must therefore be continuous. Continuing education shall address: emerging AI simulation technologies; cross-border regulatory updates; decentralized custody developments; platform policy changes; judicial decisions affecting digital access; and cybersecurity risk trends. Failure to maintain current awareness may constitute professional deficiency.

10.9 Certification Integrity Doctrine

Certification within digital estate continuity shall adhere to: transparent eligibility criteria; objective examination standards; separation from product marketing; ethical code enforcement; and due process in disciplinary review. Certification shall not function as brand endorsement or platform affiliation badge. It shall represent demonstrated competence within this Body of Knowledge.

10.10 Disciplinary and Oversight Architecture

Certification bodies shall maintain: complaint intake mechanisms; structured investigation procedures; evidentiary review standards; sanction guidelines; and appeal processes. Sanctions may include remedial education, suspension, and revocation. Disciplinary processes must preserve fairness while protecting public trust.

10.11 Institutional Accreditation Principles

Institutions providing digital estate services may seek accreditation under structured governance criteria. Accreditation evaluation may consider: authority verification procedures; audit logging capability; AI continuation policy clarity; cross-border compliance protocols;

and conflict-of-interest governance. Accreditation shall remain publicly examinable and vendor-neutral.

10.12 Liability Awareness and Risk Management

Digital estate practice introduces liability vectors including unauthorized disclosure, platform circumvention, cross-border regulatory violation, AI misrepresentation claims, and cryptographic asset mismanagement. Practitioners shall evaluate professional liability insurance scope, cyber liability coverage, and cross-border exposure. Risk management planning is integral to professional governance.

10.13 Cross-Disciplinary Collaboration Doctrine

Digital estate continuity frequently requires coordination among estate attorneys, data protection specialists, cybersecurity experts, cryptographic engineers, AI ethics advisors, and international law counsel. Professionals shall foster collaborative architecture rather than assume singular expertise sufficiency. Recognition of domain limits strengthens rather than weakens professional integrity.

10.14 Public Policy Engagement

Professionals operating under this Standard may contribute to legislative consultation, regulatory hearings, judicial education initiatives, and cross-border working groups. Engagement shall prioritize doctrinal coherence over commercial influence. Professional voices should support harmonization rather than fragmentation.

10.15 Professional Failure Modes

Common failure patterns include: overpromising enforceability; encouraging insecure credential sharing; ignoring AI continuation implications; neglecting cross-border conflict analysis; failing to document advisory risk; and treating digital assets as peripheral. Domain 10 exists to prevent these structural deficiencies.

10.16 Domain-Level Declaration

The DEPI Digital Estate Continuity Body of Knowledge and Standard™ affirms that digital estate continuity constitutes a structured professional discipline requiring demonstrated competence, ethical rigor, jurisdictional awareness, technology neutrality, documentation sufficiency, continuing education, and institutional accountability.

Professional governance is not supplementary to digital continuity. It is the enforcement mechanism that sustains it. Without structured professional standards: beneficiaries face harm; courts face inconsistency; platforms dominate interpretation; and trust in digital

continuity systems erodes. Domain 10 establishes the professional architecture necessary to operationalize the entirety of this Body of Knowledge and Standard in real-world advisory, fiduciary, and institutional contexts.

10.17 Normative Requirements — Domain 10

Professionals claiming DEPI alignment shall:

- Demonstrate competence across Domains 1–10 for applicable practice scope.
- Disclose jurisdictional limitations in writing to clients before engagement.
- Maintain continuing competence through periodic education aligned to this Standard.
- Avoid vendor-biased or platform-affiliated recommendations.
- Document engagement scope, known limitations, and liability disclosures prior to commencement.
- Escalate AI continuation and cross-border enforcement ambiguity rather than assume resolution.
- Maintain written records for all material advisory actions.

PART III — PROCESS FRAMEWORKS

Part III defines process frameworks that operationalize the doctrine established in Parts I and II. These frameworks serve two simultaneous roles: they establish common professional process language so that courts, regulators, fiduciaries, and certified practitioners can evaluate whether an estate's digital continuity posture was designed and administered with reasonable discipline; and they provide a consistent set of lifecycle processes that accredited organizations and certified professionals may implement to claim DEPI alignment.

Part III deliberately avoids prescribing local legal instruments, mandated forms, or a single workflow topology. Instead, it defines a portable process architecture implementable across jurisdictions and technologies.

> Interpretive Rule (Part III): "Shall" and "Must" statements in Part III apply only to voluntary DEPI alignment claims and do not override local law or controlling instruments.

Framework 1 — Digital Estate Continuity Lifecycle (DECL)

III.1 Overview

Digital continuity is not a document; it is a lifecycle. The lifecycle begins during life — while intent can be expressed and validated — continues through incapacity scenarios where authority operates without finality, and culminates in post-mortem administration where identity and rights persist across technical systems, contracts, and jurisdictions. The DECL defines the minimum conceptual phases required for continuity to be designed, maintained, triggered, executed, and closed with evidentiary defensibility. This framework is technology-neutral and applies whether assets are custodial, self-custodial, licensed, centralized, decentralized, or AI-mediated.

III.2 Lifecycle Phases

The lifecycle is composed of six phases. These phases are sequential in concept but may be iterative in implementation.

Phase A — Discovery and Inventory

Digital continuity fails most commonly at the earliest step: undiscovered assets, unknown licenses, inaccessible accounts, and undocumented custody models. Discovery is not

merely asset listing. It is the identification of what exists, where it resides, what controls it, what laws and contracts touch it, and what beneficiary harm could occur if mishandled.

An aligned program shall maintain a discovery method that includes, at minimum: asset identification across financial, identity, communications, creative, business, and sentimental categories; custody classification (custodial / self-custodial / hybrid); contractual characterization (owned vs. licensed; revocable vs. transferable); beneficiary liability risk classification (L1/L2/L3) as a first-class attribute; and a known location for authoritative inventory records and update responsibility.

An aligned practitioner must treat discovery as a repeatable professional activity with a recorded date, scope, and known limitations. Common output artifacts: Digital Asset Register (DAR); Custody and Control Map (CCM); License and Transferability Matrix (LTM); Beneficiary Liability Risk Map (BLRM); Known-Unknowns Log (KUL).

Phase B — Intent and Authority Architecture

Authority in digital estates is layered and frequently conflicting. Intent must be expressed in a manner that remains interpretable across probate rules, platform policies, data protection regimes, and cryptographic control realities. This phase reconciles human intent with lawful authority and operational feasibility.

An aligned program shall implement an authority architecture that: distinguishes access, ownership, and commercialization as separate governance decisions; identifies the authorized decision-maker for each asset class or risk tier; establishes instructions for licensed digital products consistent with contractual limitations; defines post-mortem communications authorization; defines any NIL-style derivative rights posture and representation constraints; and documents conflict resolution principles where platform designation tools conflict with testamentary instruments, or technical control conflicts with legal authority.

Output artifacts: Intent Declaration and Constraints Record (IDCR); Authority and Delegation Map (ADM); Post-Mortem Communications Authorization Schedule (PMCAS); Representation and Derivative Rights Schedule (RDRS).

Phase C — Continuity Design and Controls

This phase translates authority into operable continuity through controls, access gating, and governance safeguards. It is where planning becomes executable. Controls must anticipate loss of credentials, platform refusal, cross-border friction, cybersecurity threats, AI-driven identity misuse, and beneficiary liability events.

An aligned program shall implement controls appropriate to asset sensitivity and risk classification, custody model, jurisdictional exposure, and beneficiary liability risk tier. Required elements include: a documented recovery and access mechanism that avoids unlawful circumvention; role-based access segmentation; auditability for material actions; and a security-without-fragility posture.

Output artifacts: Continuity Control Plan (CCP); Access Tiering and Permissions Schedule (ATPS); Audit and Evidence Plan (AEP); Cross-Border Constraint Notes (CBCN).

Phase D — Maintenance and Drift Management

Digital estates drift continuously due to new accounts, changing passwords, platform policy updates, token migrations, employer changes, evolving family structure, and AI model proliferation. A continuity plan that is not maintained becomes a false assurance artifact.

An aligned program shall define maintenance intervals and triggers including: periodic review cadence; event-based reviews (marriage, divorce, relocation, new business, major asset acquisition, breach event); revalidation of authority appointments and platform designations; and refresh of custody maps and key control documentation. The program must record last review date, scope reviewed, changes made, and unresolved drift items.

Phase E — Triggered Activation (Incapacity / Death)

Activation is the transition from design state to operational execution. This transition is where authority is tested, disputes begin, and irreversible errors are most likely. Activation is not a single moment — it is a controlled escalation process defined by triggers.

Trigger types: Incapacity trigger (temporary, reversible governance posture; requires medical certification); Death trigger (final authority shift; requires death certificate or court documentation); Emergency trigger (security compromise, fraud event, extortion, or reputation crisis).

An aligned program shall define: trigger verification procedures; authority activation steps specifying who becomes empowered and under what scope; preservation-first rules upon dispute risk; platform engagement protocol; and logging of all activation actions and decisions.

Phase F — Administration, Transfer, Archival, and Closure

Administration includes transfer of assets where lawful and feasible, execution of licensing constraints, closure or memorialization choices, archival stewardship, AI continuation governance decisions, and completion of authorized post-mortem communications. Closure is not simply account deletion. It is the confirmation that authority was applied within scope,

beneficiaries were protected from foreseeable liability, evidence was preserved, and the estate's digital presence reached a defined end state.

An aligned program shall ensure administration includes: asset-by-asset disposition status (transfer / archive / memorialize / delete / unresolved); treatment consistent with IP, trade secret, and licensed product rules; beneficiary liability risk mitigation steps documented for L2/L3 assets; and documented handling of identity and representation artifacts including AI or synthetic risks. The program must produce an administrative closure record suitable for expert review.

Framework 2 — Role-Based Continuity Operating Model (RBCOM)

III.3 Overview

Digital continuity fails when responsibilities are implied rather than assigned. Because digital estates span legal, technical, and relational systems, they require a role-based operating model that can function across families, fiduciary structures, professional advisory teams, institutions, and platforms. RBCOM defines the minimal set of roles and interfaces required to execute the lifecycle reliably. This is not a licensing claim; it is an operating model. Local law may constrain who may serve in particular capacities.

III.4 Core Roles

RBCOM recognizes five primary roles. A single person may hold multiple roles, but role boundaries must remain explicit.

Principal

The individual or account holder. Expresses intent, configures continuity, and designates all other roles during life.

Continuity Fiduciary

The executor, trustee, or appointed representative who holds lawful authority. Approves material decisions. Ensures disputes trigger preservation and escalation. For DEPI alignment, the Continuity Fiduciary shall ensure decisions are within authority scope, documented, and beneficiary-safe.

Digital Operations Steward

The technical administrator who executes technical actions — exports, transfers, access control changes — under authority of the Continuity Fiduciary. Maintains chain-of-custody

logs. Avoids unauthorized circumvention. For DEPI alignment, the Steward must operate under documented delegation and within explicit scope.

Legal Authority Validator

The person or role that confirms which instrument governs which asset class, identifies cross-border conflicts and enforceability risks, and validates whether platform designation tools have legal effect under applicable law. For DEPI alignment, the Validator shall produce a brief, auditable authority memo when material disputes or L3 assets are involved.

Beneficiary Risk Guardian

This role exists because digital inheritance can create beneficiary exposure — financial, legal, reputational, and regulatory. The Guardian reviews proposed transfers of L2 and L3 assets and documents risk mitigation steps. For DEPI alignment, this role shall review and sign off on all L3 disposition decisions.

III.5 RACI Discipline

Aligned programs shall maintain a responsibility clarity model — RACI or equivalent — mapping who recommends, who approves, who executes, and who audits for each major asset category and risk tier.

III.6 Escalation and Separation of Powers

Aligned programs must define escalation paths where authority is disputed, platform refusal occurs, AI continuation is requested, or L3 beneficiary liability risk is present. Separation of powers is encouraged where feasible: the fiduciary approves, the steward executes, the guardian reviews.

Framework 3 — Authority and Evidence Protocol (AEP)

III.7 Overview

Digital estate continuity is frequently challenged not at the level of intent, but at the level of proof. Courts, platforms, regulators, beneficiaries, and counterparties do not evaluate intentions; they evaluate documentation, authority, and evidentiary sufficiency. The AEP establishes the structured method by which authority is validated, scope is confirmed, evidence is preserved, actions are defensible, chain-of-custody is maintained, and expert-witness scrutiny can be satisfied.

This framework exists because digital estates introduce three evidentiary distortions: technical control may precede legal authority; irreversible actions may occur before

validation; and platform rules may demand standardized documentation not aligned with probate structure. The AEP reconciles these distortions.

III.8 Core Principles of the AEP

- Verification Before Execution — no material action should occur before authority scope is confirmed.
- Preservation Before Resolution — where ambiguity exists, destructive actions shall be paused.
- Documentation Before Defense — if an action cannot be documented, it cannot be defended.
- Scope Before Access — authority may be broad in one asset class and narrow in another.
- Auditability Before Closure — closure without evidence invites future contest.

III.9 Authority Validation Process

Authority validation requires layered analysis.

Step 1 — Instrument Hierarchy Review. The reviewing party shall identify and compare express digital directives, testamentary instruments, powers of attorney, court appointments, platform designation tools, and applicable statutory digital access provisions. Conflicts must be documented explicitly rather than assumed resolved. For DEPI alignment, authority validation shall produce a short written Authority Validation Memorandum (AVM) for L3 risk assets, disputed authority, cross-border complications, AI continuation requests, and commercialization of identity.

Step 2 — Jurisdictional Alignment Check. Authority must be tested against the governing probate jurisdiction, the platform terms of service jurisdiction, the data protection jurisdiction, and the location of relevant servers where material. For DEPI alignment, the Validator must document known enforcement constraints.

Step 3 — Scope Determination. Authority may permit viewing, managing, transferring, deleting, commercializing, or representing. These are not interchangeable. Scope must be documented per asset category.

III.10 Evidence Preservation Protocol

Evidence preservation begins when activation occurs, dispute risk is identified, platform refusal is anticipated, or L3 liability exposure is present. Aligned programs shall implement: access logging; export of relevant communications where lawful; preservation of account

metadata; blockchain transaction snapshots with timestamp verification; and backup of authority documentation. Where feasible, forensic-level copies should be created without altering the original record state.

III.11 Chain-of-Custody Documentation

For DEPI alignment, material actions must record: who authorized; who executed; when executed; under what instrument; under what jurisdiction; what asset category; and what outcome. This documentation must be retained in secure form and be reviewable for audit or litigation.

III.12 Platform Engagement Documentation Package (PEDP)

Platforms often require structured documentation. Aligned programs shall prepare a standardized engagement package containing: verified death certificate or incapacity certification; letters testamentary or equivalent appointment; government identification of fiduciary; summary authority memo; citation of relevant statutory authority where applicable; and a clear request statement specifying access, memorialization, transfer, or export. The engagement package should avoid credential circumvention, informal email-based access attempts, and unauthorized password reset tactics. Platform engagement must remain lawful.

III.13 Cryptographic Asset Evidence Standards

Self-custodied digital assets require special treatment. Aligned programs shall document: public wallet address; transaction history verification; known key control state (single-signature, multi-signature, hardware-based, etc.); and known recovery mechanisms. Where private key possession is contested, forensic blockchain analysis may be required. Irreversible transfer risk necessitates heightened documentation.

III.14 AI and Representation Evidence Protocol

Where AI continuation or synthetic identity tools are involved, aligned programs shall document: consent evidence where any exists; scope of authorized use; labeling requirements; commercialization restrictions; and jurisdictional personality rights considerations. Absent documented consent, synthetic continuation should be paused pending review.

III.15 Beneficiary Liability Evidence Controls

For L2 and L3 risk assets, aligned programs shall record: nature of potential liability; mitigation steps taken; professional consultations obtained where any; and communication

to beneficiary regarding risk exposure. This documentation protects both fiduciary and beneficiary.

