DEPI
DIGITAL ESTATE
PLANNING INSTITUTE

Digital Estate Planning Institute (DEPI)

DIGITAL ESTATE CONTINUITY STANDARD™ v1.0

Contents

SECTION 1 — INTRODUCTION

1.1 Purpose of the Standard

The Digital Estate Continuity Standard establishes a unified, global framework for preserving, protecting, and transferring digital assets, digital identity credentials, AI-generated personal data, and continuity-critical information across individuals, families, businesses, and institutions.

Objectives include:

- Industry-wide interoperability
- Reliable professional practice
- Consumer protection

- Tool accreditation
- Regulatory alignment
- Ethical continuity for digital and AI-augmented identities
- Cross-border digital asset and identity continuity

1.2 Scope

This Standard applies to:

- Individuals and families
- Estate planners, fiduciaries, trustees
- Technology platforms & digital continuity tools
- Blockchain-based systems (where applicable)
- Digital identity providers
- Custodians and financial institutions
- SMBs managing digital continuity
- Cross-border estate scenarios
- AI-legacy and machine-generated personal data

1.3 Objectives

1. Establish a Digital Asset Classification Model
2. Define continuity lifecycle workflows
3. Provide identity and access continuity models
4. Establish minimum security controls
5. Provide ethical and AI continuity guidelines
6. Enable accreditation of platforms
7. Support professional certification
8. Provide a policy reference model for regulators

1.4 Terminology & Definitions

Definitions to be included in full draft:

- Digital Identity
- Digital Asset
- Emotional Digital Asset
- Continuity Trigger
- Cryptographic Key
- Legacy AI Model
- Smart-Contract Inheritance
- Delegated Access
- Multi-Party Continuity Framework
- Zero-Knowledge Access Proof
- Executor / Trustee Continuity

1.5 Relationship to Other Standards

This standard is complementary to:

- ISO/IEC 27001 (Security)
- ISO Blockchain Framework
- NIST Digital Identity Guidelines
- NIST Cybersecurity Framework
- RUFADAA (U.S. digital asset access)
- EU eIDAS 2.0
- GDPR (privacy)
- International probate & inheritance frameworks
- Blockchain interoperability standards

1.6 Applicability

This standard is voluntary and applicable to:

- Professionals

- Institutions
- Technology platforms
- Governing bodies
- Developers
- Executors & trustees
- Consumers seeking continuity guidance

1.7 Digital Continuity Lifecycle Overview

1. Creation
2. Storage & Protection
3. Access Management
4. Delegation & Continuity Configuration
5. Continuity Triggers
6. Transfer & Inheritance Execution
7. Archival Preservation
8. Destruction Protocols

SECTION 2 — DIGITAL IDENTITY CONTINUITY FRAMEWORK

2.1 Overview

The Digital Identity Continuity Framework defines the foundational identity models necessary to ensure that individuals, families, organizations, and platforms can maintain secure, continuous access to accounts, digital assets, records, services, and continuity-critical systems during:

- normal operations
- emergencies
- incapacity
- death
- succession
- and cross-generational transfer

This framework applies to:

- individuals
- trustees, executors, and authorized designees
- professional advisors
- digital continuity platforms
- identity providers
- blockchain or cryptographic identity systems
- custodians and institutions

Identity continuity is the first and most essential layer of the digital estate lifecycle.

2.2 Identity Layer Model

Digital identity is composed of multiple interconnected layers.
Continuity must be preserved across all layers.

2.2.1 Legal Identity Layer

The legal identity layer includes:

- government-issued identification
- legal documents confirming authority (power of attorney, trust documents, executor appointments)
- estate planning documents that authorize access and delegation

Continuity Requirements:

- Identity verification for executors/trustees must comply with jurisdictional laws.
- Platforms must provide workflows for legally appointed representatives to claim continuity access.
- Legal identity must override digital identity where conflicts arise.

2.2.2 Digital Identity Layer

The digital identity layer includes:

- usernames

- passwords
- authentication credentials
- platform-specific identity tokens
- login sessions
- cloud authentication profiles

Continuity Requirements:

- Platforms must support “survivorship” of accounts under legally verifiable continuity events.
- Identity reassignment must be auditable and reversible.
- Digital identity must not be permanently tied to a single device.

2.2.3 Cryptographic Identity Layer

Cryptographic identity includes:

- private/public key pairs
- blockchain addresses
- MPC or multi-sig identity constructs
- decentralized identifiers (DIDs)
- verifiable credentials (VCs)

Continuity Requirements:

- Platforms using cryptographic identity must support multi-party continuity.
- Users must not be placed at risk of continuity failure due to single-key loss.
- Recoverability must be provided via:
    - identity-based recovery
    - MPC recovery workflows
    - trustee/executor approval frameworks

2.2.4 AI-Augmented Identity Layer

Emerging identity types include:

- AI memory models
- digital personas
- personal AI knowledge graphs
- voice, image, and behavioral AI assets representing a person

Continuity Requirements:

- AI identity layers must support inheritance, access restrictions, and ethical controls.
- AI models containing personal data must support consent-based continuity transfer.
- AI identity fragments must be deletable when legally required.

2.3 Authentication Continuity

Authentication continuity ensures that identity verification mechanisms continue to function across continuity events.

