DIGITAL ESTATE PLANNING INSTITUTE
depi.org

DEPI DIGITAL ESTATE CONTINUITY

CORE SUMMARY

A Structured Overview of the Standard for Professionals, Platforms, and Implementers

Companion to the Full Normative Standard | depi.org/standards

May 2026 | Draft for Public Comment

HOW TO USE THIS DOCUMENT

This Core Summary provides structured conceptual clarity on all major components of the DEPI Digital Estate Continuity Body of Knowledge and Standard™ v1.3. It is designed for professionals, platforms, and implementers who need adoption readiness without replacing the full normative document.

Document	Purpose and Audience
Executive Summary	For executives, regulators, institutions, and policymakers. Why digital estate continuity matters and what DEPI does about it. Non-technical strategic overview.
Core Summary (this document)	For professionals, platforms, and implementers. Structured overview of all Standard components, frameworks, normative requirements, and tools.
Full Standard (Normative)	For accreditation, certification, and implementation. The complete authoritative document defining all mandatory requirements, workflows, and governance rules.

> This document does not replace the Full Standard. For normative requirements, alignment claims, accreditation criteria, and certification examination purposes, the Full Standard at depi.org is the authoritative reference.

Part I — Foundations of Digital Estate Continuity

Part I establishes the doctrinal, definitional, and principled foundation of the entire Standard. Every normative requirement, process framework, and certification criterion traces back to the principles and hierarchy established here.

Discipline Definition

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.

This definition distinguishes the discipline from password management, digital vaulting, or blockchain inheritance. It is a governance discipline — not a technology product.

Eight Governing Principles

Principle	Statement	Layer
Legal Supremacy	Technical systems are subordinate to governing law.	Foundational
Access Is Not Ownership	Credentials create access; access does not equal ownership.	Foundational
Representation Is Not Title	Tokenization does not confer legal title.	Foundational
Beneficiary Protection	Continuity systems protect beneficiaries from downstream harm.	Operational
Structured Risk Governance	All assets classified using explicit risk model including beneficiary exposure.	Operational
Ethical Stewardship	Emotional and AI-augmented assets require dignity and consent safeguards.	Ethical
Human Governance Over Automation	No automated system irreversibly executes inheritance without human oversight.	Technical
Technological Neutrality	Standard applies to all platforms and architectures without privilege.	Structural

Legal and Governance Hierarchy

All continuity systems must defer to the following authority hierarchy, in descending order: (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; (6) regulatory mandates; (7) user-level continuity configuration; (8) technical rules and automation.

Practitioner Foundations (Sections 1.10–1.16)

Part I includes a practitioner foundations layer covering the key structural differences between physical and digital estates:

- The Discoverability Problem — digital assets are credential-gated and non-public; discovery is a governance obligation, not a preliminary step.
- Digital Orphans — tens of millions of accounts abandoned annually due to undiscovery.
- Control ≠ Ownership — credentials create access; access does not create authority to act.
- RUFADAA Priority Structure — platform online tools override wills and trusts; the three-tier hierarchy every practitioner must understand.
- Beneficiary Access Risk Tiers — L1 (Administrative), L2 (Contractual/Operational), L3 (Identity and Financial Control) with concrete platform examples.
- Explicit Authorization Doctrine — intent without documented authority creates liability.
- Structured Discovery Process — four-step practitioner process for complete inventory.

Part II — Core Knowledge Domains

Part II defines ten Knowledge Domains constituting the body of knowledge for digital estate continuity practice. Each Domain includes definition, key concepts, and embedded normative requirements.