III.16 Dispute Escalation Record

Where disputes arise, aligned programs must create a dispute record containing: nature of dispute; parties involved; preservation steps taken; authority basis; jurisdictional constraints; external counsel involvement; and status and outcome. Digital disputes frequently resurface years later; records must support retrospective expert review.

III.17 Closure Certification Record

Upon completion of administration, aligned programs shall produce a Closure Certification Record (CCR) including: asset disposition status; authority confirmation; evidence preservation confirmation; unresolved matters log; and archival location of records. The CCR provides defensible closure.

III.18 Expert-Witness Readiness Standard

For DEPI alignment, a digital estate administration shall be capable of surviving expert scrutiny under the following test: Could an independent expert determine who had authority; what actions were taken; why they were lawful; whether risk was considered; whether beneficiary exposure was mitigated; and whether platform and jurisdictional constraints were acknowledged? If the answer is no, documentation is insufficient.

Framework 4 — Risk-Tiered Disposition Framework (RTDF)

III.19 Overview

Not all digital assets present equal consequences when transferred, retained, deleted, or commercialized. Some assets are economically simple and low exposure. Others embed contractual restrictions, regulatory implications, reputational sensitivity, or downstream liability risk. The RTDF operationalizes the L1/L2/L3 classification into a structured, defensible administration pathway.

RTDF does not override local inheritance law, redefine ownership, or prescribe distribution outcomes. It defines how process intensity and documentation depth scale according to risk exposure. This framework exists to prevent the most common structural failure in digital estate administration: treating all digital assets as if they are equivalent. They are not.

III.20 Foundational Principles

- Proportional Governance — process rigor shall scale to risk exposure.

- Liability Awareness — beneficiary exposure, not only asset value, drives administrative caution.
- Contractual Realism — licensed digital products and platform-governed assets must be handled within contractual constraints.
- Preservation Before Escalation — higher risk tiers trigger heightened preservation posture.
- Documentation Before Disposition — disposition of higher-risk assets requires written analysis prior to execution.

III.21 Disposition Pathways by Risk Tier

L1 Disposition Pathway

L1 assets shall require: authority confirmation; basic inventory confirmation; documentation of transfer, archive, or deletion decision; and record of execution. No formal risk memorandum is required. Audit log recommended but not mandatory unless dispute risk exists. The presumption for L1 assets is administrative efficiency.

L2 Disposition Pathway

L2 assets shall require: authority validation memo (short form acceptable); contractual transferability review; license status check (owned vs. licensed); beneficiary acknowledgement of ongoing obligations where applicable; and a disposition log with scope rationale. If commercialization or ongoing operational continuity is contemplated, a short Continuity Impact Note (CIN) shall be created. The presumption for L2 assets is controlled caution.

L3 Disposition Pathway

L3 assets must require: formal Authority Validation Memorandum (AVM); jurisdictional alignment review; contractual and regulatory exposure analysis; Beneficiary Liability Risk Memorandum (BLRM); written decision approval by Continuity Fiduciary; separation-of-roles review where feasible; audit trail preserved; and documented escalation pathway. Where AI identity or NIL-style rights are implicated, additional consent and labeling review is required before any continuation or commercialization. The presumption for L3 assets is defensive conservatism.

III.22 Disposition Modalities

RTDF distinguishes five disposition modalities: Transfer (lawful ownership or control reassignment); Archive (preservation without active control transfer); Memorialize (public presence preserved but restricted); Delete (lawful removal consistent with authority);

Commercialize/Continue (ongoing revenue or operational activity). For L3 assets, commercialization shall never occur without explicit authority and documentation.

III.23 Licensed Digital Product Handling

Licensed digital products may be non-transferable, may terminate upon death, or may prohibit account sharing. For DEPI alignment, licensed products shall be reviewed against contract terms, local law, and platform survivorship rules. Transfer attempts that violate contract should not be pursued without lawful basis.

III.24 Intellectual Property and Trade Secret Governance

Where assets contain IP or trade secrets, RTDF requires: ownership verification; registration status confirmation where applicable; trade secret confidentiality mapping; controlled access during review; and documentation of any disclosure. Trade secrets transferred without confidentiality controls may destroy value. L3 presumption applies.

III.25 Representation and NIL-Style Derivative Rights

Where digital identity, likeness, or persona value is involved, RTDF requires: confirmation of express authorization; jurisdictional personality rights review; commercial scope limitation documentation; and labeling standards compliance where continuation occurs. Absent explicit authorization, continuation for commercial gain should be paused.

III.26 Beneficiary Liability Mitigation Controls

For L2 and L3 assets, aligned programs shall document: potential regulatory exposure; tax implications at high level with referral to specialist as needed; ongoing subscription or contractual liabilities; data protection exposure; and reputation exposure. Beneficiaries should be informed in writing of known material exposure risks before transfer.

III.27 Dispute Sensitivity Override

If dispute risk arises at any tier, asset handling shall escalate to L3 procedural posture until dispute resolution clarifies scope. This override protects continuity integrity.

III.28 Administrative Efficiency Safeguard

RTDF is not designed to paralyze administration. L1 assets should not be over-governed; L2 assets should not be escalated unnecessarily; L3 rigor should be applied only when the risk profile justifies it. Proportionality is essential to preserve practicality.

Framework 5 — Platform Engagement and Refusal Playbook (PERP)

III.29 Overview

Digital estates exist largely within privately governed technological ecosystems. Platforms, custodians, exchanges, SaaS providers, hosting environments, and AI service operators function as quasi-jurisdictional actors, establishing contractual access rules, transfer restrictions, memorialization policies, non-transferability clauses, identity verification requirements, and internal dispute escalation channels. These private governance systems often intersect — and at times conflict — with probate law, fiduciary authority, data protection regimes, and cross-border enforcement rules.

PERP establishes a structured, lawful, defensible method for interacting with platforms during digital estate administration. PERP exists to prevent two common failure modes: informal or unauthorized access attempts; and unstructured confrontation with platform refusal leading to premature escalation or abandonment. PERP does not override platform contracts or local law. It defines a disciplined engagement posture consistent with DEPI alignment.

III.30 Foundational Principles of Platform Engagement

- Lawful Posture First — engagement shall occur through formal, documented channels before technical intervention is contemplated.
- Preservation Before Confrontation — where refusal risk exists, destructive actions must be paused.
- Documentation Before Escalation — escalation requires documented authority and evidence.
- Platform Neutrality — engagement must remain professional and non-adversarial until formal dispute is necessary.
- Jurisdictional Awareness — platform domicile and governing law clauses influence escalation options.
- Non-Circumvention — unauthorized bypass of technical controls is inconsistent with DEPI alignment.

III.31 Engagement Phases

Phase 1 — Pre-Engagement Preparation

Before contacting a platform, aligned programs shall confirm: authority validation complete (AEP applied); risk tier identified (RTDF applied); scope of request clearly defined (access, export, memorialization, deletion, or transfer); applicable jurisdiction identified; and platform terms reviewed for transferability and survivorship tools. For L3 assets, a Platform Engagement Brief (PEB) should be prepared summarizing authority basis, scope of request, legal citation where applicable, risk tier, and anticipated refusal grounds. Preparation prevents fragmented engagement.

Phase 2 — Formal Request Submission

Engagement should occur through the platform's designated legacy or estate portal, formal written correspondence, or documented submission channels. Requests shall include: verified authority documentation; government identification; clear articulation of request; citation to applicable law where relevant; and statement of compliance with platform terms. Informal email exchanges without documentation are discouraged.

Phase 3 — Clarification and Supplemental Documentation

Platforms may request additional identity verification, court orders, translations, notarization or apostille, or local counsel engagement. For DEPI alignment, supplemental documentation shall be logged and reviewed for proportionality relative to risk tier. Excessive or unreasonable documentation demands may trigger escalation evaluation.

Phase 4 — Refusal Assessment

Platform refusal may arise due to non-transferability clauses, privacy restrictions, insufficient documentation, jurisdictional conflict, technical infeasibility, or internal policy limitations. Refusal assessment requires analysis of whether refusal is contractually justified, whether statutory override may apply, whether a court order could compel compliance, and whether an alternative asset recovery path exists. For L3 assets, refusal analysis shall be documented in a Refusal Assessment Memorandum (RAM).

Phase 5 — Escalation Pathways

Escalation may include: internal platform appeal; formal legal notice; court petition; regulatory complaint; or cross-border judicial cooperation request. Escalation must remain proportional to asset materiality, beneficiary exposure, reputational impact, and enforcement feasibility. Unnecessary escalation may generate cost without recovery benefit.

III.32 Cross-Border Platform Conflict

Where platform domicile differs from probate jurisdiction, aligned programs shall consider: recognition of foreign court orders; data transfer restrictions; GDPR-like regulatory

implications; and platform arbitration clauses. Cross-border conflict should trigger consultation with jurisdictionally competent counsel for L3 assets.

III.33 Non-Circumvention Doctrine

Credential possession or technical ability does not legitimize access if: authority is unclear; contract prohibits transfer; platform has refused formal request; or jurisdiction prohibits access. For voluntary DEPI alignment, circumvention of technical protections shall not occur absent lawful authority and legal review. Unauthorized access may expose fiduciaries to civil or criminal liability.

III.34 Preservation During Platform Dispute

If dispute or refusal is ongoing, aligned programs shall: preserve all communications; avoid account deletion; avoid transfer attempts; document platform positions; and secure parallel evidence where lawful. Preservation supports later judicial review.

III.35 Emergency Situations

Certain scenarios may require accelerated engagement: ongoing fraud; account compromise; active business operations requiring continuity; or reputation crisis involving unauthorized AI representation. Emergency engagement should notify platform of urgency, invoke fraud or security response channels, maintain documentation, and apply preservation doctrine. Emergency posture does not suspend authority validation.

III.36 AI and Synthetic Identity Platforms

Where platforms host AI-generated or identity-replicating tools, engagement must address consent status, labeling obligations, commercialization scope, and personality rights jurisdiction. Platforms may lack established policies; escalation should remain measured and documented.

III.37 Documentation Requirements

Each material platform engagement shall record: date of contact; submission method; documents provided; platform response; follow-up actions; and escalation decision where any. Documentation must be retained consistent with AEP standards.

III.38 Closure of Platform Engagement

Platform engagement concludes when access is granted and disposition completed, memorialization completed, transfer completed, deletion lawfully executed, judicial resolution

obtained, or enforcement deemed infeasible and documented. Closure record should reference authority basis, risk tier, final outcome, and any unresolved limitations.

Framework 6 — Post-Mortem Communications and Representation Process (PMCRP)

III.39 Overview

Digital continuity does not end with asset transfer. In many estates, the most sensitive decisions concern speech, identity, likeness, voice, persona, and narrative continuation. Post-mortem communications may include public statements issued in the decedent's name, account updates or memorial messages, ongoing brand or influencer content, AI-generated speech or likeness, licensing of image, voice, or personality, NIL-style derivative uses, and management of historical digital archives.

PMCRP establishes the structured method by which such communications and representations are authorized, scoped, labeled, risk-assessed, jurisdictionally reviewed, and documented. PMCRP does not mandate speech; it governs when speech or representation occurs.

III.40 Foundational Principles

- Intent Primacy — no post-mortem communication or representation should occur absent express or inferable authorization.
- Representation Distinction — administrative notice is distinct from representational speech.
- Transparency Obligation — synthetic or representative communications must not mislead.
- Jurisdictional Sensitivity — personality, image, and publicity rights vary across jurisdictions.
- Commercial Boundary Awareness — commercial exploitation requires explicit authorization and legal review.
- Risk-Tier Proportionality — L2 and L3 representation actions require structured review.
- Preservation of Identity Integrity — continuation must not distort or materially misrepresent the decedent's identity.

III.41 Classification of Post-Mortem Communications

Administrative Notice

Factual statements: death announcement, memorialization notice, estate contact instructions. Administrative notice does not require consent for representation but must remain accurate and non-exploitative.

Stewarded Communication

Messages issued by fiduciary or authorized representative clearly labeled as such. Must avoid implying the decedent authored the communication, avoid expansion beyond authority scope, and preserve historical content integrity unless modification is lawfully justified.

Legacy Continuation Communication

Ongoing operation of brand or channel consistent with express authorization. Requires contractual compliance with platform rules, beneficiary liability review (L2 or L3), tax and regulatory referral where appropriate, and documentation of scope and decision rationale. Continuation without authority risks misrepresentation and liability.

Synthetic Communication

AI-generated or algorithmically constructed speech in the decedent's likeness or voice. Shall require: express consent (preferred); jurisdictional personality rights review; clear labeling of synthetic nature; commercial boundary documentation; and beneficiary risk acknowledgment. Absent documented consent, synthetic communication should not proceed.

Derivative Commercial Representation

Licensing or monetized use of image, likeness, voice, or identity. Requires: confirmation of transferability under governing law; confirmation of ownership of underlying IP; delineation between economic rights and moral rights; and documentation of commercial scope. Commercial exploitation without lawful basis is prohibited under DEPI alignment.

III.42 Authorization Verification

Before any post-mortem communication occurs, aligned programs shall confirm: whether express authorization exists; whether limitation clauses exist; whether commercialization is permitted; whether jurisdiction recognizes transferable publicity rights; and whether licensing agreements govern identity elements. For L3 representations, a formal AVM is required. Absent explicit authorization, synthetic or commercial representation shall not proceed under DEPI alignment.

III.43 Reputation Risk Review

Before public communication, aligned programs shall evaluate reputational impact, risk of defamation or misrepresentation, privacy exposure, family conflict potential, and cross-cultural sensitivity. For L3 identity events, a short Reputation Risk Assessment (RRA) should be recorded.

III.44 Cross-Border Representation Considerations

Personality rights vary: some jurisdictions recognize post-mortem publicity rights; others limit or extinguish such rights; moral rights may remain perpetual in certain systems. Aligned programs shall document jurisdictional review where commercial representation occurs, AI simulation is activated, or cross-border audiences are targeted.

III.45 Beneficiary Consent and Objection

Where multiple beneficiaries exist, aligned programs should identify whether consent unanimity is required, document objections, escalate disputes before representation proceeds, and apply preservation doctrine when contested. Representation should not proceed while a material dispute exists.

III.46 Documentation Requirements

For DEPI alignment, material representation actions shall record: authorization basis; risk tier; jurisdictional considerations; labeling decision; beneficiary notification where applicable; commercial scope where any; date and executor identity. These records must be retained under AEP standards.

III.47 Termination of Representation

Post-mortem communications and representations should not be indefinite without review. Aligned programs shall define review cadence for ongoing representation, sunset conditions, and termination triggers such as dispute or regulatory change. Digital identity continuation must not drift into unsupervised persistence.

Framework 7 — Cross-Border Execution Framework (CBEF)

III.48 Overview

Digital estates are inherently transnational. A single individual may reside in one jurisdiction, hold citizenship in another, operate businesses in multiple countries, store data across globally distributed servers, use platforms incorporated under foreign law, and maintain crypto assets governed by no centralized jurisdiction. Traditional probate assumes territorial coherence. Digital infrastructure does not. CBEF establishes a structured, jurisdiction-aware

methodology for administering digital estates where multiple legal systems apply, enforcement may be fragmented, data protection rules conflict, and platform domicile diverges from probate authority. CBEF does not harmonize law. It provides a disciplined process for navigating divergence.

III.49 Foundational Principles

- Legal Supremacy Doctrine — local governing law remains controlling; DEPI alignment does not override statutory authority.
- Jurisdictional Layering — digital estates often implicate more than one jurisdiction simultaneously.
- Enforcement Realism — not all foreign orders are enforceable in practice.
- Data Sovereignty Awareness — data localization and transfer restrictions must be respected.
- Platform Domicile Relevance — platform incorporation and governing law clauses materially influence outcomes.
- Identity Rights Variability — post-mortem personality and publicity rights differ significantly across jurisdictions.
- Regulatory Exposure Sensitivity — certain assets may trigger foreign regulatory scrutiny upon transfer.
- Documentation Before Escalation — cross-border assumptions must be documented before action.