Platforms must support the following:

2.3.1 Multi-Factor Authentication Continuity

All MFA methods must include continuity pathways, including:

- password continuity
- device change or loss
- biometric fallback
- email/phone recovery
- continuity account keys
- identity-based recovery via legal documentation

Continuity Requirements:

- MFA must never create lockout scenarios for estates or continuity delegates.
- MFA reassignment must be logged with timestamped audit trails.
- Emergency continuity modes must bypass MFA safely, with multi-party approval where possible.

2.3.2 Delegated Authentication Models

Delegated authentication enables:

- pre-authorized individuals
- executors and trustees
- continuity delegates
- corporate continuity managers

to authenticate into accounts or systems without impersonation.

Continuity Requirements:

- Delegated access must be distinct from personal access.
- Delegates must receive access only to what they are legally entitled to.
- The system must prevent unauthorized inheritance escalation.

2.3.3 Cryptographic Authentication Continuity

If cryptographic keys are used as authenticators:

- platforms must provide multi-party authentication options
- platforms must provide continuity workflows for:
  - lost private keys
  - compromised keys
  - inheritance transitions
  - incapacity events

Key continuity must not expose private keys to delegates.

2.4 Delegation & Authority Continuity

Delegation defines how identity rights are transferred or shared.

Platforms must provide support for:

Pre-death delegation

Incapacity delegation

Post-death executor/trustee delegation

Emergency access delegation

Organizational continuity delegation

2.4.1 Trusted Contacts

Platforms must allow users to designate trusted contacts for:

- identity verification
- continuity notifications
- non-privileged alerts

Trusted contacts do not receive asset access by default.

2.4.2 Continuity Delegates (Pre-Authorized Individuals)

Delegates may include:

- spouses
- partners
- adult children
- professional advisors
- fiduciaries

Continuity Requirements:

- Delegation rights must be granular (per asset or account).
- Delegation changes must be logged.
- Delegates must complete identity verification.

2.4.3 Executor & Trustee Identity Assignment

Platforms must support legally recognized successors with:

- access proportional to their authority

- multi-step verification
- document upload and validation
- automatic revocation when roles change

2.4.4 Corporate & SMB Identity Delegation

For businesses:

- continuity managers
- IT administrators
- financial officers
- operational continuity officers

must be able to assume identity responsibilities upon incapacity or death of key personnel.

2.5 Blockchain Identity Anchors (Integrated Blockchain Requirement)

If a platform uses blockchain or decentralized identifiers (DIDs) for identity:

2.5.1 Requirements

Platforms must:

- ensure blockchain identity anchors map to a verified off-chain identity
- support identity migration between chains where needed
- provide inheritance workflows without requiring private key exposure
- store no personal data directly on-chain
- use hash anchoring or cryptographic attestations for continuity metadata

2.5.2 DID & VC Requirements

Platforms using DIDs or Verifiable Credentials must:

- support revocable credentials
- support transfer of authority under legal documentation
- maintain audit logs of credential issuance and revocation

2.5.3 Key Loss & Recovery Requirements

Blockchain identity systems must implement:

- multi-party key recovery
- identity-based recovery
- trustee-assisted recovery
- cryptographic recovery workflows

Continuity must never depend on a single private key.

2.6 Identity Recovery & Revocation

Identity recovery ensures continuity despite:

- device loss
- key loss
- authentication system failure
- incapacitation
- death
- account seizure attempts
- estate disputes
- cross-jurisdictional conflicts

2.6.1 Recovery Requirements

Platforms must provide:

- multi-factor recovery
- identity-document-based recovery
- contact-based recovery (trusted contacts)
- legal document recovery (executor/trustee)
- biometric fallback
- blockchain recovery (if applicable)

Recovery must be:

- auditable
- secure

- reversible
- compliant with privacy laws
- proportional to the authority level being restored

2.6.2 Revocation Requirements

Platforms must allow:

- revocation of delegate rights
- revocation of trustee rights
- revocation of cryptographic credentials
- revocation of AI-generated identity models
- revocation of DIDs and VCs

Revocations must be:

- logged
- reversible if needed
- legally compliant
- propagated across all continuity systems

2.7 Identity Continuity Documentation

Platforms must provide:

- continuity documentation workflows
- identity continuity summaries
- downloadable continuity plans
- executor/trustee continuity packets
- AI identity usage disclosures
- blockchain continuity diagrams (if applicable)

Users and successors must be able to understand:

- who can access which assets
- under which conditions

- using which identity layer
- with what safeguards

SECTION 3 — DIGITAL ASSET CLASSIFICATION MODEL

3.1 Overview

The Digital Asset Classification Model establishes a standardized taxonomy for categorizing all digital assets relevant to estate planning, continuity, inheritance, identity preservation, and cross-generational transfer.

This taxonomy ensures:

- clarity for users
- uniformity for professionals
- enforceable rules for platforms
- consistent inheritance workflows
- legal and regulatory alignment
- accreditation compatibility
- continuity across technologies, including blockchain

Digital assets must be classified into one or more of the categories defined herein.