Domain Summary Table

Domain	Key Coverage
Domain 1 — Identity Continuity	Four identity layers (legal, platform, cryptographic, AI-augmented). Identity risk surfaces. Authorized Post-Mortem Communications (APMC). MFA continuity pathways.
Domain 2 — Digital Asset Taxonomy, Origination, and Rights	Nine asset categories (Financial; Communication; Personal Data; Emotional; AI-Cognitive; Business; Cryptographic; Intellectual Property; Representation/Derivative; Immersive/Spatial). L1/L2/L3 beneficiary-centric risk classification. Origination modes. Ownership vs. licensing distinction.
Domain 3 — Continuity Lifecycle and Execution Governance	Ten lifecycle stages from origination through destruction. Digital Execution Plan (DEP) doctrine. Executor authority mapping. Versioned DEP requirements.
Domain 4 — Cryptographic and Smart Contract Governance	Key management discipline. Tokenization doctrine. Smart contract governance requirements. Blockchain-specific regulatory considerations.
Domain 5 — Risk and Security Governance	Beneficiary protection as primary risk driver. Core control areas. Immutable audit doctrine. Incident response requirements.
Domain 6 — Platform Architecture and Operational Continuity	Deployment models. Cloud governance. Custodial vs. non-custodial architecture. Platform survivability and shutdown risk.
Domain 7 — Regulatory and Jurisdictional Alignment	Legal precedence model. Data protection alignment. IP and regulatory interface. Financial and securities considerations. AI governance interface.
Domain 9 — Dispute Resolution, Enforcement, and Institutional Interfaces	Dispute typology (7 categories). Preservation and non-destruction doctrine. Evidentiary integrity. Cross-border enforcement doctrine.
Domain 10 — Professional Standards, Certification, and Continuing Competence	Professional identity doctrine. Competency architecture. Standard of care. Disclosure obligations. Continuing competence imperative.

> Note: Domain 8 (Ethics and Post-Mortem Governance) is developed at full depth in Part X of the Standard, positioned as the governing conscience of the entire document.

Part III — Process Frameworks

Seven canonical operational frameworks translate doctrinal requirements into executable professional practice. Each framework defines process architecture, required outputs, and alignment obligations.

Framework Reference Table

Framework	Summary
Framework 1 — DECL Digital Estate Continuity Lifecycle	Six phases: Discovery/Inventory → Intent/Authority Architecture → Continuity Design/Controls → Maintenance/Drift → Triggered Activation → Administration/Closure. Required output artifacts per phase.
Framework 2 — RBCOM Role-Based Continuity Operating Model	Five core roles: Principal, Continuity Fiduciary, Digital Operations Steward, Legal Authority Validator, Beneficiary Risk Guardian. RACI discipline and escalation pathways.
Framework 3 — AEP Authority and Evidence Protocol	Three-step authority validation (Instrument Hierarchy → Jurisdictional Alignment → Scope Determination). Evidence preservation protocol. Chain-of-custody documentation. Expert-witness readiness standard.
Framework 4 — RTDF Risk-Tiered Disposition Framework	L1/L2/L3 disposition pathways with defined documentation requirements per tier. Five disposition modalities (Transfer, Archive, Memorialize, Delete, Commercialize). Dispute sensitivity override.
Framework 5 — PERP Platform Engagement and Refusal Playbook	Five engagement phases: Pre-Engagement Preparation → Formal Request → Clarification → Refusal Assessment → Escalation. Non-circumvention doctrine. Emergency situation protocols.
Framework 6 — PMCRP Post-Mortem Communications and Representation Process	Five communication categories (Administrative Notice, Stewarded, Legacy Continuation, Synthetic, Derivative Commercial). Authorization verification. Reputation risk review.
Framework 7 — CBEF Cross-Border Execution Framework	Jurisdictional Exposure Map (JEM). Governing law conflict analysis. Data protection transfer compliance. Platform governing law clauses. Cross-border dispute escalation.

Workflow Specifications

Seven detailed operational workflows cover every continuity scenario:

- PF-1: Primary Continuity Workflow — baseline configuration and planning
- PF-2: Emergency Access Workflow — incapacity, lockout, crisis scenarios
- PF-3: Executor and Trustee Workflow — legally authorized post-death succession
- PF-4: Family Continuity Workflow — emotional assets, staged releases, AI model governance
- PF-5: SMB Continuity Workflow — key-person risk, business operational continuity
- PF-6: High-Risk Asset Workflow — crypto, unrecoverable vaults, smart-contract-locked assets
- PF-7: Post-Mortem Workflow — eight-step complete post-mortem administration process

Parts IV–V — Normative Requirements and Accreditation

Part IV — Normative Standard Requirements

Part IV consolidates all shall/must requirements into four structured sections for DEPI voluntary alignment claims:

Section	Coverage
Section IV-A: Governance and Structural	Governance foundation, identity continuity, asset classification, beneficiary protection, DEP requirements.
Section IV-B: Operational and Documentation	Lifecycle implementation, documentation and auditability, platform engagement.
Section IV-C: Blockchain, AI, and Representation	Smart contract requirements, post-mortem representation, cross-border review.
Section IV-D: Alignment Declaration and Integrity	Alignment representation, scope accuracy, revocation triggers.