III.50 Cross-Border Trigger Identification

CBEF activates when any of the following conditions exist: principal residence differs from asset domicile; platform governing law differs from probate jurisdiction; beneficiaries reside in foreign jurisdictions; data stored in a jurisdiction with a restrictive transfer regime; crypto assets or exchanges located abroad; AI or identity rights governed by foreign statute; or business operations cross national boundaries. Cross-border triggers shall be recorded in the administrative file for all material assets.

III.51 Jurisdiction Mapping Process

Aligned programs shall identify: principal domicile; probate court jurisdiction; citizenship(s); location of beneficiaries; platform incorporation and governing law; data storage region where material; location of custodial financial institutions; applicable data protection regimes; and location of business registrations where applicable. This produces a Jurisdictional Exposure Map (JEM).

III.52 Governing Law Conflict Analysis

Where multiple jurisdictions are implicated, aligned programs shall assess which law governs succession, contractual relationships, data protection, publicity and personality rights, cryptocurrency regulation, and tax obligations. For L3 assets, a short Cross-Border Alignment Memorandum (CBAM) should be created summarizing conflicts identified, enforcement uncertainties, and escalation recommendations.

III.53 Data Protection and Transfer Compliance

Cross-border execution frequently implicates GDPR-style restrictions, data export controls, sector-specific privacy laws, and biometric and health data restrictions. Aligned programs shall identify whether representative access triggers cross-border data transfer, determine whether standard contractual clauses or adequacy findings are relevant, and avoid unauthorized bulk export of data without lawful basis. High-risk data categories — biometric, medical, financial, minor data — require heightened review.

III.54 Recognition of Foreign Court Orders

Foreign court orders may require recognition proceedings, apostille or legalization, local counsel validation, or reissuance under domestic jurisdiction. Aligned programs shall not assume automatic enforceability. Where enforcement feasibility is uncertain, the limitation shall be documented.

III.55 Platform Governing Law Clauses

Platforms frequently include arbitration clauses, exclusive jurisdiction provisions, choice-of-law clauses, and non-transferability clauses. CBEF requires analysis of whether the governing law clause supersedes local probate authority, whether statutory override provisions exist, and whether the arbitration clause binds the estate representative. For L3 disputes, consultation with jurisdictionally competent counsel is recommended.

III.56 Cryptocurrency and Decentralized Systems

Crypto assets introduce jurisdictional ambiguity: nodes distributed globally, wallet ownership pseudonymous, exchanges domiciled abroad, and enforcement limited by technical architecture. Aligned programs shall: identify exchange domicile where custodial; identify applicable regulatory regime; assess tax consequences under both domicile and beneficiary jurisdiction; and document technical recovery feasibility. Enforcement realism applies: court authority may not compel decentralized protocol action.

III.57 Cross-Border Tax Exposure Awareness

Digital assets may trigger estate taxes, capital gains taxes, VAT or sales tax implications, withholding obligations, and transfer taxes. CBEF does not provide tax advice. For DEPI alignment, cross-border tax exposure risk shall be identified and referred to qualified advisors where material.

III.58 Cross-Border Dispute Escalation

Where conflict arises between probate authority and platform domicile, data protection authority and estate representative, or multiple national inheritance rules, aligned programs shall evaluate escalation options including mutual legal assistance treaties, cross-border judicial recognition, local counsel engagement, regulatory complaint, and controlled asset freeze where lawful. Escalation must remain proportionate to materiality and recovery feasibility.

III.59 Preservation in Cross-Border Dispute

Where jurisdictional conflict creates uncertainty: destructive actions shall be paused; asset transfers shall be suspended; representation shall not proceed; and evidence shall be preserved. Preservation doctrine applies until conflict is resolved.

III.60 Documentation Requirements

For DEPI alignment, cross-border files shall include: Jurisdictional Exposure Map (JEM); Cross-Border Alignment Memorandum (CBAM) for L3 assets; data transfer compliance notes; platform domicile analysis; enforcement feasibility summary; and professional referral record where applicable.

Framework 1A — Continuity Workflow Specifications

This framework specifies the step-by-step operational procedures for each of the six continuity workflow types. These procedures are referenced by Framework 1 (DECL) Phase E and are binding on all DEPI-aligned platforms.

PF-1 Primary Continuity Workflow

The primary workflow is the baseline process used for initial configuration, updates, identity transitions, and continuity planning. It establishes the continuity posture from which all other workflows operate.

Step 1 — Identity Verification. The user verifies identity via MFA, cryptographic key, or institutional authentication. Step 2 — Asset Discovery or Import. Assets are automatically detected or manually imported and classified per Domain 2 taxonomy. Step 3 — Continuity

Configuration. The user configures delegates, triggers, inheritance rules, visibility rules, emotional asset timing, and SMB continuity mappings. Step 4 — Metadata Binding. Continuity metadata is bound to each asset, off-chain or on-chain as appropriate. Step 5 — Backup Continuity Creation. Platforms must create fallback continuity paths ensuring no single point of failure. Step 6 — Review and Finalization. Users review their complete Continuity Plan and provide documented confirmation.

PF-2 Emergency Access Workflow

This workflow is triggered when a user is medically incapacitated, temporarily unable to authenticate, unresponsive but not deceased, experiencing a technical lockout, or in a crisis requiring third-party intervention. Emergency access does not imply post-mortem rights.

Step 1 — Trigger Event. Activation may be initiated by delegated request, emergency contact request, biometric unavailability, device loss, or automated risk-engine detection. Step 2 — Identity Verification of Requestor. Strict but rapid verification of the emergency requestor is required before any access is granted. Step 3 — Access Scope Determination. Only assets pre-designated as emergency-accessible are made available; scope must be explicitly bounded. Step 4 — Time-Limited Access Window. Access automatically closes after the defined window unless formally extended by an authorized party. Step 5 — Logging and Audit. Full transparency is required; all emergency access events must be logged with timestamp, identity, and scope.

Platforms must implement: automatic scope limitation preventing access to emotional and high-risk assets; a mandatory reversion mechanism returning to normal governance state; and real-time notification to the principal where technically possible.

PF-3 Executor and Trustee Workflow

This workflow governs access by legally authorized successors following a verified death or incapacity event.

Step 1 — Submission of Legal Documentation. The executor or trustee submits: death certificate; letters testamentary or trustee appointment; and any applicable court orders. Step 2 — Identity Verification of Executor. Multi-factor, document-based, and biometric verification where available. Step 3 — Authority Mapping. Asset categories determine what may be accessed; authority is proportional to legal documentation. Step 4 — Continuity Mode Activation. The system transitions to post-mortem or continuity governance mode, freezing user identity and AI models. Step 5 — Access Release. Read-only access is provided for sensitive and emotional assets; full access for financial accounts where legally permitted; operational access for SMB accounts per delegation mapping. Step 6 — Inheritance

Execution. Triggered according to legal documents and user-defined rules; follows asset-category-specific procedures. Step 7 — Audit and Logging. Every action is logged with timestamp, executor identity, authority basis, and asset category.

PF-4 Family Continuity Workflow

This workflow governs the inheritance of emotional digital assets, legacy letters, future messages, memory archives, AI-generated identity or memory models, and sentimental content.

Step 1 — Verification of Beneficiary Identity. Non-financial verification is permitted with appropriate restrictions; lower-bar identity confirmation may apply for minor beneficiaries under guardian oversight. Step 2 — Visibility Rules Applied. Beneficiaries see only what they are explicitly authorized to access per the user's continuity configuration. Step 3 — Staged Releases. Time-based or milestone-based release of letters, videos, messages, and memory archives as pre-configured. Step 4 — Ethical Handling of AI Models. AI memories and personas must be frozen in post-mortem state; must not evolve without explicit configuration; and must be clearly labeled as AI-generated assets. Step 5 — Download and Preservation Options. Families must be able to save emotional assets offline in standard formats. Step 6 — Permanent Archival Options. Platforms must support long-term preservation for the retention period specified by the user.

Immersive Memory Experience Delivery. Platforms must support inheritance of volumetric recordings, holographic messages, and spatial family memories with encryption, staged exposure, and emotional harm safeguards. Platforms must provide exportable formats (.usdz, .glb, .mp4 fallback), cross-platform compatibility, and long-term rendering support.

PF-5 SMB Continuity Workflow

For small and medium businesses, continuity workflows must ensure business operations continue, employees retain access, customers are not harmed, business data is preserved, and digital identity is transferred to the successor. Platforms must prevent SMB shutdown due to sole-owner digital failure.

Step 1 — Key-Person Risk Identification. Identify individuals whose absence jeopardizes business continuity. Step 2 — Continuity Delegation Assignment. Assign designated roles: IT administrator, operations lead, and financial controller. Step 3 — Trigger Event. Activation occurs upon incapacity, death, emergency, or planned offboarding. Step 4 — Identity Transition. Business accounts transition to designated continuity managers per the authority map. Step 5 — Operational Recovery. Systems are brought back online per the documented

recovery procedure. Step 6 — Authority Reassessment. New leadership transitions must be formally recorded and authenticated.

PF-6 High-Risk Asset Workflow

High-risk assets requiring this workflow include: crypto wallets without recovery mechanisms; smart-contract-locked assets; password vaults; cloud accounts controlling financial or legal operations; AI-powered accounts; and blockchain assets protected only by a single seed phrase. Platforms must not allow users to configure continuity that results in irreversible asset loss.

Step 1 — Risk Classification. Asset must be formally classified as high-risk per the L3 criteria in Domain 2. Step 2 — Mandatory Warning to User. Platform must display explicit risk disclosures before configuration is accepted. Step 3 — Mandatory Backup and Recovery Plan. A documented recovery pathway must exist before the asset is accepted into the continuity plan. Step 4 — Mandatory Multi-Party Continuity. No high-risk asset may be governed by a single-party control structure. Step 5 — Mandatory Delegation or Executor Assignment. A verified continuity fiduciary must be assigned. Step 6 — Increased Verification Upon Access Requests. All access to high-risk assets requires heightened verification regardless of trigger type.

PF-7 Post-Mortem Workflow

This workflow begins once death is verified and governs the complete transition from user-controlled to executor-controlled digital estate administration.

Step 1 — Notification Event. Triggered by: executor; trusted contact; legal authority; verified obituary; medical institution; or blockchain oracle where configured for blockchain systems.

Step 2 — Verification and Validation. Platform must: verify all submitted documentation; authenticate the requestor; cross-reference the estate plan on file; and apply risk-engine checks to detect fraudulent claims.

Step 3 — Executor Identity Verification. Requires: government-issued identification; legal appointment documents; multi-factor authentication; and biometric or verifiable credential verification. Hybrid verification methods are permitted.

Step 4 — Continuity Mode Activation. Platform transitions to continuity mode: user identity is frozen; AI models are frozen; configured triggers are activated; delegate permissions are restricted; and executor authority is formally mapped.

Step 5 — Asset Inventory Release. Executor receives a categorized inventory showing access levels per asset, emotional asset separations, and AI asset summary. Assets

themselves are not immediately released; only the authorized inventory is provided at this stage.

Step 6 — Inheritance Execution. Execution proceeds by asset category: for digital identity access, limited view is provided for executors; for financial assets, full or partial release per applicable legal rules; for emotional assets, staged release with encrypted content delivery; for blockchain assets, multi-sig release, key recovery workflows, and smart contract execution logs.

Step 7 — Account Closure or Preservation. Accounts are closed per will, trust, or default protocol; accounts are preserved if explicitly configured; AI assets are archived or deleted per user directive.

Step 8 — Final Audit and Reporting. Platforms must generate: continuity logs; executor audit reports; asset transfer summaries; long-term preservation packets; and a certificate of inheritance completion.

PART IV — NORMATIVE STANDARD REQUIREMENTS

Part IV establishes the formal alignment requirements for entities and professionals claiming voluntary conformance with the DEPI Digital Estate Continuity Body of Knowledge and Standard™ v1.3. Part IV does not create new legal obligations. It defines voluntary structural requirements that operationalize Parts I–III, provide measurable alignment criteria, enable accreditation and certification under Part V, and support judicial, regulatory, and institutional reference.

> Where conflict exists between DEPI alignment and governing law, governing law prevails under the Legal Supremacy Doctrine defined in Part I. Alignment may apply at Program Level (institutional programs), Professional Level (individual practitioners), Case Level (specific estate administration instances), or Platform/Custodial Level (service providers adopting DEPI governance architecture).

Section IV-A — Governance and Structural Requirements

IV.1 Governance Foundation

An entity claiming DEPI Program-Level Alignment shall maintain a documented digital estate continuity governance policy; defined role assignments consistent with RBCOM; a written authority validation procedure; a risk-tiered disposition methodology with L1/L2/L3 integrated; a platform engagement procedure; a cross-border review mechanism; and post-mortem representation governance controls. These policies shall be written, version-controlled, reviewable, and available for audit.

IV.2 Identity Continuity Requirements

- Support recovery without estate lockout.
- Verify executor identity and authority before granting access.
- Log identity state transitions and revocations.
- Prevent single-key dependency for cryptographic identity.
- Freeze AI identity layers upon verified death by default.

IV.3 Asset Classification and Rights Requirements

- Classify assets by ownership, transferability, and licensing for all material digital assets.
- Flag licensed non-transferable assets explicitly in continuity plans.
- Distinguish token ownership from underlying IP rights.
- Apply beneficiary-centric L1/L2/L3 risk classification.
- Classify emotional, biometric, and AI-derived assets with heightened governance.

IV.4 Beneficiary Protection Controls

- Prevent beneficiary exposure to illegal withdrawal actions without legal authority.
- Prevent discretionary impersonation-by-default.
- Provide read-only modes where appropriate for L2 assets.
- Provide mandatory warnings and confirmations for all L3 actions.
- Notify beneficiaries in writing of material L2/L3 exposure risks before transfer.

IV.5 Digital Execution Plan Requirements

- Generate structured DEP with inventory, entitlement mapping, risk classification, and rights structure.
- Version DEP upon each material change.
- Ensure DEP is exportable and interpretable by non-technical executors.
- Support sharing to authorized professionals with consent.
- Prohibit DEP from being represented as a testamentary instrument.

Section IV-B — Operational and Documentation Requirements

IV.6 Lifecycle Implementation

- Implement a lifecycle consistent with DECL (Framework 1), with all six phases identifiable in documentation.
- Define and document maintenance intervals and event-based review triggers.
- Record last review date, scope reviewed, changes made, and unresolved drift items.

IV.7 Documentation and Auditability

- Maintain action logs for all material decisions.
- Maintain evidence preservation records.
- Produce Platform Engagement Documentation Packages for all platform interactions.
- Produce risk memoranda for all L3 assets.

- Produce Closure Certification Records upon completion of administration.
- Retain documentation in secure form reviewable for audit.

IV.8 Platform Engagement

- Engage platforms through lawful, documented channels.
- Avoid technical circumvention of platform security controls.
- Document refusal analysis for each platform refusal encountered.
- Apply proportional escalation based on risk tier and asset materiality.
- Preserve records during any platform dispute.

Section IV-C — Blockchain, AI, and Representation Requirements

IV.9 Blockchain and Smart Contract Requirements

- Audit all inheritance smart contracts.
- Support human override and dispute holds for all smart contract execution.
- Prohibit inactivity-triggered inheritance.
- Maintain on-chain and off-chain logs with documented linkage.
- Store no PII on-chain.

IV.10 Post-Mortem Representation Requirements

- Require express authorization for synthetic or commercial representation of the deceased.
- Clearly label all stewarded or synthetic communications.
- Document jurisdictional personality rights review before any commercial representation.
- Evaluate reputational and beneficiary liability risk before any public communication.
- Suspend representation during any material dispute.

IV.11 Cross-Border Review Requirements

- Produce a Jurisdictional Exposure Map (JEM) when cross-border triggers exist.
- Document governing law conflicts.
- Identify enforcement feasibility limitations.
- Assess data transfer compliance obligations.
- Document all unresolved jurisdictional limitations.

Section IV-D — Alignment Declaration and Integrity

IV.12 Alignment Representation

- Represent scope of alignment accurately and without overstatement.
- Avoid implying DEPI alignment overrides local law.
- Disclose limitations of alignment claims where applicable.
- Avoid representing DEP as equivalent to testamentary instruments.