3.2 Classification Principles

All digital assets should be classified according to:

3.2.1 Ownership Type

- Individual
- Joint ownership
- Shared ownership
- Corporate or SMB ownership
- Distributed / decentralized ownership

3.2.2 Access Dependency

- Password-based

- Cryptographic key–based
- Identity-based
- Device-dependent
- Multi-party access

3.2.3 Sensitivity Level

- Highly sensitive
- Moderately sensitive
- Low sensitivity
- Public

3.2.4 Continuity Priority

- Critical continuity assets
- High-value assets
- Emotional continuity assets
- Time-delayed or future release assets

3.2.5 Legal Constraints

- Regulated
- Contractually restricted
- Jurisdiction-specific
- Probate-restricted
- Transfer-limited

Each classification determines which continuity workflows apply.

3.3 Asset Category 1 — Financial Digital Assets

Includes:

- Online bank accounts
- Investment portals
- Digital brokerage accounts
- Online mortgage, insurance, and pension systems

- Payment platforms (PayPal, Stripe accounts, Wise, etc.)
- Reward points and loyalty accounts (legally recognized digital value)
- Accounting systems critical to SMB continuity

Continuity Requirements:

- Must support legal appointment of executor/trustee
- Access transfer must comply with financial regulations
- Platforms must clearly define survivorship pathways

Cryptographic financial assets (crypto, tokenized securities) appear in Section 3.7.

3.4 Asset Category 2 — Communication & Social Identity Assets

Includes:

- Email accounts
- Messaging apps
- Social media profiles
- Contact lists
- Personal communication history
- Professional or influencer digital identity channels

Continuity Requirements:

- Executors/trustees require limited access, not full impersonation
- Platforms must support memorialization or closure
- Identity-based continuity must prevent fraud or impersonation
- AI-generated communication models must not operate post-mortem unless configured

These assets often connect to business and emotional continuity categories.

3.5 Asset Category 3 — Personal Data & Records

Includes:

- Photos and videos

- Cloud file storage
- Educational records
- Medical records
- Password managers
- Subscription accounts
- Digital purchase history
- Licenses and entitlements

Continuity Requirements:

- Executors require access to inventory but not necessarily content
- Beneficiaries require the ability to retrieve specific classes of data
- Emotional assets (see 3.5.1) require special ethical handling

3.5.1 Emotional Digital Assets (Subcategory)

Emotional digital assets include:

- Legacy letters
- Future-dated messages
- Story archives
- AI-generated family memory models
- Video diaries
- Personal reflections or private messages for children/heirs
- NFT-based emotional artifacts representing memories or relationships

Continuity Requirements:

- Must support privacy-respecting inheritance
- Must support time-delayed or staged release
- Must support encryption
- Must protect content from unauthorized access
- Must preserve metadata (dates, intent, source)

Platforms must distinguish emotional inheritance from financial inheritance.

3.6 Asset Category 4 — AI-Generated Cognitive Assets

Includes:

- AI memory models trained on the user’s data
- AI-generated personal writing, voice, or likeness
- AI personas
- Predictive behavioral models
- AI executive assistants holding proprietary knowledge
- Cognitive datasets (“digital brain archives”)

Continuity Requirements:

- Must support inheritance workflows
- Must include allergy to misuse (AI must not impersonate user post-mortem unless explicitly authorized)
- Must support revocation, deletion, or archival
- Freezing models upon death may be required
- Beneficiaries may inherit outputs, but not necessarily model rights

These assets require the strongest ethical governance in the Standard.

3.7 Asset Category 5 — Business & Operational Digital Assets

Includes:

- SMB cloud systems
- Internal documentation
- CRM systems
- Password managers for company accounts
- Key operational software
- Vendor accounts
- Operational AI automations
- Business identity credentials

Continuity Requirements:

- Must support key-person risk reduction
- Delegation must support SMB continuity
- Executors must be able to triage accounts
- Ownership must be preserved across business transitions

3.8 Asset Category 6 — Cryptographic & Blockchain Assets

Cryptographic digital assets include:

- Cryptocurrency wallets
- On-chain tokens
- Fungible asset tokens
- NFTs (including memory assets, tokenized documents, rights)
- Decentralized identifiers (DIDs)
- Smart-contract–bound assets
- Tokenized legal titles (where applicable)

Continuity Requirements:

3.8.1 Wallet Requirements

Platforms must support:

- multi-sig or MPC for inheritance
- key recovery
- delegated access rights
- device-agnostic access
- “continuity mode” in case of death/incapacity

3.8.2 Smart Contract Requirements

Smart contracts must be:

- audited
- upgradable under governance
- capable of multi-party continuity triggers

3.8.3 NFT Requirements

NFTs used for:

- documentation
- emotional assets
- identity anchors

must support:

- metadata permanence
- redaction (if required legally)
- continuity workflows

3.8.4 Tokenized Rights

Tokenized property rights or digital titles must have:

- cross-jurisdictional mapping
- accessible continuity pathways
- authenticated beneficiary proof

3.8.5 Disclosure Requirements

Platforms must inform users:

- network location
- immutability risks
- continuity risks
- identity recovery risks

3.9 Asset Category 7 — High-Risk Assets (Special Handling)

High-risk digital assets include:

- Crypto wallets with no recovery
- Password managers without backup
- Cloud systems with no identity delegation
- Unregulated digital assets
- Platforms without continuity protocols

- Accounts containing deepfake or synthetic media
- AI agents capable of generating harmful content
- Blockchain assets stored exclusively behind non-recoverable seed phrases

Continuity Requirements:

- Require stronger verification
- Must not rely on a single point of failure (e.g., one seed phrase)
- Must support inheritance without compromising security
- Must provide warnings and risk scoring to users

Platforms failing to meet these requirements cannot be accredited under DEPI.