> Alignment Levels: DEPI alignment may be claimed at Program Level (institutional), Professional Level (individual), Case Level (specific estate administration), or Platform/Custodial Level (service providers). Each level has defined requirements in Part IV.

Part V — Accreditation and Certification Framework

Part V establishes the governance structure for organizational accreditation and individual certification.

Accreditation Level	Requirements
Foundational Alignment	Core governance controls implemented. Policy review and basic lifecycle evidence.
Advanced Alignment	Structured documentation, cross-border capability, L3 risk management maturity.
Institutional Alignment	Enterprise-level governance, audit discipline, continuous improvement evidence.

Individual certifications: Certified Digital Estate Professional (CDEP), Advanced Digital Continuity Practitioner (ADCP), and Digital Estate Governance Specialist (DEGS). Competency assessment covers all ten Knowledge Domains with scenario-based evaluation. See Appendix F for the full Certification Competency Map.

Parts VI–IX — Technical, Security, and Regulatory Governance

Part VI — Smart Contract and Blockchain Inheritance Framework

Mandatory requirements for all platforms using blockchain, smart contracts, wallets, DIDs, NFTs, or cryptographic assets:

- Mandatory third-party audit of all inheritance smart contracts before deployment.
- Deterministic behavior, human override, and upgradeability requirements.
- Four trigger types: time-based, event-based, oracle-based, multi-party approval.
- Key management: multi-sig or MPC mandatory; single-seed-phrase dependency prohibited for accreditation.
- Prohibited practices: inactivity-triggered inheritance, PII on-chain, execution without human confirmation, unverifiable oracles.

Part VII — Risk Management and Security Controls

Five-category threat model (Technical, Human, Operational, Legal, AI-Related) with blockchain-specific additions. Security controls cover: AES-256 encryption, TLS 1.2+, zero-knowledge architecture, spatial privacy controls, RBAC, MFA, seven-year log retention, and asset-specific requirements for emotional, cognitive, and high-risk assets.

Part VIII — Platform Accreditation Requirements

Eight accreditation domains evaluated during DEPI platform accreditation:

- 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
- Domain 8: User Protection, Transparency, and Ethics

Three accreditation tiers: Accredited, Accredited (Conditional), Not Accredited. Annual renewal required.

Part IX — Regulatory and Compliance Alignment

Jurisdiction/Domain	Key Requirements
United States	RUFADAA (three-tier priority structure in detail), HIPAA, GLBA, COPPA, ESIGN/UETA, federal and state blockchain regulations.
European Union	GDPR (post-mortem application), eIDAS 2.0, Digital Markets Act, Digital Services Act.
Asia-Pacific	Singapore PDPA, Australia Privacy Act, Japan digital asset regulations, South Korea PIPA, India DPDP Act.
LATAM	Civil law inheritance structures, Brazil LGPD, tokenized securities considerations.

Jurisdiction/Domain	Key Requirements
Blockchain Systems	Data protection compliance, smart contract override protocol, geographic jurisdiction disclosure.
AI Systems	EU AI Act, OECD AI Principles, US AI safety guidance, national AI risk frameworks.

Part X — Ethics, Dignity, and Post-Mortem Governance

Part X is the governing conscience of the Standard — positioned after all technical and regulatory content deliberately, as the ethical framework that governs everything that precedes it.

Nine Core Ethical Principles

Autonomy, Informed Consent, Dignity of the Deceased, Privacy and Confidentiality, Beneficiary Protection, Fairness and Non-Discrimination, Transparency, Accountability, and Non-Exploitation. These principles apply to all DEPI-aligned platforms and professionals.

Key Governance Areas

- AI and Synthetic Continuation — model freezing requirements; controlled post-mortem AI behavior; data minimization.
- Emotional Digital Asset Ethics — staged release; intergenerational timing; harm avoidance.
- Consent, Rights, and Revocation — explicit, documented, asset-specific consent; propagation of revocation.
- Ethical Use of Blockchain — human-in-the-loop for all inheritance-critical blockchain actions.
- Digital Dignity — right to be remembered; right to erasure; right to non-impersonation; right to accurate legacy.
- Fiduciary Liability Exposure — documentation requirements for L2/L3 post-mortem actions.
- Algorithmic Influence After Death — post-mortem data use and model training considerations.