IV.13 Alignment Revocation Triggers

Alignment may be revoked where: non-circumvention doctrine is violated; synthetic identity is misused without consent; authority is not validated prior to material action; risk-tiered governance is deliberately ignored; documentation is absent for L3 decisions; trade secrets are mishandled; or licensed product terms are knowingly violated.

PART V — ACCREDITATION AND CERTIFICATION FRAMEWORK

Part V establishes the governance structure under which organizations may seek DEPI Accreditation, professionals may seek DEPI Certification, alignment claims may be audited, use of DEPI marks and designations may be regulated, and misuse may be sanctioned. DEPI functions as a standards-setting body, alignment framework, voluntary accreditation authority, and certification credentialing entity. It does not replace statutory licensure.

Section V-A — Foundational Governance Principles

Principle	Statement
Independence	Accreditation decisions must be structurally independent from commercial influence.
Transparency	Criteria for accreditation and certification shall be publicly defined and version-controlled.
Due Process	Revocation or suspension shall follow documented procedural safeguards including opportunity to respond and appeal pathway.
Technology Neutrality	Accreditation shall not require adoption of any specific product or vendor.
Jurisdictional Respect	Certification does not supersede local professional licensure rules.
Defensibility	All alignment claims must be capable of surviving independent expert scrutiny.

Section V-B — Accreditation Framework (Organizations)

V.1 Accreditation Scope and Levels

DEPI Accreditation may apply to estate planning firms, trust companies, digital custodians, financial institutions, digital asset platforms, advisory organizations, and enterprise continuity programs.

Level	Requirements
Foundational Alignment	Demonstrates implementation of core governance controls under Part IV. Policy review, basic lifecycle evidence, and authority validation process.
Advanced Alignment	Demonstrates structured documentation, cross-border review capability, and L3 risk management maturity. Includes sample case review and documentation sufficiency testing.
Institutional Alignment	Demonstrates enterprise-level governance integration, audit discipline, and policy lifecycle management. Includes cross-border scenario analysis and continuous improvement evidence.

V.2 Accreditation Audit Methodology

Accreditation review shall include: policy review; sample case review (redacted where necessary); authority validation demonstration; risk-tier application demonstration; documentation sufficiency test; non-circumvention posture confirmation; and cross-border scenario analysis. Audit may be documentation-based, interview-based, or hybrid. Audit scope must be documented.

V.3 Accreditation Validity and Renewal

Accreditation shall be time-limited and require periodic renewal with confirmation of continued compliance. Renewal intervals shall be defined in DEPI governance policy. Grounds for revocation include: material deviation from Part IV requirements; misleading alignment claims; unauthorized circumvention; synthetic identity misuse; failure to apply L3 governance; and failure to maintain documentation.

Section V-C — Certification Framework (Individual Professionals)

V.4 Certification Categories

DEPI Certification may be issued under defined designations including: Certified Digital Continuity Professional (CDCP); Advanced Digital Continuity Practitioner (ADCP); and Digital Estate Governance Specialist (DEGS). Designation criteria shall be published and version-controlled.

V.5 Competency Assessment

Certification assessment shall cover Domains 1–10, include scenario-based evaluation, and test: authority validation reasoning; risk-tier classification; cross-border conflict identification; AI representation governance reasoning; and platform refusal response logic. Assessment may include written examination, case analysis, and oral defense for advanced tiers.

V.6 Continuing Competence and Ethical Code Enforcement

Certified professionals shall complete periodic continuing education; remain current on regulatory and technological developments; and reaffirm ethical code adherence. Violations may include: misrepresentation of authority; unauthorized credential circumvention; synthetic identity misuse without consent; commercial exploitation without authorization; overstating enforceability; and failure to disclose material risk. Disciplinary review shall include complaint intake, preliminary assessment, formal review, opportunity to respond, decision issuance, and appeal pathway.

Section V-D — Use of Marks, Public Registry, and Oversight

Accredited entities and certified professionals may use DEPI marks only within granted scope and must not imply regulatory endorsement, jurisdictional supremacy, or platform exclusivity. DEPI shall maintain a public registry of accredited organizations and certified professionals including current status and revocations where appropriate. DEPI shall establish an independent review committee with conflict-of-interest safeguards, documented audit procedures, a revocation and appeal framework, and a periodic standards review process.

PART VI — SMART CONTRACT AND BLOCKCHAIN INHERITANCE FRAMEWORK

This Part defines the mandatory requirements for any platform that utilizes blockchain, smart contracts, wallets, DIDs, NFTs, or tokenized assets in continuity or inheritance processes. Smart contracts may enhance continuity workflows by offering tamper-proof execution, deterministic asset transfer, verifiable event logs, multi-party access control, programmable inheritance logic, and cryptographic assurance. However, smart contracts cannot replace legal estate authority, and blockchain inheritance must integrate with legal, ethical, and identity-continuity requirements.

7.1 Smart Contract Requirements

7.1.1 Mandatory Third-Party Audit

Before deployment, all inheritance-related smart contracts must be: audited by a qualified security firm; validated for logic correctness; tested for attack vectors including re-entrancy, signature forgery, and oracle manipulation; and analyzed for upgrade safety. Audit reports must be retained by the platform, made available to DEPI upon accreditation review, and summarized for end users in plain language.

7.1.2 Deterministic Behavior

Smart contracts must behave predictably; execute only when conditions are met; not rely on ambiguous or unverifiable conditions; not allow unauthorized execution; and ensure clear input and output states. Continuity rules must be machine-verifiable.

7.1.3 Human Override and Governance Controls

Smart contracts must support human override when: disputes arise; legal authority supersedes contract logic; documents contradict contract assumptions; fraud is detected; death is incorrectly reported; oracles fail; or beneficiaries contest a transfer. Override execution must be logged and require multi-party approval from either executor plus platform, or platform plus a DEPI-recognized continuity governance body.

7.1.4 Upgradeability and Governance-Controlled Contracts

All smart contracts must be upgradeable, include proxy-based governance mechanisms, or allow migration while preserving state continuity. This protects users from outdated inheritance logic, contract vulnerabilities, evolving legal requirements, and multi-jurisdictional

compliance updates. Immutable smart contracts cannot be used for inheritance unless they include a DEPI-approved override framework.

7.2 Blockchain Identity Requirements

Smart contract inheritance depends on identity correctness. Platforms must: map smart contract roles to verified off-chain identity; support DIDs or verifiable credentials where appropriate; verify executor or beneficiary roles before granting on-chain authority; and provide cryptographic attestations during inheritance execution. Identity verification must precede all contract execution.

7.3 Trigger Systems for Smart Contract Inheritance

Smart contracts may only execute continuity rules upon legitimate, verified triggers. Triggers fall into four categories.

7.3.1 Time-Based Triggers

Time-based triggers must include: user-defined release dates; time-locked delivery; milestone-based releases; and future message or memory releases. Protection requirements include: user ability to modify or revoke time triggers at any point before activation; delayed execution with defined objection windows; and multi-party override capability in emergencies.

7.3.2 Event-Based Triggers

Event triggers include: medical incapacity; business continuity events; trustee activation; SMB key-person loss; and regulatory events. Event verification must be logged, reversible, and include multi-factor identity validation.

7.3.3 Oracle Triggers

Oracles used in blockchain inheritance systems must be: tamper-resistant; provide proof-of-origin; support redundancy; require multi-attestation for death verification; and prevent trigger spoofing. Oracles must not rely solely on inactivity, user silence, single-source data, or unverifiable online claims. Oracles must support dispute resolution and override.

7.3.4 Multi-Party Approval Triggers

Inheritance must support multi-party approvals combining any of: executor plus platform; executor plus beneficiary; platform plus trusted contact; or legal authority plus platform. This reduces risk of unilateral malicious action.

7.4 Continuity Logic and Role Assignment

Contract roles must be explicitly defined: Contract Owner (the user); Executor or Trustee; Beneficiaries; Delegates; and Guardian roles where applicable. Authority mapping determines who can modify contracts, who can approve execution, who can revoke access, and who can trigger override. Mapping must reflect legal documents including will, trust, and power of attorney.

7.5 Key Management Requirements

Platforms must support continuity-friendly key systems including: multi-signature wallets; MPC-based key splitting; shard-based recovery; hierarchical key structures; and backup keys stored securely by executor or platform. Executors must never require access to the user's private keys, need the user's device, or bypass continuity rules to obtain keys. Key inheritance must occur via delegated authority, not secret sharing.

7.6 Smart Contract Execution Requirements

Before contract execution, platforms must verify: authenticity of the trigger event; legal authority of the requesting party; identity of executor or beneficiary; absence of active disputes; and override eligibility in case of conflicts. Post-execution requirements: state changes must be logged; beneficiaries must receive cryptographic proof of execution; and residual contract functions must be disabled when appropriate.

7.7 Auditability and Transparency

7.7.1 On-Chain Event Logs

On-chain logs must record: event triggers; inheritance actions; approvals; denials; overrides; transaction hashes; and timestamps. Logs must be human-readable, exportable, and legally admissible.

7.7.2 Off-Chain Continuity Logs

Off-chain logs are required for: identity verification; document validation; disputes; recovery events; manual override; and cross-border inheritance events. Off-chain logs must link to on-chain events via hash references to maintain a complete and verifiable audit chain.

7.8 NFT-Based Emotional and Memory Asset Requirements

Where NFTs represent personal memories, emotional content, or family legacy, the following requirements apply: metadata permanence; encrypted storage of sensitive content; no public-chain exposure of private assets; staged release (time-based or milestone-based); explicit ethical configuration; and redaction support where legally required. Platforms must prevent unauthorized post-mortem access and AI manipulation of emotional NFTs without user consent.

7.9 Legal, Regulatory, and Ethical Alignment

Smart-contract inheritance does not override wills, trusts, probate orders, estate laws, GDPR, privacy rights, or AI ethics frameworks. Smart contracts must be subordinate to legal authority at all times. Platforms must ensure: smart contract logic aligns with the user's legal estate plan; executors can override code under legal mandate; cross-border inheritance rules are respected; and AI and identity continuity remains ethical and transparent.

7.10 Prohibited Smart Contract Practices

Platforms may not use smart contracts that: automatically transfer assets upon inactivity; expose private keys; lack override mechanisms; require irreversible execution without human confirmation; misalign with legal authority; use unverifiable oracles; store personal data on-chain; bypass executor verification; or allow unrestricted beneficiary access. Non-compliance with any of these prohibitions results in non-accreditation under DEPI.

PART VII — RISK MANAGEMENT AND SECURITY CONTROLS

Digital continuity requires a robust, multi-layered security and risk-management framework. Security controls must not impair continuity, and continuity controls must not weaken security. The governing principle is secure continuity — neither security at the expense of inheritance, nor continuity at the expense of protection.

8.1 Risk Assessment Framework

All platforms must implement a formal, documented risk-assessment methodology that includes: identification of all asset categories; risk scoring per asset; continuity impact assessment; threat modeling; inheritance scenario analysis; identity failure mode analysis; blockchain-specific risk where applicable; and AI-legacy risk assessment. Risk assessments must be updated annually, or sooner when major features change, legal frameworks evolve, new cryptographic risks emerge, or new AI behavior patterns are introduced.

8.1.1 Threat Categories

Technical Threats include: account takeover; credential theft; session hijacking; device compromise; API misuse; smart contract exploit; and cryptographic key exposure.

Human Threats include: malicious heirs; insider abuse; executor impersonation; trustee misrepresentation; social engineering attacks; and phishing attacks.

Operational Threats include: service outages; data corruption; cloud provider failure; blockchain network downtime; and continuity misconfiguration.

Legal Threats include: disputed wills or trusts; jurisdictional incompatibility; conflicting beneficiaries; misaligned inheritance triggers; and probate freezes on digital assets.

AI-Related Threats include: AI impersonation of the deceased; hallucinated or altered AI memories; synthetic identity risk; and misuse of AI persona post-mortem.

8.1.2 Blockchain-Specific Threat Modeling

Platforms using blockchain must additionally assess: smart contract vulnerabilities; oracle manipulation; chain reorganization and rollback; seed phrase loss; signature forgery; key mismanagement; cold-storage continuity failure; custodial versus non-custodial risk; and NFT metadata loss. High-risk blockchain inheritance workflows cannot be accredited unless they include MPC, multi-sig, and structured recovery pathways.

8.1.3 Immersive Asset Risk Factors

Platforms handling AR/VR/XR assets must assess risks related to: deepfake spatial impersonation; unauthorized holographic simulation; psychological impact on beneficiaries; sensitive spatial detail leakage; and volumetric capture privacy violations.

8.2 Security Controls

8.2.1 Encryption Requirements

All continuity-relevant data must be encrypted in transit using TLS 1.2 or stronger; at rest using AES-256 or stronger; within backups; and in transit between internal services. Encryption keys must never be stored in plaintext, be accessible to unauthorized roles, or be used as inheritance triggers themselves.

8.2.2 Access Control Requirements

Access must be enforced using MFA, role-based access control (RBAC), least-privilege principles, robust permission auditing, and account isolation. These controls apply to users, delegates, executors, trustees, administrators, and platform developers without exception.

8.2.3 Zero-Knowledge Access Principles

If a platform claims zero-knowledge architecture: the platform must never have the ability to decrypt user content; continuity pathways must not require private keys to be shared; and inheritance must occur through authority mapping, not secret disclosure. Platforms must document all zero-knowledge exceptions for accreditation review.

8.2.4 On-Chain Encryption and Privacy

Blockchain-based systems must: never store personal data on public chains; use hash anchoring instead of plaintext storage; encrypt sensitive content off-chain; use zero-knowledge proofs where appropriate; and ensure compliance with GDPR, CCPA, and eIDAS requirements. Blockchain immutability must not conflict with deletion rights.

8.2.5 Spatial Privacy Controls

Platforms handling immersive assets must: redact sensitive background elements in spatial captures; encrypt volumetric frames; and prevent unauthorized 3D reconstruction of private spaces or individuals.

8.3 Identity and Key Management Controls

8.3.1 Identity Integrity Requirements

Platforms must: verify user identity at onboarding; verify executor identity during inheritance; validate delegates through MFA or verifiable credential authentication; and maintain identity continuity across device and account transfers.

8.3.2 Key Storage Requirements

Keys controlling continuity must be encrypted; use hardware-backed secure storage where possible; never be exposed to unauthorized parties; and use key rotation when risk is detected.

8.3.3 Continuity-Focused Key Recovery

Key recovery is mandatory for blockchain assets, cryptographic identity systems, encrypted emotional assets, and AI memory archives. Acceptable recovery methods include multi-sig, MPC, shard recovery, identity-verified recovery, and executor-assisted recovery. No platform may rely solely on a single seed phrase.

8.4 Monitoring and Anomaly Detection

8.4.1 Session Monitoring

Platforms must monitor and alert on: unusual access patterns; unusual geographic access; and multiple failed login attempts.

8.4.2 Dynamic Risk Scoring

Platforms must dynamically score: delegate actions; executor actions; post-mortem access requests; and account anomalies. Risk scores must inform access decisions and trigger escalation where thresholds are exceeded.

8.4.3 Behavioral Detection for AI-Enabled Systems

For AI-enabled systems, platforms must: detect unauthorized AI actions; detect attempts to impersonate deceased individuals; and detect changes in AI model behavior that deviate from configured parameters.

8.5 Incident Response Requirements

Platforms must maintain an incident response plan covering: account compromise; key compromise; fraudulent executor activation; inheritance disputes; smart contract exploits; blockchain network downtime; AI model corruption; and major outages. Incident response

must include containment, user notification, audit-level documentation, legal escalation where needed, and continuity restoration. Continuity must not be permanently interrupted by any incident.

8.6 Vendor and Third-Party Risk Management

Digital continuity depends on cloud providers, identity verification services, blockchain networks, API providers, AI model hosting services, and storage systems. Platforms must: assess vendor risk; maintain SLAs; evaluate vendor continuity plans; enforce encryption requirements in vendor contracts; monitor provider performance; and maintain secondary providers for redundancy. Vendor failures must not compromise estate continuity.