3.10 Cross-Category & Compound Assets

Many digital assets fall into multiple categories simultaneously, e.g.:

- crypto wallets that contain sentimental NFTs
- cloud accounts storing financial statements + emotional videos
- AI models trained on business and personal data
- digital identities tied to financial accounts
- NFT-bound property rights with emotional value

Platforms must:

- preserve category distinctions
- apply continuity workflows based on the *strictest* applicable category
- ensure beneficiaries inherit only what they are authorized to access
- preserve privacy for emotional or sensitive content

3.11 Continuity Metadata Requirements

All assets, regardless of type, must include metadata for:

- category classification
- continuity priority
- sensitivity level

- inheritance rules
- asset ownership
- audit trails
- encryption state
- storage location (on-chain, off-chain, hybrid)

Metadata must be:

- consistent
- exportable
- interpretable by executors/trustees
- compatible with DEPI-accredited platforms

3.12 Immersive AR/VR/XR Spatial Digital Assets (Immersive Continuity Assets)

Immersive digital assets include:

- augmented reality (AR) memory objects
- virtual reality (VR) environments
- mixed-reality (XR) digital heirlooms
- holographic recordings
- volumetric spatial captures
- immersive “life scenes” recorded by spatial computing devices
- 3D reconstructions of personal artifacts or events
- AI-augmented immersive simulations representing the user

Continuity Requirements for Immersive Assets

1. Preservation Requirements
   Spatial assets must preserve:

- 3D rendering metadata
- device capture details
- AI augmentation markers
- continuity metadata

2. Inheritance Requirements
   Immersive assets must support:

- staged release
- beneficiary-specific access
- age gating for minors
- encrypted delivery

3. Ethical Requirements
   Immersive assets must not:

- fabricate false memories
- impersonate the deceased without authorization
- expose sensitive content inadvertently

4. Technical Requirements
   Platforms must offer:

- exportable formats (.usdz, .glb, .mp4 fallback)
- cross-platform compatibility
- long-term rendering support

SECTION 4 — CONTINUITY LIFECYCLE MODEL

4.1 Overview

The Digital Continuity Lifecycle describes the complete sequence of processes required to protect, preserve, and transfer digital assets and identity layers throughout a user's life, through incapacity, and after death.

The lifecycle includes:

1. Creation
2. Storage
3. Protection
4. Access Management
5. Delegation
6. Continuity Trigger Events
7. Transfer & Inheritance Execution

8. Archival Preservation
9. Post-Mortem Continuity Phase *(newly added)*
10. Destruction Protocols (when applicable)

This lifecycle applies to:

- individuals
- families
- executors & trustees
- professional advisors
- digital continuity platforms
- identity providers
- SMBs
- blockchain-integrated systems

4.2 Creation Phase

Digital assets are created through:

- account creation
- document generation
- AI model training
- file uploads
- business operations
- blockchain activity (wallets, NFTs, smart contracts)

Continuity Requirements:

- Assets must be automatically classified when possible
- Metadata must be attached upon creation
- Assets must include initial ownership and access rules
- AI assets must include ethical metadata (intended use, visibility, inheritance rules)
- Blockchain assets must be linked to an identity layer that supports continuity

Platforms should automatically detect high-risk assets and warn the user.

4.3 Storage Phase

Digital assets may reside in:

- cloud systems
- local devices
- password managers
- blockchain networks
- decentralized storage
- hybrid environments

Continuity Requirements:

- Storage systems must support metadata export
- Storage must support continuity workflows
- Assets must be retrievable by authorized parties
- Backups must be encrypted
- Cloud-based systems must not delete continuity-critical data prematurely

4.3.4 Blockchain Anchoring (Integrated)

If blockchain is used to anchor storage metadata:

Platforms must:

- Store only NON-PII data on-chain
- Use hash anchors instead of raw data
- Provide versioning for updated metadata
- Support “soft updates” for continuity (not breaking old chains)
- Provide fallback if blockchain network is unavailable

Blockchain anchoring does not replace secure off-chain storage.

4.3.5 Immersive Storage Requirements

Spatial assets must include:

- encrypted storage
- versioning
- fallback 2D representations
- rendering compatibility safeguards

4.4 Protection Phase

Digital assets must be protected through:

- encryption
- access controls
- device safeguards
- MFA
- cryptographic signatures
- redundancy
- data loss prevention

Continuity Requirements:

- Protections must not prevent inheritance
- Encryption keys must be recoverable by designated heirs (without exposing secrets)
- Device-based security must include cross-device continuity
- Identity-based protection must include successor pathways

Platforms must prevent continuity failures caused by:

- lost keys
- lost devices
- account lockout

4.4.6 Cryptographic Access Continuity (Integrated)

If cryptographic keys control asset access:

Platforms must provide:

- multi-sig / MPC–based inheritance

- identity-based recovery
- trustee onboarding without exposing private keys
- emergency override mechanisms
- continuity signals independent of device loss

Single point of failure = non-accreditable.

