DEPI
DIGITAL ESTATE
PLANNING INSTITUTE

Digital Estate Planning Institute (DEPI)

Core Summary

Digital Estate Continuity Standard™ v1.0

This Core Summary provides a structured overview of the **Digital Estate Continuity Standard™** for professionals, platforms, and implementers.

It explains the conceptual architecture of the Standard, how its major components fit together, and how it is intended to be used in practice.

This summary is explanatory and non-normative. The Full Standard remains the authoritative reference.

Purpose and Scope

The Digital Estate Continuity Standard™ defines how digital identity, digital assets, authority, and governance must be preserved and transferred across all continuity events, including emergency access, incapacity, succession, and post-mortem administration.

The Standard applies across individuals, families, businesses, platforms, and institutions operating in multi-jurisdictional and multi-technology environments.

Digital Identity Continuity Framework

At the core of the Standard is the principle that identity continuity precedes asset continuity.

Digital identity is defined as a multi-layer construct consisting of:

- Legal identity (government authority and legal documentation)
- Digital identity (accounts, credentials, authentication systems)
- Cryptographic identity (keys, wallets, signatures, decentralized identifiers)
- AI-augmented identity (AI models, memory systems, digital personas)

Continuity must be preserved across all layers.
Failure at any single layer can result in total loss of access or authority.

Digital Asset Classification Model

The Standard establishes a uniform taxonomy for classifying digital assets, including:

- Financial digital assets
- Communication and identity assets
- Personal data and records
- Emotional digital assets
- AI-generated cognitive assets
- Business and operational systems
- Blockchain and cryptographic assets
- High-risk assets requiring special handling

Asset classification determines applicable continuity workflows, access scope, inheritance rules, ethical constraints, and security requirements.

Continuity Lifecycle Model

The Standard defines a complete lifecycle covering:

1. Creation
2. Storage
3. Protection
4. Access management
5. Delegation
6. Continuity triggers
7. Inheritance execution
8. Post-mortem governance
9. Archival preservation
10. Destruction (where applicable)

Continuity planning must be proactive, auditable, and resilient to device loss, credential failure, and organizational change.

Continuity Workflows

Standardized workflows are defined for:

- Primary continuity planning
- Emergency access
- Executor and trustee activation
- Family and emotional asset inheritance
- Small and medium-business continuity
- High-risk asset recovery

All workflows require identity verification, authority mapping, proportional access control, and comprehensive logging.

Blockchain, Security, and Risk Management

Blockchain technologies may support continuity but must not override legal authority or create irreversible failure modes.

The Standard requires:

- Multi-party or recoverable key management
- Human oversight and legal override mechanisms
- No reliance on inactivity-based triggers
- Defense-in-depth security controls
- Risk management that supports inheritance rather than preventing it

---

Ethics and AI Governance

The Standard introduces explicit ethical requirements governing:

- Dignity of the deceased
- Persistent and revocable consent
- Privacy beyond death
- Protection of minors and vulnerable beneficiaries
- Default freezing of AI models post-mortem
- Prohibition of AI impersonation without authorization

Emotional and AI-generated assets are treated as high-sensitivity by default.

Relationship to the Full Standard

This Core Summary provides conceptual understanding only.

The **Full Standard (Normative)** defines all mandatory requirements, controls, workflows, accreditation criteria, and ethical obligations. The Full Standard is required for DEPI accreditation and certification programs.