8.7 Post-Mortem Access Security Controls

8.7.1 Death Verification Protection

Systems must: require multi-factor verification of death events; validate all submitted documents; evaluate risk indicators for fraudulent claims; and specifically check for early or premature death reporting.

8.7.2 Executor and Trustee Access Controls

Must include: identity proofing; legal authority verification; granular access scopes mapped to asset categories; and complete audit logs of all executor actions.

8.7.3 AI Post-Mortem Safeguards

Platforms must ensure AI does not impersonate the deceased; does not create new content post-mortem unless explicitly authorized; and does not generate harmful or misleading output. AI memory models must be frozen upon verified death unless the user has explicitly configured continued operation.

8.7.4 Smart Contract Post-Mortem Safeguards

Smart contracts must: require human approval before execution; allow legal override; disable auto-trigger inheritance based solely on time or inactivity; and log all execution steps with full attribution.

8.7.5 Multi-Party Approval for High-Risk Actions

High-risk post-mortem actions must require either: executor plus platform approval; executor plus beneficiary approval; or executor plus DEPI-accredited governance module approval. No high-risk post-mortem action may be executed by a single party.

8.8 Security Logging and Audit Requirements

All continuity-relevant actions must be logged. Identity events include: authentication; recovery; delegations; and revocations. Inheritance events include: trigger verification; authority mapping; asset release; and key transitions. Cryptographic events include: blockchain event logs; smart contract execution records; oracle results; and multi-sig approvals. AI events include: model access; model updates; and memory archive access. All logs must be append-only, exportable, tamper-resistant, and stored for a minimum of seven years.

8.9 Asset-Specific Security Requirements

8.9.1 Emotional Digital Assets

Emotional assets require: encryption at rest and in transit; no default visibility for beneficiaries; staged, timed, or conditional release only; protection of sensitive content from unauthorized parties; prevention of content leakage via metadata; and explicit configuration for any AI-based emotional content. Emotional assets are treated as high-sensitivity by default.

8.9.2 AI-Generated Cognitive Assets

AI identity assets require: prevention of unauthorized use of AI persona; mandatory model freezing post-mortem unless release is explicitly configured; prevention of harmful AI behavior including impersonation and fabrication; inheritance of outputs only, not model rights, unless separately authorized; protection of training data from unauthorized access or export; and allowance of deletion under legal authority.

8.9.3 High-Risk Asset Security

High-risk assets including crypto-only wallets and unrecoverable password vaults must: use multi-party controls; reject single-seed-phrase systems for accreditation purposes; include enhanced KYC verification; include restricted access policies; include mandatory warnings to users; and require continuity configuration review before accreditation is granted. Platforms failing to meet these controls cannot be DEPI-accredited.

PART VIII — PLATFORM ACCREDITATION REQUIREMENTS

This Part defines the criteria and controls required for DEPI Accreditation — a formal process evaluating whether a digital continuity platform adheres to standards governing security, identity continuity, inheritance workflows, data integrity, consumer protection, AI-legacy management, blockchain components, emotional asset handling, and regulatory alignment. Accreditation is voluntary but strongly recommended for digital vaults, inheritance platforms, blockchain-based continuity solutions, AI-persona and memory systems, SMB continuity tools, and custodial and non-custodial digital asset systems.

9.1 Accreditation Structure — Eight Core Domains

DEPI evaluates platforms across eight core domains. Platforms must meet minimum compliance in all applicable domains and enhanced compliance in domains relevant to their architecture.

Domain	Scope
Domain 1	Security and Encryption Controls
Domain 2	Identity Continuity and Delegation Systems
Domain 3	Continuity Workflows
Domain 4	Inheritance Execution Controls
Domain 5	Data Management, Integrity, and Retention
Domain 6	AI, Emotional, and Cognitive Asset Governance
Domain 7	Blockchain and Cryptographic Controls (if applicable)
Domain 8	User Protection, Transparency, and Ethics

9.2 Domain 1 — Security and Encryption Controls

9.2.1 Encryption Standards

Platforms must implement: AES-256 or stronger at rest; TLS 1.2 or higher in transit; encrypted backups; and hardware-backed key storage where available.

9.2.2 Access Security

Required: MFA across all privileged access; session monitoring; role-based access controls; and least-privilege enforcement.

9.2.3 Secrets Management

Required: encrypted secret storage; no plaintext credential storage; and rotation policies for any compromised secrets.

9.2.4 System Integrity

Required: mandatory code review for security-critical paths; continuous vulnerability scanning; and annual penetration testing. Platforms must prove these controls through documentation and audit evidence.

9.3 Domain 2 — Identity Continuity and Delegation Systems

9.3.1 Identity Verification

Platforms must demonstrate: KYC and KYB processes; multi-factor authentication; identity recovery mechanisms; and executor identity verification workflows.

9.3.2 Delegation Controls

Required support for: pre-death delegation; incapacity delegation; post-mortem executor and trustee assignment; and granular permission scopes per asset category.

9.3.3 Identity Mapping

Mapping of user, delegates, executors, and business continuity officers must be stored in continuity metadata and be accessible for audit.

9.3.4 Device Independence

Identity access must not be tied to a single device, a single phone number, or a single authentication token.

9.4 Domain 3 — Continuity Workflows

Platforms must support all applicable workflows: primary continuity workflow with full asset configuration capability; emergency workflow that is time-limited, monitored, and logged; incapacity workflow supporting legal incapacity proof, restricted caregiver access, and continuity without impersonation; post-mortem workflow with death verification, executor

authentication, identity transition, rules-based asset release, and full logging; and SMB workflow with key-person delegation and operational continuity.

9.5 Domain 4 — Inheritance Execution Controls

Platforms must: validate legal authority through will, trust, letters testamentary, and court orders; enforce asset-specific inheritance rules with different procedures for financial, emotional, AI, and business assets; limit unauthorized access ensuring executors cannot see unauthorized emotional assets and beneficiaries cannot access restricted categories; and provide exportable evidence including inheritance reports, chain-of-custody logs, identity verification logs, and cryptographic proofs for blockchain assets.

9.6 Domain 5 — Data Management, Integrity, and Retention

Platforms must: maintain data integrity through versioning, integrity checks, and tamper-evident logs; manage metadata properly with fields for asset category, continuity rules, visibility rules, retention schedule, encryption status, and storage location; support user-level data control including export, rule updates, delegate revocation, and content deletion subject to legal limitations; and maintain retention and archival with emotional assets preserved as configured, AI models frozen or archived, and logs retained for a minimum of seven years.

9.7 Domain 6 — AI, Emotional, and Cognitive Asset Governance

If a platform handles emotional or AI-generated assets, it must demonstrate: ethical handling of emotional assets with encryption, staged releases, inheritance-level control, privacy preservation, and metadata preservation; AI continuity controls including post-mortem model freezing, prohibition on impersonation, training data integrity, revocation capability, and prohibition on generating post-mortem content without consent; synthetic identity and deepfake protection through detection tools, warning systems, identity verification checks, and anti-abuse controls; and immersive asset governance for AR/VR/XR assets with encrypted spatial storage, ethical staging, minor protection, AI augmentation labeling, and cross-device continuity.

9.8 Domain 7 — Blockchain and Cryptographic Controls

If a platform uses blockchain, smart contracts, NFTs, wallets, or cryptographic identity, it must demonstrate: key management including mandatory multi-sig or MPC, key recovery mechanisms, and prohibition on single-seed-phrase dependency; smart contract controls with audited, upgradeable, override-capable, deterministic, and transparent contracts; oracle

integrity with tamper-proof, multi-attestation oracles supporting dispute resolution; NFT metadata integrity with no sensitive data stored publicly, preservation support, and lawful deletion capability; auditability through blockchain event logs, continuity chain-of-custody, and hash proofs of off-chain data; and for tokenized immersive assets, off-chain encrypted storage with no volumetric data on-chain.

9.9 Domain 8 — User Protection, Transparency, and Ethics

Platforms must provide full transparency so users understand what data is stored, where it is stored, who can access it, what the continuity rules are, what the inheritance triggers are, and what risks are specific to blockchain or AI usage. Risk disclosures must cover: risk of asset loss; risk of key loss; smart contract risk; AI impersonation risk; and continuity limitations. User controls must enable: continuity configuration; rule modification; delegate revocation; asset export or deletion; and AI model freezing. Ethical standards must be met: honoring privacy; not manipulating emotional assets; protecting minors; and ensuring AI-generated content is labeled.

9.10 Accreditation Tiers

Tier	Description
Tier 1 — DEPI Accredited Digital Continuity System™	Full compliance across all applicable domains. No material gaps. Annual renewal required.
Tier 2 — DEPI Accredited (Conditional)	Conditional approval where minor gaps exist, a documented remediation roadmap exists, and no continuity-critical risks are present. Remediation deadline required.
Tier 3 — DEPI Not Accredited	Reasons include: single-seed-phrase design; missing inheritance workflows; inadequate identity verification; sensitive data stored on public blockchains; no AI safeguards; or no emergency or incapacity workflow.

9.11 Accreditation Process

Phase 1 — Application Submission. Platform submits: technical architecture documentation; policy documentation; security practices; continuity workflow diagrams; and smart contract code where applicable. Phase 2 — Review and Testing. DEPI reviews documentation,

security controls, identity workflows, blockchain components, AI assets, and user experience for inheritance flows. Phase 3 — Interview. Platform leadership must attend a DEPI review interview. Phase 4 — Remediation Window. If issues are discovered, DEPI may grant a corrections period with a defined deadline. Phase 5 — Final Determination. Platform receives Accredited, Accredited (Conditional), or Not Accredited status.

9.12 Renewal and Ongoing Compliance

Platforms must: undergo annual compliance reviews; submit updated documentation for all major releases; disclose security incidents to DEPI within defined timeframes; and maintain all user protection commitments. Failure to maintain compliance revokes accreditation.

PART IX — REGULATORY AND COMPLIANCE ALIGNMENT

Digital estate continuity operates at the intersection of traditional estate law, digital identity regulations, privacy and data protection law, cybersecurity frameworks, blockchain and cryptographic regulation, AI governance, and cross-border inheritance rules. DEPI is technology-neutral and jurisdiction-neutral. Compliance requires adherence to this Standard in harmony with governing legal authority in all applicable jurisdictions.

11.1 Legal Hierarchy and Precedence Rules

Continuity systems must follow this hierarchy in descending order of authority: governing law of the estate — wills, trusts, and court orders supersede platform-level continuity settings; jurisdictional probate authority governing inheritance rights, documentation requirements, executor authority, and digital asset access rules; statutory digital asset frameworks including RUFADAA (USA), GDPR (EU), eIDAS 2.0 (EU identity), HIPAA (USA medical data), and local data protection and succession laws; platform contracts which must comply with DEPI and legal frameworks; user continuity instructions which are binding unless overridden by law; and technical rules and smart contract logic which must always defer to legal authority.

11.2 United States Regulatory Alignment

11.2.1 RUFADAA

The Revised Uniform Fiduciary Access to Digital Assets Act governs fiduciary access in states where enacted. Platforms must: distinguish between content and catalogue information; allow fiduciary access consistent with user directives; require proper legal documentation; avoid giving executors higher privileges than legally authorized; and support revocation of legacy credentials.

11.2.2 Federal Privacy Laws

Platforms must: restrict health-related data access per HIPAA; protect minor children from privacy breaches per COPPA; and comply with financial data handling restrictions under GLBA.

11.2.3 ESIGN and UETA

Platforms supporting electronic signatures must: ensure records remain accessible; maintain permanent audit trails; and support long-term verification of electronically signed continuity documents.

11.2.4 Federal and State Blockchain Regulations

Platforms must: disclose where blockchain networks operate; comply with KYC/AML requirements for financial assets; support subpoena compliance; and ensure tokenized rights reflect actual legal ownership.

11.3 European Union Regulatory Alignment

11.3.1 GDPR

Key requirements include: data minimization; data subject rights; lawful basis for processing; right to rectification; right to erasure with post-mortem requests delegated to executors; and breach reporting within 72 hours. Platforms must support executor-driven GDPR requests post-mortem.

11.3.2 eIDAS 2.0

Platforms must: support digital identity wallets; integrate verifiable credentials; and align decentralized identity systems with EU identity trust frameworks.

11.3.3 EU Digital Markets Act and Digital Services Act

Platforms must: provide transparency in algorithmic systems; support exportability of user data; protect users from digital manipulation; and enforce content governance for AI assets.

11.4 Asia-Pacific Regulatory Alignment

Platforms operating in the Asia-Pacific region must align with: Singapore PDPA; Australia Privacy Act; New Zealand Privacy Framework; Japan digital asset regulations; South Korea PIPA; and India's DPDP Act. Key requirements include localized data transfers, explicit consent models, restrictions on biometric and genetic data, and digital executor compliance.

11.5 LATAM Regulatory Alignment

Platforms operating in Latin America must support: civil law-based inheritance structures; mandatory executor authority validation; LGPD compliance for data processing in Brazil; and localization of data processing where required. Blockchain usage must consider local tax implications and restrictions on tokenized securities.

11.6 Cross-Border Digital Estate Conflicts

Cross-border estates raise conflicts in identity, jurisdiction, asset classification, inheritance rights, executor recognition, recognition of smart contract triggers, and AI persona treatment. Platforms must implement jurisdiction mapping covering storage location, citizen and resident status, corporate domicile, blockchain node locations, and legal system of origin. Multi-jurisdictional executor support must provide verification under jurisdiction of death, jurisdiction of asset location, and jurisdiction of platform operation. Platforms must prevent unlawful data export, restrict access based on jurisdiction, support legal disputes, and escrow continuity events when not legally permissible.

11.7 Compliance Requirements for Blockchain Systems

No personal data may be stored on public chains without encryption or zero-knowledge proofs. Smart contracts must be override-capable. Platforms must disclose where nodes operate, jurisdictional risk, immutability implications, and applicable regulatory regimes. Tokenized legal rights must reflect actual legal title.

11.8 Compliance Requirements for AI Systems

Platforms using AI must comply with emerging global AI regulations including the EU AI Act, OECD AI Principles, US AI safety guidance, and national AI risk frameworks. Requirements include: risk assessment of AI identity models; labeling of AI-generated content; preventing AI impersonation post-mortem; protecting minors from harmful emotional content; enabling deletion or revocation; and ensuring AI does not override legal estate instructions.

11.9 Required Documentation for Compliance

Platforms must maintain: compliance statements covering data protection, identity workflows, blockchain disclosure, AI governance, and continuity workflow documentation; audit logs for identity events, delegation events, inheritance events, AI model changes, and smart contract execution; and annual regulatory risk assessments. Platforms must be capable of producing regulator-ready outputs on continuity workflows, death verification processes, inheritance execution, blockchain event logs, AI behavior logs, identity verification events, and cross-border inheritance documentation.

PART X — ETHICS, DIGNITY, AND POST-MORTEM GOVERNANCE

This Part establishes the ethical, fiduciary, and governance principles governing human digital identity across incapacity, death, and post-mortem administration. It addresses the moral, legal, and governance framework that sits beneath all technical and operational governance in this Standard. Ethics is not an addendum to digital estate continuity — it is its governing conscience.

This Part applies to: fiduciaries and estate representatives; trustees and executors; digital custodians; platform providers; AI model operators; accreditation bodies; courts and regulators; and all certification holders under DEPI designations. Under voluntary DEPI alignment, adherence to this Part is required for accreditation and certification; it does not create independent legal obligations or supersede governing law.

10.1 Core Ethical Principles

All DEPI-aligned platforms and professionals must adhere to nine foundational principles.