4.5 Delegation Phase

Delegation defines who may act on behalf of the user during:

- life
- incapacity
- emergencies
- after death

Delegation includes:

- trusted contacts
- continuity delegates
- executors & trustees
- business continuity officers
- legal guardians
- corporate administrators

Continuity Requirements:

- Delegation rules must be granular
- Delegates must be authenticated
- All delegation must be logged
- Delegation must support revocation
- Delegates may not gain unauthorized access

Delegation is NOT equivalent to inheritance.

4.6 Continuity Trigger Events

Trigger events activate continuity processes.

Approved events include:

4.6.1 Life-Based Triggers

- user-initiated continuity
- time-based releases (e.g., message delivery)
- life-event triggers (birthdays, milestones)

4.6.2 Emergency Triggers

- medical incapacity
- inability to authenticate
- loss of device
- risky anomaly detection

4.6.3 Death Triggers

- official death certificate
- verified obituary
- verified hospital notification
- court documentation
- blockchain oracle triggering (if used)

4.6.4 Multi-Party Triggers

- approval from trusted contacts
- approval from executor
- dual approval from heirs

Platforms must prevent malicious triggering.

4.7 Inheritance Execution Phase

Inheritance execution is the formal transfer of:

- access
- identity layers
- account rights

- cryptographic control
- emotional digital assets
- AI models
- operational authority (SMB continuity)

Continuity Requirements:

- Execution must follow legal orders
- Asset category determines inheritance workflow
- Smart contracts must support fallback or override
- Executor must be provided tooling to triage assets
- Identity must transfer without impersonation

Blockchain assets require:

- multi-sig release
- smart contract event execution
- oracle-based verification (if applicable)

4.7.1 Immersive Asset Inheritance

Platforms must:

- support staged or milestone-based delivery
- protect minors from premature exposure
- preserve immersive context
- ensure no AI-generated post-mortem editing unless pre-approved

---

4.8 Archival Preservation Phase

Archival processes govern long-term retention of:

- emotional digital assets
- documents
- financial history
- family legacy data
- AI identity models

- blockchain proofs (hash anchors)

Continuity Requirements:

- Archives must be encrypted
- Archives must support export
- Archives must be inheritable
- Archives must not be deleted prematurely
- AI models may be frozen in “post-mortem state”
- Blockchain metadata must remain interpretable over time

4.9 Post-Mortem Continuity Phase

The Post-Mortem Continuity Phase begins upon verified death and continues until all continuity processes are completed.

4.9.1 Death Verification Protocols

Acceptable verification sources include:

- certified death documents
- medical authority verification
- obituary validation
- court documents
- blockchain oracle verification (if configured)

Platforms must:

- audit verification
- log all events
- prevent automatic activation from inactivity

4.9.2 Executor / Trustee Activation

Platforms must:

- authenticate executor identity

- verify legal authority
- map authority to asset categories
- allow limited or full access based on rules
- log every continuity action

4.9.3 Post-Mortem Identity Transition

Identity rights transition to executor or trustee:

- access rights
- authentication rights
- authority to delete/preserve
- authority to manage AI assets
- authority over continuity configurations

Transitions must be:

- secure
- reversible
- auditable

4.9.4 Asset Transfer Protocols

Transfer includes:

- digital asset release
- smart contract execution
- cryptographic key transition
- release of emotional assets
- staged releases (if configured)
- business account triage

Blockchain assets require multi-party approval.

4.9.5 Post-Mortem Data Governance

Platforms must:

- protect sensitive data of the deceased
- support deletion or preservation
- support revocation of old credentials
- adhere to privacy laws
- provide heirs with appropriate export capabilities

4.9.6 Fraud & Abuse Prevention

Systems must defend against:

- false death claims
- forged documents
- impersonation
- malicious heirs
- premature asset release

Controls must include:

- multi-party validation
- delay timers (optional)
- continuous monitoring

4.10 Destruction Phase

Some assets require secure destruction:

- confidential files
- sensitive emails
- specific AI memory models
- accounts flagged for deletion under estate plan
- cryptographic keys no longer required

Destruction Requirements:

- must be irreversible

- must be logged
- must not compromise continuity of other assets
- must respect legal and ethical considerations

For blockchain, destruction may involve:

- key burning
- revoking authority
- rendering smart contracts inactive
- freezing associated assets

SECTION 5 — CONTINUITY WORKFLOWS

5.1 Overview

Continuity workflows provide repeatable, auditable, interoperable procedures for ensuring access to digital assets and identity layers through:

- normal circumstances
- emergencies
- loss of device
- incapacity
- death
- SMB operational failure
- catastrophic or unexpected continuity events

These workflows ensure that:

- users maintain control during life
- designated delegates can act when necessary
- executors and trustees can take lawful control
- beneficiaries and successors can receive inherited assets
- AI and blockchain systems execute continuity rules correctly
- no single point of failure jeopardizes continuity

Each workflow must include:

- authentication
- verification
- logging
- authority mapping
- rights assignment
- access release
- auditability

Platforms must implement each workflow without requiring users to manually orchestrate complex processes.