Consolidated ethical presumptions: preserve before delete; restrict before expand; escalate rather than improvise. Synthetic continuation requires affirmative consent. Commercial exploitation requires explicit authorization.

Part XI — Future-State Continuity Systems

Part XI is non-normative guidance for emerging technology contexts. It establishes that DEPI's ethical principles and governance architecture apply to technologies not yet in widespread deployment.

- Neuro-Digital Identity — brain-computer interfaces, cognitive activity models, biometric neuro-signatures.
- Synthetic Identity Constructs — AI-trained identity proxies, predictive digital twins, co-evolving AI personas.
- Spatial-Life Archives — volumetric recordings, holographic presence assets, digital twin IP.
- AI Memory Clouds — multi-generational cognitive datasets, cross-generational memory inheritance.
- Post-Biological Governance — prohibition on default digital reincarnation; governance of digital personhood beyond biological life.

DEPI commits to annual Standard updates as emerging technologies mature.

Part XII — Appendices Reference Guide

Appendix	Content	Type
Appendix A	Glossary — 30 defined terms	Reference
Appendix B	Digital Asset Taxonomy — 9 categories with continuity requirements	Reference
Appendix C	Emotional Digital Asset Guidelines — privacy, staging, ethics, NFTs	Guidance
Appendix D	Smart Contract Template Models — 5 template types	Tools
Appendix E	Accreditation Audit Checklist — 8 control areas	Audit
Appendix F	Certification Competency Map — 5 tracks mapped to domains	Certification
Appendix G	Risk Assessment Templates — 6 template types	Tools
Appendix H	Smart Contract Governance Checklist — 12 items	Audit
Appendix I	Standards Interoperability Reference — 8 frameworks	Reference
Appendix J	Expert-Witness Review Checklist — 13 areas	Audit
Appendix K	Risk-Tier Decision Reference Matrix	Reference
Appendix L	Alignment Maturity Reference Model — 5 levels	Reference
Appendix M	Version Control and Change Log	Reference
Appendix N	Digital Execution Plan Schema — all required fields	Tools
Appendix O	APMC Templates — 4 template types	Tools
Appendix P	Advisory Clause Library — 6 clause types	Tools
Appendix Q	Jurisdictional Autonomy Statement	Reference

Quick Reference: Key Concepts

The L1/L2/L3 Risk Classification Model

Tier	Definition and Examples
L1 — Low Exposure	Minimal legal and regulatory risk. Administrative efficiency presumed. Examples: streaming, WiFi, food delivery.
L2 — Conditional Exposure	Contractual constraints, ongoing obligations, conditional transferability. Examples: email (read access), licensed accounts, monetized social channels.
L3 — High Exposure	Regulatory, criminal, civil, or IP exposure likely. Examples: bank accounts, cryptocurrency portfolios, AI-trained identity tools, trade secret repositories.

The Digital Execution Plan (DEP)

A structured continuity annex — not a testamentary instrument — providing: asset inventory; ownership classification; rights mapping; risk-tier assignment; delegation configuration; APMC instructions; cross-border annotations; audit references; and version history. Must be exportable, interpretable by non-technical executors, and version-controlled.

The RUFADAA Three-Tier Priority Structure

Priority	Description
Tier 1 — Platform Online Tools	Google Inactive Account Manager, Apple Digital Legacy, Facebook Legacy Contact. THESE OVERRIDE WILLS AND TRUSTS.
Tier 2 — Legal Documents	Will, trust, POA. Operative if no online tool governs. Constrained by platform terms.
Tier 3 — Terms of Service / Default Law	Controls if neither online tools nor legal documents address the question.

Seven DEPI Process Frameworks at a Glance

Framework	Core Function
DECL	Six-phase lifecycle from discovery through closure.
RBCOM	Five roles with RACI discipline and escalation pathways.
AEP	Three-step authority validation with expert-witness readiness standard.
RTDF	Risk-tiered disposition with L1/L2/L3 documentation requirements.
PERP	Five-phase platform engagement with non-circumvention doctrine.
PMCRP	Five communication categories with authorization and labeling requirements.

Framework	Core Function
CBEF	Jurisdictional Exposure Map with cross-border enforcement analysis.

DEPI Digital Estate Continuity Body of Knowledge and Standard™ v1.3 | Digital Estate Planning Institute | depi.org

This Core Summary is a companion document. It does not replace the Full Standard. For normative requirements, accreditation criteria, and certification examination purposes, consult the Full Standard at depi.org/standards.