Principle	Requirement
Autonomy	The individual must retain control over their digital identity, continuity instructions, emotional digital assets, and AI personas derived from their data. No system may override the user's explicit continuity settings except by court order.
Informed Consent	Users must understand what continuity means, who will gain access, what assets will transfer, how AI may behave post-mortem, how blockchain immutability affects inheritance, and how metadata may be preserved indefinitely. Platforms must provide clarity, not obscurity.
Dignity of the Deceased	Digital systems must never exploit the deceased, impersonate them for commercial gain, alter AI personas in misleading ways, or expose private emotional content without authorization. Legacy dignity is paramount.
Privacy and Confidentiality	Even after death, privacy rights must be respected. Platforms must restrict access to sensitive content, separate emotional content from general access, encrypt

Principle	Requirement
	all emotionally sensitive data, and ensure AI memories cannot be misused. Privacy persists beyond death.
Beneficiary Protection	Beneficiaries must be protected from inappropriate emotional content, digital manipulation, unmanaged AI content, dangerous financial assets, and incomplete or inaccurate continuity data. The goal is protection, not burden.
Fairness and Non-Discrimination	Systems must not privilege one heir incorrectly, discriminate by geography, gender, age, or identity, or restrict inheritance arbitrarily. Continuity pathways must reflect the user's wishes and legal authority.
Transparency	Platforms must disclose continuity processes, AI content behaviors, blockchain usage, smart contract logic in plain language, identity handling, and key recovery mechanisms. No black-box inheritance.
Accountability	Executors, trustees, continuity delegates, and platforms are accountable for lawful handling of assets, ethical preservation, correct distribution, maintaining audit trails, and respecting user intent. Accountability must be enforceable.
Non-Exploitation	No stakeholder may use inheritance systems for personal gain, manipulate beneficiaries, harvest data of the deceased, use AI versions of the deceased for business purposes without authorization, or promote unethical emotional interactions.

10.2 Authority and Legitimacy

Ethical governance requires lawful authority. However, lawful authority may not be ethically sufficient. This Part distinguishes: Statutory Authority — granted under probate or fiduciary law; Contractual Authority — granted via platform designation tools; Instrument-Based Authority — granted in wills, trusts, or powers of attorney; and Technological Authority — derived from possession of private keys or credentials.

Ethical legitimacy requires alignment among these authorities where possible. Possession of credentials alone does not create ethical entitlement. Conversely, lawful appointment does not automatically justify unrestricted digital intrusion. Practitioners shall evaluate scope of authority, express restrictions, nature of asset, sensitivity level, and intent indicators before acting.

10.3 Post-Mortem Privacy

Post-mortem privacy is jurisdictionally inconsistent but ethically significant. Even where legal privacy rights terminate upon death, ethical duties may persist. Governance frameworks shall consider: sensitive communications; confidential professional exchanges; medical or biometric data; private correspondence; and unpublished creative works.

Fiduciaries shall apply a principle of minimum necessary exposure. Where disclosure is required, the fiduciary must document justification, limit scope, and preserve an audit trail.

10.4 AI and Synthetic Continuation

10.4.1 Model Freezing

Upon verified death, AI models must be frozen unless explicitly authorized for continued operation. Freezing prevents uncontrolled evolution, inaccurate personality drift, unintended impersonation, and exploitation of the deceased's identity.

10.4.2 Controlled Post-Mortem AI Behavior

If the user authorizes AI activity after death: models must be clearly labeled as AI; beneficiaries must receive disclaimers; emotional safeguards must exist; commercial usage is not allowed unless explicitly permitted; and output must not misrepresent legal intent. Platforms must ensure AI never makes financial decisions, influences legal processes, imitates the deceased deceptively, or manipulates vulnerable beneficiaries.

10.4.3 Ethical AI Output Controls

AI assets must: filter harmful content; avoid rewriting personal history; provide accurate and unaltered memory summaries; and prevent hallucinated advice from being treated as real estate instructions. AI cannot override legal estate documents under any circumstances.

10.4.4 Data Minimization

Only essential training data should be used for AI memory models. Highly sensitive data must be excluded, encrypted, or subject to deletion under user or executor authority.

10.5 Platform Governance and Digital Remains

Digital remains may exist within platforms that retain contractual control, limit account transferability, prohibit credential sharing, or offer memorialization tools. Governance must reconcile platform terms, estate law, and ethical expectations. Practitioners shall evaluate whether the account is transferable, whether data is exportable, whether memorialization preserves or limits rights, and whether deletion conflicts with beneficiary interest. Digital remains should not be treated solely as data inventory; they may embody public persona, community archives, revenue streams, and intellectual property.

10.6 Emotional Digital Asset Ethics

Emotional assets require heightened ethical care. Platforms must: restrict emotional assets from executors unless explicitly authorized; release emotional content only to intended recipients; enforce staging, timing, or milestone gates; and encrypt all emotional content.

For children and minors, content may be delayed until a specified age, may be staged over years, and guardians may not override these settings. The user's emotional intent is binding.

Platforms must ensure emotional content does not cause psychological harm, deliberately manipulate heirs, include abusive or damaging content without safeguards, or violate the privacy of third parties. Immersive and holographic emotional assets must not mislead heirs, must clearly label AI involvement, must reflect authentic legacy content, and must avoid manipulation or distortion of the deceased's recorded presence.

10.7 Consent, Rights, and Revocation

Consent must be explicit, documented, revocable, and asset-specific. Platforms cannot rely on blanket consent. Revocation rights must cover: delegates; executor consent before death; emotional asset access; AI post-mortem activity; and blockchain execution triggers. Revocation must propagate across all continuity systems.

Heirs have rights to: see clear continuity logs; receive assets legally designated to them; challenge unethical or inaccurate AI-inheritance content; and request correction of inherited digital misinformation. Heirs do not have default rights to emotional or private content not designated to them.

Executors must: honor privacy; act without exploitation; protect emotional data; disclose actions to beneficiaries when appropriate; follow legal authority; and preserve audit logs. Executors cannot use continuity systems for personal gain.

10.8 Ethical Use of Blockchain in Inheritance

Blockchain-based inheritance must preserve consent, legal compliance, privacy, reversibility, dignity, and transparency. Platforms must avoid irreversible errors, unverified triggers, auto-transfer without human confirmation, storing sensitive content on-chain, and exploiting beneficiaries with complex or unsafe blockchain mechanics. DEPI requires a human-in-the-loop for all inheritance-critical blockchain actions. Smart contracts must be subordinate to legal authority; immutability does not create ethical permission.

10.9 Conflicts Among Beneficiaries

Digital assets frequently create unique conflicts including competing claims to social media control, disputes over deletion versus preservation, conflicts regarding AI continuation, reputation management disagreements, and access to private communications. Governance shall prioritize expressed decedent intent, instrument hierarchy, statutory law, and court supervision where necessary. Absent clear instruction, fiduciaries should default to preservation pending resolution.

10.10 Digital Identity Persistence and Termination Protocols

Digital identity does not terminate automatically upon biological death. Governance must distinguish between biological death, legal death, platform-recognized death, and operational termination of digital presence. A structured termination or persistence protocol shall consider whether the decedent expressed preferences for deletion, memorialization, archival preservation, transfer of management, or AI continuation; whether ongoing digital presence creates security exposure, identity fraud risk, or emotional harm; and whether automatic deletion would destroy economic value or prevent lawful distribution.

Absent instruction, governance frameworks shall avoid irreversible deletion until lawful authority is confirmed and stakeholder review is completed.

10.11 Digital Reputation Stewardship

Digital estates frequently include public-facing profiles, publications, and reputational records. Post-mortem governance shall address who may speak on behalf of the decedent, whether new content may be published under the decedent's name, whether existing public posts may be edited, and whether controversial content should be removed. Modification of historical content should be avoided unless necessary to prevent harm or legal violation.

Historical integrity should be preserved except where defamation exposure exists, sensitive data was improperly published, or statutory compliance requires removal.

10.12 Emotional and Psychological Harm Mitigation

Digital estates can produce unanticipated psychological effects including repeated resurfacing of algorithmic memories, automated birthday reminders, AI chat simulations, and public tagging in social platforms. Governance shall account for survivors' emotional well-being and the risk of digital retraumatization. Where AI or automated memory features exist, fiduciaries shall evaluate whether continuation aligns with expressed intent, whether beneficiaries consent to persistence, and whether labeling clearly distinguishes simulation from the historical person. Platforms are encouraged to incorporate opt-in, not opt-out, synthetic continuation defaults.

10.13 Commercialization of Digital Legacy

Commercialization of personality-based digital identity raises distinct ethical questions: whether the decedent intended commercial continuity; whether commercialization alters posthumous identity; and whether monetization conflicts with moral rights where applicable. Governance doctrine requires express authorization for post-mortem commercialization when possible; clear delineation between asset liquidation and identity exploitation; and documentation of fiduciary reasoning. Absent instruction, commercial exploitation of personality-based digital identity should be approached conservatively.

10.14 Minor and Dependent Considerations

Where a minor is the decedent, digital records may include images, social media archives, educational data, and biometric information. Governance shall prioritize privacy preservation, prevention of posthumous exploitation, and restricted public disclosure.

Where a minor is a beneficiary, access should be developmentally appropriate, custodial oversight should be defined, and risk-tiered distribution applies. Governance shall consider staged access models consistent with fiduciary best practices.

10.15 Cultural and Religious Considerations

Digital remains intersect with diverse cultural and religious doctrines regarding memory preservation, image retention, voice replication, burial rites, and posthumous representation. Practitioners shall inquire into religious directives, cultural expectations, and familial norms.

Governance shall avoid imposing technologically driven defaults that conflict with cultural identity. DEPI will maintain a Cultural Governance Appendix for regional adaptation.

10.16 Biometric and Genetic Data Governance

Digital estates may include facial recognition datasets, voiceprints, DNA data, health platform records, and wearable device archives. Such data implicates not only the decedent but living relatives. Deletion, retention, or disclosure decisions involving biometric or genetic data require heightened scrutiny. Certified practitioners shall treat biometric data as high-sensitivity assets irrespective of monetary value.

10.17 Decentralized Systems and Immutable Records

Distributed ledger systems present unique post-mortem challenges: irreversibility of transactions, immutability of records, public visibility of wallet addresses, and absence of centralized authority. Ethical governance must address whether irreversible transfers align with expressed intent, whether pseudonymity compromises estate transparency, and whether public ledger permanence conflicts with privacy norms. Where blockchain records are immutable, governance shall focus on control of associated keys, layered identity protections, and minimization of unnecessary public linkage. Immutability does not eliminate ethical responsibility.

10.18 Delegated Authority and Overreach Risk

Digital executors and continuity representatives may possess technical capabilities exceeding the decedent's express delegation. Governance safeguards shall include role-based access controls, explicit scope documentation, independent audit logging, and separation of powers where feasible. Technical ability does not equate to ethical permission. Practitioners shall counsel clients against granting blanket credential access without layered authorization protocols.

10.19 Memorialization Versus Active Continuation

Memorialization — static profile preservation, archive mode, tribute pages, and locked content view — is presumed acceptable absent contrary instruction. Active continuation — posting new content, engaging in communication, commercial brand activity, or AI-generated interaction — requires affirmative consent. These two modes must be distinguished clearly in planning instruments. Deceptive continuation — presenting new content as authored by the deceased — is categorically prohibited under DEPI alignment.

10.20 Fiduciary Liability Exposure

Digital estates create novel fiduciary exposure categories including unauthorized access claims, privacy breach liability, data security failures, cross-border compliance violations, intellectual property mismanagement, and AI misrepresentation disputes. Governance shall integrate risk mitigation measures: written digital asset inventory, consent documentation, platform compliance review, jurisdictional conflict analysis, and professional liability insurance review. Certification holders shall disclose liability boundaries in engagement letters.

10.21 Temporal Governance

Digital estates evolve over time. Governance frameworks must address long-term account inactivity, platform insolvency or shutdown, technological obsolescence, encryption decay or key loss, and successor fiduciary transitions. Continuity planning shall include periodic review cycles, succession for digital representatives, data migration strategies, and key escrow protocols where legally permissible. Ethical governance extends beyond immediate probate administration.

10.22 Algorithmic Influence After Death

Algorithms may continue to recommend the decedent's content, generate derivative outputs, and incorporate historical data into model training. Governance must consider whether the decedent consented to ongoing algorithmic use, whether data removal rights apply post-mortem, and whether AI training datasets should exclude deceased individuals absent consent. This area remains evolving across jurisdictions; practitioners shall disclose uncertainty where law is unsettled.

10.23 Moral Rights and Intellectual Integrity

In jurisdictions recognizing moral rights of integrity, attribution, and protection against distortion, digital estates may include literary works, software code, artistic creations, audio-visual materials, and NFTs tied to creative output. The distinction between economic rights and moral rights shall be maintained. Economic transfer does not extinguish moral protection where law preserves it. Where moral rights are perpetual or inalienable, fiduciaries must avoid actions that compromise artistic integrity.

10.24 Post-Mortem Data Protection and Regulatory Interface

Data protection law provides limited or no direct rights to deceased individuals in most jurisdictions. However, secondary rights may persist through executor authority, heir-based rights of access, reputation and personality protections, contractual data portability rights, and consumer protection doctrines. Post-mortem governance shall include a structured regulatory interface analysis. Certified practitioners shall not assume data protection law ceases relevance at death; rather, they shall analyze its indirect and derivative applications.

10.25 Institutional and Platform Responsibilities

Platforms and custodians bear ethical responsibilities including: clear legacy tools; transparent memorialization policies; accessible authority designation processes; defined AI continuation rules; and clear data export mechanisms. Ethical governance encourages default preservation upon verified death, avoidance of forced deletion absent fraud risk, and role-based permission structures. Platforms should not rely solely on terms-of-service clauses to override lawful estate authority where statute provides access rights. Platforms violating DEPI ethical requirements lose accreditation.

10.26 Governance Failure Modes

Common failure patterns include: overbroad credential sharing during life; failure to categorize sensitive assets; lack of AI consent planning; ignoring cross-border implications; automatic deletion without audit; conflation of access with ownership; and failure to disclose enforcement uncertainty. These failure modes expose beneficiaries to harm, fiduciaries to liability, courts to ambiguity, and practitioners to disciplinary risk.

10.27 Public Policy Interface

Digital estate governance has implications beyond individual estates, affecting consumer protection, cybersecurity stability, AI governance debates, cross-border data sovereignty, and democratic trust in digital identity. Regulators and policymakers may rely upon doctrine-level standards to clarify fiduciary authority, define post-mortem privacy boundaries, address AI replication ethics, and reduce litigation uncertainty. This Part provides a structured baseline suitable for citation in regulatory deliberations.

10.28 Consolidated Ethical Presumptions

In the absence of express instruction, the following presumptions govern as doctrine-level guardrails:

- Identity integrity shall be preserved.

- Synthetic continuation requires affirmative consent.
- Access shall be tiered and purpose-limited.
- Deletion shall be deliberate and documented.
- Audit logs shall be maintained for all material actions.
- Cross-border uncertainty shall trigger escalation, not assumption.
- Commercial exploitation shall require explicit authorization.
- Biometric and genetic data shall be treated as high-sensitivity assets.
- Preserve before delete; restrict before expand; escalate rather than improvise.

10.29 Normative Requirements — Part X

Aligned systems and practitioners shall:

- Enforce staged release of emotional assets with explicit consent controls.
- Protect minors in all access, inheritance, and AI continuation workflows.
- Prohibit exploitative monetization of the deceased without explicit prior authorization.
- Maintain transparent, auditable governance of AI personas and synthetic artifacts.
- Freeze AI identity systems upon verified death by default.
- Label all synthetic, AI-generated, and representative communications clearly.
- Apply minimum necessary exposure in all post-mortem data disclosures.
- Treat biometric and genetic data as high-sensitivity assets irrespective of financial value.
- Suspend representation during any material beneficiary dispute.
- Document ethical risk assessment for all L2 and L3 post-mortem actions.
- Require a human-in-the-loop for all inheritance-critical blockchain actions.
- Disclose known uncertainty in AI continuation, cross-border enforceability, and platform resistance.

10.30 Part-Level Declaration

The DEPI Digital Estate Continuity Body of Knowledge and Standard™ affirms that ethical and post-mortem governance of digital estates is not an ancillary consideration — it is a structural necessity. Digital infrastructure has extended the temporal reach of identity beyond biological life. Governance must therefore evolve correspondingly.