5.2 The Primary Continuity Workflow

This is the baseline workflow used for:

- configuration
- updates
- identity transitions
- continuity planning

5.2.1 Steps in the Primary Workflow

1. Identity Verification
   The user verifies identity via MFA, cryptographic key, or institutional authentication.
2. Asset Discovery or Import
   Assets are automatically detected or manually imported.
   Classification (Section 3) is applied.
3. Continuity Configuration
   The user configures:
   - delegates
   - triggers
   - inheritance rules
   - visibility rules
   - emotional asset timing

    - SMB continuity mappings

4. Metadata Binding
   Continuity metadata is bound to the asset, off-chain or on-chain.

5. Backup Continuity Creation
   Platforms must create fallback continuity paths.

6. Review & Finalization
   Users review their Continuity Plan and confirm.

5.3 Emergency Access Workflow

Triggered when a user is:

- medically incapacitated
- temporarily unable to authenticate
- unresponsive but not deceased
- experiencing a technical lockout
- in a crisis requiring third-party intervention

5.3.1 Emergency Workflow Steps

1. Trigger Event
    - delegated request
    - emergency contact request
    - biometrics unavailable
    - device lost
    - risk engine detection

2. Identity Verification of Requestor
   Strict but rapid verification.

3. Access Scope Determination
   Only emergency-allowed assets are accessible.

4. Time-Limited Access Window
   Access automatically closes unless extended.

5. Logging & Audit
   Full transparency required.

Emergency access does not imply post-mortem rights.

5.4 Executor / Trustee Workflow

This workflow governs access by legally authorized successors.

5.4.1 Steps in the Executor Workflow

1. Submission of Legal Documentation
    - death certificate
    - letters testamentary
    - trustee appointment
    - court order
2. Identity Verification of Executor
   Multifactor, document-based, biometric where available.
3. Authority Mapping
   Asset categories determine what can be accessed.
4. Continuity Mode Activation
   The system transitions to post-mortem or continuity governance mode.
5. Access Release
    - read-only for sensitive assets
    - full access for financial accounts where permitted
    - operational access for SMB accounts
6. Inheritance Execution (Section 4.7)
   Triggered according to legal and user-defined rules.
7. Audit & Logging
   Every action is logged and timestamped.

5.5 Family Continuity Workflow

This focuses on:

- emotional digital assets
- legacy letters
- future messages
- memory archives

- AI-generated identity or memory models
- inheritance of sentimental content

5.5.1 Steps in the Family Workflow

1. Verification of Beneficiary Identity
   (Non-financial, lower-bar verification allowed with restrictions.)
2. Visibility Rules Applied
   Beneficiaries see only what they are allowed to see.
3. Staged Releases
   Time-based or milestone-based release of letters, videos, messages, etc.
4. Ethical Handling of AI Models
   AI memories or personas must:
   - be frozen in post-mortem state
   - not evolve without configuration
   - be clearly labeled as AI assets
5. Download & Preservation Options
   Families must be able to save emotional assets offline.
6. Permanent Archival Options
   Platforms must support long-term preservation.

5.5.2 Immersive Memory Experience Delivery

Platforms must support inheritance of:

- volumetric recordings
- holographic messages
- spatial family memories
  with
- encryption
- staged exposure
- emotional harm safeguards

5.6 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
- digital identity is transferred to the successor

5.6.1 Steps in SMB Workflow

1. Key-Person Risk Identification
   Identify individuals whose absence jeopardizes continuity.
2. Continuity Delegation Assignment
   - IT administrator
   - operations lead
   - financial controller
3. Trigger Event
   - incapacity
   - death
   - emergency
   - offboarding
4. Identity Transition
   Business accounts transition to continuity managers.
5. Operational Recovery
   Systems brought back online.
6. Authority Reassessment
   New leadership transitions must be recorded.

Platforms must prevent SMB shutdown due to sole-owner digital failure.

5.7 High-Risk Asset Workflow

High-risk assets include:

- crypto wallets without recovery
- smart-contract–locked assets
- password vaults

- cloud accounts controlling financial or legal operations
- AI-powered accounts
- blockchain assets protected only by a single seed phrase

5.7.1 Required Steps

1. Risk Classification
2. Mandatory Warning to User
3. Mandatory Backup & Recovery Plan
4. Mandatory Multi-Party Continuity
5. Mandatory Delegation or Executor Assignment
6. Increased Verification Upon Access Requests

Platforms must not allow the user to configure continuity that results in irreversible asset loss.

5.8 Post-Mortem Workflow

This workflow begins once death is verified.

5.8.1 Step 1 — Notification Event

Triggered by:

- executor
- trusted contact
- legal authority
- verified obituary
- medical institution
- oracle (for blockchain systems)

5.8.2 Step 2 — Verification & Validation

Platform must:

- verify documentation

- authenticate requestor
- cross-reference estate plan
- apply risk engine checks

5.8.3 Step 3 — Executor Identity Verification

Requires:

- government ID
- legal documents
- MFA
- biometric or VC credential verification

Hybrid verification allowed.

5.8.4 Step 4 — Continuity Mode Activation

Platform transitions to continuity mode:

- user identity frozen
- AI models frozen
- triggers activated
- delegates restricted
- executor authority mapped

5.8.5 Step 5 — Asset Inventory Release

Executor receives:

- categorized inventory
- access levels per asset
- emotional asset separations
- AI asset summary

Assets are not immediately released; only the inventory is.