Digital estates are not merely repositories of value. They are structured continuations of human narrative. Failure to govern them ethically creates legal exposure, social harm, institutional instability, and erosion of trust in digital systems.

Ethical governance is not optional discretion. It is the governing conscience of this entire Standard.

PART XI — FUTURE-STATE CONTINUITY SYSTEMS

As humanity transitions into an era defined by multimodal AI, spatial computing, extended reality, neuro-integrated interfaces, decentralized digital identity, biometrically anchored cryptographic systems, high-fidelity volumetric capture, and long-term digital presence technologies, the nature of personal continuity, family legacy, business succession, and identity preservation will evolve in unprecedented ways. This Part provides a forward-looking framework to guide technology builders, policymakers, institutions, professionals, and families as continuity systems extend beyond traditional inheritance, single-generation asset transfer, device-based digital identity, and physical-world documentation.

DEPI recognizes that continuity must operate across decades, geographies, legal systems, platforms, and technologies that do not yet exist. This Part is non-normative but strongly recommended as guidance for emerging technology contexts.

12.1 Future Identity Constructs

12.1.1 Neuro-Digital Identity

Identity signals derived from neural interfaces, brain-computer interfaces, cognitive activity models, and biometric neuro-signatures will require specific continuity governance. NDI systems must have ethical inheritance boundaries; must not enable post-mortem impersonation; must be frozen upon death unless explicitly permitted; and must integrate with legal identity frameworks as they evolve.

12.1.2 Synthetic Identity Constructs

Future identity models may include AI-trained personal identity proxies, predictive digital twins, emotionally adaptive AI guardians, and co-evolving AI personas. Synthetic identities must be labeled clearly; must not override or replace real identity instructions; must have explicitly defined succession rules; and AI co-agents must be bound by ethical constraints.

12.1.3 Distributed and Multi-Anchor Identity

As identity becomes decentralized, continuity must map authority across distributed anchors. Inheritance must unify multi-anchor identity; executors must be able to manage distributed identity clusters; and metadata must bind identity to the user, not the system.

12.2 Future Digital Asset Classes

12.2.1 Spatial-Life Archives

High-fidelity volumetric recordings capturing life events, conversations, experiences, surroundings, and personal history raise continuity concerns around long-term rendering compatibility, privacy of third parties captured in spatial scenes, and emotional sensitivity of the content.

12.2.2 Holographic Presence Assets

Holographic last messages, 3D presence archives, and volumetric AI avatars must be clearly labeled as immersive assets; must not be used for exploitation or misrepresentation; and must require explicit user authorization.

12.2.3 Digital Twin Intellectual Property

Digital twins containing business knowledge, trade processes, and professional expertise require SMB inheritance governance, IP ownership verification, and multi-party governance structures.

12.2.4 Cross-Platform AI Memory Clouds

Future families may inherit multi-generational AI-enhanced memory clouds and merged parental memory repositories. Continuity governance must address what is ethically inheritable, the rights to AI interpretations of personal histories, and the prevention of memory distortion across generations.

12.3 Future Continuity Triggers

Bio-digital triggers initiated by biometric events, neural inactivity, or medical device integration must always require human verification before activation. AI predictive triggers — where AI detects cognitive decline or health risk patterns — may inform but must never solely initiate inheritance; AI-triggered warnings must require human confirmation. Cross-system event triggers spanning devices, chains, and cloud services must use verified multi-source data, override mechanisms, and interoperability protocols.

12.4 Long-Term Preservation and Ultra-Longevity

As digital assets persist across centuries, continuity must address 100-plus year archives, AI-enhanced genealogical systems, and multi-generational digital storytelling. Immersive and cognitive assets must remain readable for decades, support format migration, preserve contextual meaning, and avoid technological decay. Multi-generational continuity must enforce ethical controls and prevent identity misuse across generations.

12.5 Future Ethics and Post-Biological Governance

AI and synthetic identities based on user data must remain subordinate to legal estate instructions, avoid simulating conversations on behalf of the deceased unless authorized, and prevent misrepresentation as living entities. Unless explicitly enabled by the user, platforms must not create persistent post-mortem digital selves, must not allow autonomous AI evolution, and must not permit generative simulation beyond configured boundaries. Future memory technologies must prevent false-history generation, unauthorized reinterpretation, harmful emotional manipulation, and synthetic distortion of truth.

12.6 Future Interoperability Standards

Continuity across future systems requires: cross-platform asset portability; identity linking across devices and chains; long-term metadata preservation; heir-friendly playback environments; and standardized export formats. DEPI will publish updates as emerging technologies mature.

12.7 Regulatory Foresight

DEPI anticipates future regulation in AI post-mortem rights, immersive data inheritance, neuro-data governance, synthetic identity governance, cross-border XR asset jurisdiction, and blockchain inheritance law. Platforms should design systems expecting strong consent laws, identity authenticity requirements, AI activity restrictions, and expanded executor authority. DEPI commits to maintaining technology-neutral standards; updating the Standard on an annual cycle; monitoring AI, AR/VR/XR, BCI, and identity innovation; collaborating with legislators; educating professionals; and stewarding ethical digital legacy.

PART XII — APPENDICES AND REFERENCE MODELS

This Part provides non-binding reference materials designed to support interpretation of Parts I–XII, enhance consistency in implementation, provide defensible documentation models, assist expert witnesses and regulators, and support accreditation audits.

Appendix A — Glossary of Defined Terms

Term	Definition
Access	The technical ability to view or interact with a digital asset. Access does not imply ownership or commercialization rights.
AI-Augmented Identity	Digital identity layer consisting of AI-generated models, memory structures, behavior profiles, or cognitive simulations trained on personal data.
AI Memory Model	A machine-learning model representing an individual's knowledge, preferences, or history, requiring ethical inheritance controls.
Alignment	Voluntary conformance with the normative requirements of this Standard.
Asset Category	Classification grouping defining digital assets based on purpose, sensitivity, inheritance rules, and continuity requirements.
Authority Validation Memorandum (AVM)	A documented analysis confirming lawful authority, scope, and jurisdictional considerations prior to material digital asset action.
Beneficiary Liability Risk (L1/L2/L3)	A classification model identifying potential downstream regulatory, contractual, financial, or reputational exposure resulting from digital asset transfer or control.
Blockchain Anchor	A cryptographic hash representing off-chain metadata, used for provenance and audit without storing personal data on-chain.

Term	Definition
CDEP — Certified Digital Estate Professional	DEPI's primary professional certification covering continuity standards, asset governance, and estate workflows.
Cognitive Continuity	Preservation of a person's digital knowledge, AI-generated content, or augmented memory assets across time and succession events.
Commercialization	Use of digital assets, identity, likeness, or intellectual property for economic gain.
Continuity Fiduciary	The person or entity holding lawful authority to administer digital assets.
Continuity Plan	A structured set of inheritance, identity, and delegation rules defining what happens in emergency, incapacity, and post-mortem scenarios.
Continuity Trigger	A verified event (death, incapacity, emergency) that initiates continuity workflows.
Cross-Border Trigger	Any fact pattern implicating more than one jurisdiction in digital asset administration.
Cryptographic Identity	Identity derived from cryptographic keys, signatures, MPC, multi-sig access structures, or DIDs.
Custody Model	The structural method by which digital assets are held: custodial, self-custodial, or hybrid.
Delegated Authority	Role-based permissions allowing designated individuals to access specific assets or continuity functions.
Digital Execution Plan (DEP)	A structured continuity annex providing asset inventory, rights mapping, risk classification, and entitlement mapping. Not a testamentary instrument.
Digital Executor / Trustee	The legally authorized individual responsible for administering the digital portion of an estate.
Digital Identity	A collection of credentials, login artifacts, identifiers, and authentication mechanisms representing a user online.
Emotional Digital Asset	Sentimental content intended for heirs: letters, messages, videos, memory NFTs, and AI-based legacies.

Term	Definition
Executor Authority Mapping	The process of matching legal executor authority to digital asset categories and access scopes.
Inheritance Execution	The procedural transfer of identities, keys, rights, and access following a verified post-mortem event.
Key Recovery Workflow	Mechanism enabling continuity of cryptographic assets without exposing private keys.
Licensed Digital Product	A digital asset governed by contractual license rather than ownership; typically non-transferable at death.
Multi-Sig / MPC	Security schemes requiring multiple parties or cryptographic shards for access — mandatory for blockchain inheritance.
Post-Mortem Continuity	Phase in which digital assets and identity layers transition to executors, trustees, or beneficiaries following verified death.
Preservation Doctrine	The requirement to pause destructive or irreversible actions when authority or scope is uncertain.
Smart Contract Governance	Rules for updating, overriding, or modifying smart contracts in response to legal or continuity events.
Synthetic Communication	AI-generated speech, likeness, or representation of a deceased individual.
Trusted Contact	An individual authorized to receive notifications or initiate continuity checks but not asset-level access.

Appendix B — Digital Asset Taxonomy

A consolidated taxonomy spanning all asset categories defined in Domain 2.

Category	Description and Continuity Requirements
Category 1 — Financial Digital Assets	Online bank accounts; brokerages and trading platforms; payment systems (PayPal, Stripe, Zelle); crypto exchanges (centralized); insurance and retirement portals; reward points and loyalty programs; SMB accounting

Category	Description and Continuity Requirements
	systems. Continuity: high verification and legal authority required.
Category 2 — Communication and Identity Assets	Email accounts; phone numbers and SIM identity; messaging apps; social media accounts; contact directories; influencer and business identity accounts. Continuity: executor read-limited; identity continuity required to prevent impersonation.
Category 3 — Personal Data and Cloud Storage	Photos and videos; cloud drive content; password managers; documents and records; subscription accounts. Continuity: granular access required.
Category 3A — Emotional Digital Assets	Legacy letters; videos for children; voice messages including stored voicemail; future-dated messages; memory NFT artifacts; AI-generated emotional content. Continuity: privacy-first, staged delivery only.
Category 4 — AI-Generated Cognitive Assets	AI personas; autobiographical models; AI knowledge graphs; predictive behavioral engines. Continuity: freeze post-mortem unless explicitly authorized.
Category 5 — Business and Operational Assets	CRM systems; operational and productivity cloud and hosted accounts; password vaults; digital business identity; vendor portals; AI automation systems. Continuity: SMB workflow required.
Category 6 — Blockchain and Cryptographic Assets	Crypto wallets; on-chain tokens; NFTs (identity or emotional); smart-contract-locked assets; tokenized rights. Continuity: multi-sig and MPC mandatory.
Category 7 — Intellectual Property Assets	Code repositories; CAD files; patents; trade secrets; proprietary designs; model weights; open-source contributions. Continuity: ownership verification and confidentiality preservation required.
Category 8 — Representation and Derivative Rights	NIL-style rights; digital twin licensing; geospatial monetization rights; royalties; avatar-based appearances. Continuity: L3 governance; express authorization required for continuation.
Category 9 — Immersive and Spatial Digital Assets	AR/VR/XR environments; holographic recordings; volumetric spatial captures; AI-augmented immersive

Category	Description and Continuity Requirements
	simulations. Continuity: encrypted storage; staged release; age gating for minors.

Appendix C — Emotional Digital Asset Guidelines

C.1 Privacy and Sensitivity Requirements

Emotional assets must be encrypted; hidden from executors unless explicitly authorized; released only to designated beneficiaries; and never used for marketing or AI training without consent.

C.2 Staged Release Mechanisms

Emotional assets may use time delays, milestone releases such as birthdays and graduations, segmented releases by content type, and conditional releases based on defined events. These release schedules may not be overridden by executors or platforms except by court order.

C.3 Ethical Content Guidelines

Platforms must detect harmful emotional content; warn beneficiaries before exposure to potentially distressing material; and provide configurable options to block content containing violence or abuse.

C.4 AI-Generated Emotional Assets

If AI generates messages or simulations: AI must not be mistaken for the deceased; AI must not fabricate false memories; AI must not interact beyond user-defined boundaries; and AI emotional assets must be labeled as AI-generated at all points of access.

C.5 Inheritance of Emotional NFTs

Emotional NFTs must: store no private content on-chain; link to encrypted off-chain assets; provide metadata permanence; and preserve authenticity provenance for families.

Appendix D — Smart Contract Template Models

Template 1 — Time-Locked Release Contract

Features: timelock expiry with user-defined date; revocation mechanism allowing cancellation before expiry; multi-sig override requiring multiple parties; and human-in-the-loop confirmation before release. Use case: messages and emotional assets.

Template 2 — Multi-Party Approval Inheritance Contract

Required approvals: executor; platform continuity module; and optional beneficiary confirmation. Use case: financial or high-risk crypto assets requiring coordinated authority.

Template 3 — Oracle-Based Death Verification Contract

Required elements: multi-source oracle verification; redundancy mechanisms; manual override pathway; and dispute resolution protocol. Use case: automated triggering under verified death events.

Template 4 — Key Rotation and Reassignment Contract

Functions: key revocation; successor key assignment; inheritance of multi-sig roles; and continuity recovery pathways. Use case: continuity of blockchain identity across succession.

Template 5 — AI Model Continuity Contract

Tracks: model provenance; freeze state; authorized use cases; and beneficiary rights. Use case: AI persona and memory model inheritance governance.

Appendix E — Accreditation Audit Checklist

This checklist is used during DEPI platform accreditation. Platforms must pass all mandatory items.

Area	Requirements
E.1 Security	AES-256 encryption at rest; TLS 1.2+ in transit; encrypted backups; password hashing best practices; zero-knowledge architecture verified if claimed.
E.2 Identity	KYC and identity verification; robust delegate assignment; executor verification workflows; recovery mechanisms for device and credential loss.
E.3 Continuity Workflows	Emergency workflow functional; post-mortem workflow functional; incapacity workflow functional; delegation mapping functional; inheritance execution complete.

Area	Requirements
E.4 Data Integrity	Versioning implemented; audit logs maintained; metadata exportable; retention rules enforced; 7-year log retention confirmed.
E.5 AI and Emotional Asset Controls	Model freezing implemented; ethical labeling enforced; sensitive content safeguards active; emotional staging functional.
E.6 Blockchain Controls (if applicable)	Multi-sig or MPC implemented; smart contracts audited; override controls functional; no PII on-chain confirmed; oracle redundancy verified.
E.7 Transparency and User Protection	Disclosures clear and understandable; risks explained at onboarding; terms understandable in plain language; consent revocation supported.
E.8 Documentation	Internal policies documented; compliance artifacts available; incident response plan documented; continuity technical diagrams current.

Appendix F — Certification Competency Map

This appendix defines the knowledge domains required for DEPI certifications (CDEP, DAC, DCP) and maps them to curriculum tracks.

Certification Track	Core Domains and Parts	Core Frameworks and Appendices
Legal and Fiduciary Track	Domains 1, 2, 3, 7, 8, 9; Regulatory Part XI	Frameworks 1, 2, 3, 7; Workflows PF-3, PF-7
Platform and Engineering Track	Domains 1, 4, 5, 6; Parts VII, VIII	Frameworks 1, 3, 4, 5; Workflows PF-6, PF-7
Risk, Security, and Governance Track	Domains 2, 3, 5, 6, 7; Part VIII	Frameworks 3, 4, 7; Appendix E, G
AI and Ethics Track	Domains 1, 4, 8, 10; Parts X, XII	Frameworks 6, 7; Appendix C
Blockchain and Cryptographic Track	Domains 1, 4, 5; Parts VII, VIII	Frameworks 3, 4, 5, 7; Appendix D

Foundation knowledge required for all tracks includes: digital asset taxonomy; continuity principles; identity layers; and legal frameworks governing wills, trusts, and probate. Regulatory and compliance knowledge including GDPR, RUFADAA, eIDAS, HIPAA, and cross-border conflict doctrine is required for all tracks. Professional ethics per Part X is required for all certification holders.

Appendix G — Risk Assessment Templates

G.1 Asset Risk Evaluation Template

Minimum required fields: asset identifier; asset category (Categories 1–9); platform or provider; custody type (custodial / self-custodial / hybrid); ownership type; licensed versus owned status; risk tier (L1/L2/L3); cross-border trigger indicator; authority instrument reference; continuity risk score (1–5); mitigation required; and disposition status.

G.2 Identity Risk Template

Fields to assess: identity layer risks per Domain 1; MFA dependencies and fallback mechanisms; device-loss risk; key loss probability; and executor verification complexity.

G.3 Continuity Workflow Risk Template

Assess: emergency workflow gaps; incapacity workflow gaps; post-mortem workflow vulnerabilities; and orphaned asset scenarios where no continuity configuration exists.

G.4 Blockchain Risk Template

Fields: key management architecture; oracle dependencies; smart contract immutability and upgrade status; network risk; multi-party governance structure; and irreversible loss potential.

G.5 AI-Legacy Risk Template

Assess: model integrity risk; harmful output risk; impersonation risk; synthetic memory distortion risk; and post-mortem misuse risk.

G.6 SMB Continuity Risk Template

Fields: key-person dependency mapping; operational asset risk; credential sprawl assessment; account survivorship analysis; and vendor lock-in risk.

Appendix H — Smart Contract Governance Checklist

Item	Verification Question
Audit documentation	Has the smart contract been formally audited by an independent qualified security firm?
Determinism verification	Is the contract's behavior fully deterministic and documented?
Override mechanism	Is a human override mechanism implemented and tested?
Upgrade pathway	Is the contract upgradeable or migratable without asset loss?
Inactivity prohibition	Is inactivity-triggered inheritance explicitly prohibited in contract logic?
On-chain/off-chain linkage	Are on-chain events linked to off-chain authority verification records?
PII exclusion	Is the contract confirmed to contain no PII on-chain?
Dispute hold capability	Can execution be paused upon dispute trigger?
Multi-party approval	Does the contract require multi-party approval for L3 asset actions?
Oracle redundancy	Are oracle sources redundant and tamper-resistant with multi-attestation?
Migration plan	Is a network migration or chain-fork contingency plan documented?
Plain language summary	Has a plain-language summary been provided to end users?

Appendix I — Standards Interoperability Reference

Framework	Domain	DEPI Alignment Notes
ISO/IEC 27001:2022	Information security management	Domain 5 security controls align with Annex A control objectives.
NIST SP 800-63 (Rev. 4)	Digital identity assurance	Domain 1 identity layer model references IAL/AAL assurance levels.

Framework	Domain	DEPI Alignment Notes
NIST Cybersecurity Framework 2.0	Cybersecurity risk management	Part VIII risk controls map to Identify/Protect/Detect/Respond/Recover.
RUFADAA / UFADAA (USA)	Fiduciary access to digital assets	Domain 7 and Part XI defer to RUFADAA where enacted.
EU eIDAS 2.0	Digital identity and trust services	Domain 1 cryptographic layer references DID/VC requirements.
EU AI Act (2024)	AI governance	Domain 8 and Part X AI doctrine aligns with high-risk AI obligations.
GDPR and analogous statutes	Data protection and privacy	Domain 7 and Part XI map to controller obligations for post-mortem data.
ISO Blockchain Framework	Blockchain and distributed ledger technology	Part VII blockchain requirements are complementary to ISO TC 307 standards.

Appendix J — Expert-Witness Review Checklist

Area	Expert Review Test
Authority	Was authority validated prior to material action? Was an AVM produced for L3 assets?
Risk Classification	Was L1/L2/L3 classification applied? Was process intensity proportional to risk?
Cross-Border Analysis	Were cross-border triggers identified? Was a JEM produced?
Preservation Doctrine	Was preservation doctrine applied under uncertainty? Were destructive actions paused during disputes?
Platform Engagement	Were platform interactions lawful, documented, and non-circumventive?
Licensed Products	Were licensed digital products treated contractually and not assumed transferable?
Representation Governance	Were synthetic or commercial representations authorized, labeled, and documented?

Area	Expert Review Test
Beneficiary Liability	Was beneficiary liability exposure evaluated and documented for L2/L3 assets?
Smart Contract Compliance	Were smart contracts audited, override-capable, and free of prohibited practices?
AI Governance	Were AI models frozen upon death? Were all AI outputs labeled? Was consent documented?
Security Controls	Were encryption, access control, and logging requirements met per Part VIII?
Documentation Sufficiency	Is documentation audit-ready and capable of supporting independent expert review?
Closure Record	Was administration formally closed with a Closure Certification Record?

Appendix K — Risk-Tier Decision Reference Matrix

Asset Example	Suggested Tier
Domestic network credential shared with explicit authorization	L1
Sentimental archive with no confidentiality issues	L1
Licensed streaming account — read/view access only	L2
Email account — read-only access	L2
Monetized social media channel	L2
Digital art with royalty structures	L2 or L3 depending on commercial scope
Intellectual property portfolio	L2 or L3
Business operating accounts	L3
Material cryptocurrency portfolio	L3
AI-trained identity or persona tool	L3

Asset Example	Suggested Tier
Trade secret repository	L3
Digital health or biometric data store	L3
Cross-border asset with regulatory exposure	L3
NIL-style derivative rights or likeness licensing	L3
Smart-contract-locked asset	L3
NFT-based emotional asset with public chain linkage	L2 or L3

Appendix L — Alignment Maturity Reference Model

Maturity Level	Description
Level 1 — Ad Hoc	No documented lifecycle; reactive handling; no risk-tier governance; no platform engagement protocol.
Level 2 — Documented	Lifecycle and risk-tier framework present but inconsistently applied; some documentation maintained.
Level 3 — Structured	Consistent authority validation, documentation, risk-tiered disposition, and cross-border review applied.
Level 4 — Integrated	Enterprise-level governance, audit logs, representation controls, and AI governance integrated into practice.
Level 5 — Institutionalized	Cross-border policy harmonization, regular independent audit, continuous improvement cycle, and public accountability mechanisms in place.

Appendix M — Version Control and Change Log

Version	Material Revisions
v1.0 (February 2026)	Initial published standard. Platform-requirements format. Sections 1–11 covering identity, asset taxonomy, lifecycle,

Version	Material Revisions
	workflows, smart contracts, security, accreditation, ethics, regulatory alignment, and future-state framework. Established digital asset classification model and continuity lifecycle.
v1.1 (Working Draft)	Repositioned as Body of Knowledge and Standard. Added Domains 6–10 (Platform Architecture, Regulatory Alignment, Ethics, Dispute Resolution, Professional Standards). Added seven Process Frameworks. Added Parts IV–VI structure. Introduced L1/L2/L3 beneficiary liability classification. Added legal boundary statements and DEP doctrine.
v1.2 (Draft Standard, May 2026)	Full synthesis of v1.0 and v1.1. Retained all v1.0 technical specificity including six operational workflows, smart contract framework, security controls, eight accreditation domains, ethics framework, regulatory alignment framework, and future-state guidance. Integrated v1.1 doctrinal architecture including ten Knowledge Domains, seven Process Frameworks, and normative standard requirements. Ethics consolidated into Part X. Twelve parts, thirteen appendices (A–M). All editorial scaffolding removed. All numbering reconciled.

Appendix N — Digital Execution Plan Schema

The Digital Execution Plan (DEP) is a structured continuity annex — not a testamentary instrument — that provides the inventory, rights mapping, risk classification, and entitlement mapping necessary for defensible estate administration. The following schema defines the minimum required fields for a DEPI-aligned DEP.

Field	Description
Asset Identifier	Unique reference number assigned at onboarding.
Asset Name and Description	Plain-language description of the asset.
Asset Category	Classification per Domain 2 taxonomy (Categories 1–9).
Platform or Provider	Name, URL, or identifying information.
Custody Type	Custodial / self-custodial / hybrid.

Field	Description
Ownership Type	Individual / joint / corporate / licensed / work-for-hire.
Licensed vs. Owned	Licensed use or full ownership. If licensed, transferability status.
Risk Tier	L1 / L2 / L3 with documented rationale.
Identity Layer Mapping	Which identity layer(s) control access to this asset.
Delegation Configuration	Who may access, what they may do, and under what conditions.
Authorized Post-Mortem Communications	APMC instructions if any (see Appendix O).
Cross-Border Annotations	Known jurisdictional triggers or constraints.
Authority Instrument Reference	Will / trust / DEP / POA / platform designation tool.
License and IP Constraints	Open-source obligations, royalty structures, export controls.
Disposition Instructions	Transfer / archive / memorialize / delete / commercialize.
Audit References	Linkage to audit logs, AVM, BLRM, or other documentation.
Version History	Date, scope, changes, and reviewer for each revision.
Last Review Date	Date of most recent review and next scheduled review.

The DEP schema is structured but adaptable. Fields may be added for specific asset types or jurisdictional requirements. The DEP must be exportable, interpretable by non-technical executors, and version-controlled. It must not be represented as a testamentary instrument.

Appendix O — Authorized Post-Mortem Communication Templates

Authorized Post-Mortem Communications (APMC) are pre-authorized, bounded communications configured during life for delivery after death or incapacity. The following template models illustrate the major APMC categories. These templates are advisory; they do not interpret platform policy or statutory authority. All APMC must be explicitly authorized in the DEP or continuity plan and must comply with applicable jurisdiction and platform rules.

O.1 Administrative Notice Template

Purpose: Factual notification of death or incapacity for administrative purposes. No representational content.

Suggested content elements: name of the deceased or incapacitated person; date of event; name and contact information of the authorized representative or estate; reference to governing legal authority; instructions for further contact.

Governance notes: Does not require AI labeling. Must remain factually accurate. Must not create financial commitments or legal representations. Appropriate for out-of-office messages, domain registrar notifications, and professional directory updates.

O.2 Memorialization Notice Template

Purpose: Public notification of death and transition of account to memorial status.

Suggested content elements: announcement of passing; direction to memorial page or estate contact; statement of intent for account (preserve / memorialize / close); acknowledgment of community relationships.

Governance notes: Must be issued by authorized representative, not impersonating the deceased. Should be clearly attributed to the estate or representative. Appropriate for social media platforms with memorialization tools.

O.3 Staged Release Message Format

Purpose: Delivery of pre-written personal communications on a scheduled or milestone basis.

Suggested content elements: personal message authored by the principal during life; delivery trigger (date, age of recipient, milestone event); recipient designation; instructions for recipient regarding the nature of the communication.

Governance notes: Must be pre-written by the principal — not AI-generated post-mortem unless explicitly authorized. Must be encrypted until delivery. Must respect staging schedule; no override by executor unless authorized. Appropriate for legacy letters, birthday messages, milestone communications.

O.4 Synthetic Output Labeling Format

Purpose: Required labeling for any AI-generated or algorithmically constructed communication issued in connection with a digital estate.

Required label elements: clear statement that the content is AI-generated or synthetically constructed; name of the deceased whose data informed the output; date of generation; name of the authorized party who approved the output; statement of scope of authorization.

Governance notes: This labeling is mandatory under DEPI alignment for all synthetic outputs. Synthetic content that could be mistaken for communications authored by the deceased requires heightened disclosure. Platforms must enforce this requirement for any AI continuation tools.

Appendix P — Advisory Clause Library

The following illustrative language blocks support continuity planning in estate documents, engagement letters, and continuity plans. All clauses are illustrative only and must be reviewed and tailored under governing law by qualified legal counsel. These clauses do not constitute legal advice and do not create enforceable obligations independent of the instruments in which they are incorporated.

P.1 Authority Subordination Statement

Suggested language: "Any digital continuity plan, digital execution plan, or technical continuity configuration associated with this estate shall remain subordinate to the governing instruments of this estate, applicable probate law, and court orders. In the event of conflict, governing law and court authority shall prevail."

P.2 Digital Execution Plan Incorporation Clause

Suggested language: "I have prepared a Digital Execution Plan (DEP) as a continuity reference document for my digital assets. The DEP is not a testamentary instrument and does not govern the distribution of my estate. It provides inventory, access guidance, and administrative instructions to assist my executor. The DEP is located at [location] and was last updated on [date]. My executor should treat the DEP as an operational reference, not as a legal directive."

P.3 AI Activation Consent Clause

Suggested language: "I [do / do not] authorize the use of AI-generated or synthetic representations of my voice, likeness, or persona after my death. [If authorized:] Such use is limited to the following scope: [specify]. All AI-generated content must be clearly labeled as AI-generated and must not be used for commercial purposes without the express written consent of my estate. [If not authorized:] All AI systems trained on my personal data shall be

frozen upon my death and shall not be activated, commercialized, or extended without court authorization."

P.4 Beneficiary Access Exposure Disclosure

Suggested language: "I acknowledge that certain digital assets designated in my estate plan carry access exposure risks for beneficiaries. My executor is directed to review the risk tier classification in my Digital Execution Plan before releasing access to any Tier 2 or Tier 3 assets and to provide beneficiaries with written disclosure of known legal exposure before any transfer or access is effectuated."

P.5 Licensed Digital Product Acknowledgment

Suggested language: "I acknowledge that certain digital products in my estate, including but not limited to [describe categories], are licensed rather than owned and may not be transferable at death. My executor is directed to review platform terms before attempting any transfer and to disclose licensing limitations to affected beneficiaries."

P.6 Cross-Border Uncertainty Disclosure

Suggested language: "My estate includes digital assets that may be subject to the laws of jurisdictions other than [primary jurisdiction]. My executor is directed to seek legal counsel regarding any digital asset with cross-border implications before taking action and to document enforcement feasibility assessments for any asset that cannot be governed under [primary jurisdiction] alone."

Appendix Q — Jurisdictional Autonomy Statement

Digital estate continuity operates across diverse legal systems. No single national doctrine governs the full scope of digital estate administration. This Standard recognizes the following jurisdictional realities that practitioners and platforms must account for:

- Succession laws vary by jurisdiction — inheritance rights, executor authority, and estate administration procedures differ materially across countries and, in the United States, across states.
- Digital asset access statutes vary — RUFADAA adoption is not universal; analogous statutes exist in some jurisdictions and are absent in others.
- Data protection frameworks differ — GDPR, CCPA, LGPD, PDPA, and their equivalents impose different obligations regarding post-mortem data handling.
- Personality and post-mortem rights vary — publicity rights, moral rights, and the duration of post-mortem identity protections differ significantly across jurisdictions.

- Blockchain and tokenized asset recognition varies — legal status of cryptocurrency, NFTs, and smart contract instruments is not uniform globally.

This Standard does not resolve these jurisdictional differences. It provides a governance framework that is designed to operate within them. Where jurisdictional conflict exists, practitioners shall document the conflict, assess enforcement feasibility, and escalate to qualified jurisdictional counsel rather than assume that governing law of the principal's domicile resolves all questions.

Multiple legal systems may apply to a single account. When statutory variation meets layered jurisdiction, structured planning becomes essential.

FINAL DECLARATION

The Digital Estate Planning Institute publishes this Body of Knowledge and Standard™ as a structured governance framework addressing the complexity of digital identity and digital asset continuity.

This Standard:

- Clarifies the structure of the digital estate ecosystem and its intersection with governing legal systems.
- Operates subordinate to governing law at all times.
- Integrates technical, legal, ethical, and infrastructural considerations into a unified governance architecture.
- Provides a beneficiary-centric access exposure model that protects heirs, fiduciaries, and practitioners.
- Establishes structured lifecycle governance from discovery through closure.
- Integrates blockchain and AI systems within lawful boundaries.
- Defines voluntary alignment criteria for accreditation and certification.

Digital Estate Continuity is a governance discipline.

It is not a substitute for law.

It is not a reinterpretation of statute.

It is not a replacement for fiduciary duty.

It is a structured framework enabling practitioners, platforms, and institutions to operate responsibly within the evolving digital estate ecosystem — protecting individuals, families, and enterprises from the preventable loss, liability, and harm that result from ungoverned digital estates.

The work of digital estate continuity is the work of preserving what people built, protecting those they leave behind, and ensuring that the digital dimension of a life is governed with the same care and intention as the physical one.

— Digital Estate Planning Institute

Draft Standard v1.3 — May 2026