5.8.6 Step 6 — Inheritance Execution

Based on asset category:

For digital identity access:

- limited view for executors

For financial assets:

- full or partial release per legal rules

For emotional assets:

- staged release
- encrypted content delivery

For blockchain assets:

- multi-sig release
- key recovery workflows
- smart contract execution logs

5.8.7 Step 7 — Account Closure or Preservation

- Accounts closed per will, trust, or default protocol
- Accounts preserved if configured
- AI assets archived or deleted per directive

5.8.8 Step 8 — Final Audit & Reporting

Platforms must generate:

- continuity logs
- executor audit reports
- asset transfer summaries
- long-term preservation packets
- certificate of inheritance completion

SECTION 6 — SMART CONTRACT & BLOCKCHAIN INHERITANCE FRAMEWORK

6.1 Overview

Smart contracts and blockchain-based mechanisms may be used to enhance continuity and inheritance workflows by offering:

- tamper-proof execution
- deterministic transfer of assets
- verifiable event logs
- multi-party access control
- programmable inheritance logic
- cryptographic assurance

However:

Smart contracts cannot replace legal estate authority and Blockchain inheritance must integrate with legal, ethical, and identity-continuity requirements.

This section defines the mandatory requirements for any platform that utilizes blockchain, smart contracts, wallets, DIDs, NFTs, or tokenized assets in continuity or inheritance processes.

6.2 Smart Contract Requirements

Smart contracts used for inheritance MUST comply with the following controls.

6.2.1 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 (re-entrancy, signature forgery, oracle manipulation, etc.)
- analyzed for upgrade safety

Audit reports must be:

retained by the platform

made available to DEPI (upon accreditation review)

summarized for end users in plain language

6.2.2 Deterministic Behavior

Smart contracts must:

- behave predictably
- execute only when conditions are met
- not rely on ambiguous or unverifiable conditions
- not allow unauthorized execution
- ensure clear input/output states

Continuity rules must be machine-verifiable.

6.2.3 Human Override & 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
- beneficiaries contest the transfer

Override execution must be logged and require multi-party approval (executor + platform OR platform + DEPI-recognized continuity governance body).

6.2.4 Upgradeable & Governance-Controlled Contracts

All smart contracts must:

- be upgradeable OR
- include proxy-based governance mechanisms OR
- allow migration while preserving state continuity

This protects users from:

- outdated inheritance logic
- contract vulnerabilities
- evolving legal requirements
- multi-jurisdictional compliance updates

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

6.3 Blockchain Identity Requirements

Smart contract inheritance depends on identity correctness. Platforms must:

map smart contract roles to off-chain identity

support DIDs or VCs where appropriate

verify executor or beneficiary roles before granting on-chain authority

provide cryptographic attestations during inheritance execution

Identity verification must precede contract execution.

6.4 Trigger Systems for Smart Contract Inheritance

Smart contracts may only execute continuity rules upon legitimate, verified triggers.

Triggers fall into:

1. Time-Based Triggers
2. Event-Based Triggers
3. Multi-Party Approval Triggers
4. Oracle-Based Triggers

6.4.1 Time-Based Triggers

Time-based smart contract triggers must include:

- user-defined release dates
- time-locked delivery
- milestone-based releases
- future messages/memories release

Protection Requirements:

- user ability to modify or revoke time triggers
- delayed execution allowing objection windows
- multi-party override in emergencies

6.4.2 Event-Based Triggers

Event triggers include:

- medical incapacity
- business continuity events
- trustee activation
- SMB key-person loss
- regulatory events

Event verification must:

- be logged
- be reversible
- include multi-factor identity validation

6.4.3 Oracle Triggers (Blockchain Integration)

Oracles must:

- be tamper-resistant
- provide proof-of-origin

- support redundancy
- require multi-attestation for death verification
- prevent trigger spoofing

Oracles must NOT rely solely on:

- inactivity
- user silence
- single-source data
- unverifiable online claims

Oracles must support dispute resolution and override.

6.4.4 Multi-Party Approval Triggers

Inheritance must support multi-party approvals, such as:

- executor + platform
- executor + beneficiary
- platform + trusted contact
- legal authority + platform

This reduces risk of unilateral malicious action.

6.5 Continuity Logic & Role Assignment

Smart contract inheritance requires clear role definitions:

6.5.1 Contract Roles

- Contract Owner (user)
- Executor/Trustee
- Beneficiaries
- Delegates
- Guardian roles (optional)

6.5.2 Authority Mapping

Authority mapping determines:

- who can modify contracts
- who can approve execution
- who can revoke access
- who can trigger override

Mapping must reflect legal documents (will, trust, POA, etc.).

6.6 Key Management Requirements

If smart contracts rely on cryptographic keys:

6.6.1 Multi-Sig / MPC Requirements

Platforms MUST support continuity-friendly key systems:

- multi-signature wallets
- MPC-based splitting
- shard-based recovery
- hierarchical key structures
- backup keys stored securely by executor or platform

6.6.2 Executor Key Acquisition

Executors must never:

- require access to the user’s private keys
- need the user’s device
- bypass continuity rules to obtain keys

Key inheritance must occur via delegated authority, not secret sharing.

6.7 Smart Contract Execution Requirements

Before contract execution, platforms must verify:

1. authenticity of trigger event
2. legal authority
3. identity of executor or beneficiary
4. absence of disputes

5. override eligibility (in case of conflicts)

Post-execution:

- state changes must be logged
- beneficiaries must receive cryptographic proof
- residual contract functions must be disabled when appropriate

---

6.8 Auditability & Transparency

Smart contract inheritance must include:

6.8.1 On-Chain Event Logs

Logs must record:

- event triggers
- inheritance actions
- approvals
- denials
- overrides
- transaction hashes
- timestamps

Logs must be:

human-readable

exportable

legally admissible

6.8.2 Off-Chain Continuity Logs

Required for:

- identity verification
- document validation
- disputes

- recovery events
- manual override
- cross-border inheritance events

Off-chain logs must link to on-chain events via hash references.

6.9 Special Requirements for NFT-Based Emotional or Memory Assets

Where NFTs represent personal memories, emotional content, or family legacy:

Continuity Requirements

- metadata permanence
- encrypted storage of sensitive content
- no public-chain exposure of private assets
- staged release (time-based or milestone-based)
- explicit ethical configuration
- redaction support where legally required

Platforms must prevent:

- unauthorized post-mortem access
- AI manipulation of emotional NFTs without user consent

6.10 Legal, Regulatory & Ethical Alignment

Smart-contract inheritance DOES NOT override:

- wills
- trusts
- probate orders
- estate laws
- GDPR
- privacy rights
- AI ethics frameworks

Smart contracts must be subordinate to legal authority.

Platforms must ensure:

- smart contract logic aligns with user’s legal estate plan
- executors can override code under legal mandate
- cross-border inheritance rules are respected
- AI/identity continuity remains ethical and transparent

6.11 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
- misalign with legal authority
- use unverifiable oracles
- store personal data on-chain
- bypass executor verification
- allow unrestricted beneficiary access

Noncompliance results in non-accreditation under DEPI.

SECTION 7 — RISK MANAGEMENT & SECURITY CONTROLS

7.1 Overview

Digital continuity requires a robust, multi-layered security and risk-management framework that protects:

- identity
- access
- digital assets
- emotional and AI assets
- cryptographic materials
- continuity workflows

- inheritance processes
- family and SMB digital operations

Platforms and professionals must implement a risk-based, defense-in-depth model that supports:

- life-phase continuity
- incapacity continuity
- post-mortem continuity
- legal compliance
- cyber resilience
- multi-party authority
- technology neutrality
- blockchain-appropriate controls

Security controls MUST NOT impair continuity.
Continuity controls MUST NOT weaken security.

The goal is secure continuity, not continuity at the cost of security.

7.2 Risk Assessment Framework

All platforms must implement a formal, documented risk-assessment methodology that includes:

- identification of asset categories (Section 3)
- risk scoring
- continuity impact assessment
- threat modeling
- inheritance scenarios
- identity failure modes
- blockchain-specific risk (if applicable)
- AI-legacy risk assessment

Risk assessments must be updated annually, or sooner if:

- major features change

- legal frameworks evolve
- new cryptographic risks emerge
- new AI behavior patterns are introduced

7.2.1 Threat Categories

Threats include:

Technical Threats

- account takeover
- credential theft
- session hijacking
- device compromise
- API misuse
- smart contract exploit
- cryptographic key exposure

Human Threats

- malicious heirs
- insider abuse
- executor impersonation
- trustee misrepresentation
- social engineering attacks
- phishing attacks

Operational Threats

- service outages
- data corruption
- cloud provider failure
- blockchain network downtime
- continuity misconfiguration

Legal Threats

- disputed wills or trusts
- jurisdictional incompatibility
- conflicting beneficiaries
- misaligned inheritance triggers
- probate freezes on digital assets

AI-Related Threats

- AI impersonation of the deceased
- hallucinated or altered AI memories
- synthetic identity risk
- misuse of AI persona post-mortem

7.2.4 Blockchain-Specific Threat Modeling (Integrated Requirement)

Platforms using blockchain MUST additionally assess:

- smart contract vulnerabilities
- oracle manipulation
- chain reorganization / rollback
- seed phrase loss
- signature forgery
- key mismanagement
- cold-storage continuity failure
- custodial vs non-custodial risk
- NFT metadata loss

High-risk blockchain inheritance workflows cannot be accredited unless they include MPC, multi-sig, and recovery pathways.

7.2.7 Immersive Asset Risk Factors

Consider risks related to:

- deepfake spatial impersonation

- unauthorized holographic simulation
- psychological impact
- sensitive spatial detail leakage
- volumetric capture privacy

7.3 Security Controls

Platforms must implement advanced security controls across:

7.3.1 Encryption Requirements

All continuity-relevant data must be encrypted:

- in transit (TLS 1.2+)
- at rest (AES-256 or stronger)
- within backups
- in transit between services

Encryption keys must never:

- be stored in plaintext
- be accessible to unauthorized roles
- be used as inheritance triggers themselves

7.3.2 Access Control Requirements

Access must be enforced using:

- MFA
- role-based access control (RBAC)
- least-privilege principles
- robust permission auditing
- account isolation

Control requirements apply to:

- users
- delegates

- executors
- trustees
- administrators
- platform developers

7.3.3 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
- inheritance must occur through authority mapping, not secret disclosure

Platforms must document all zero-knowledge exceptions.

7.3.4 On-Chain Encryption & Privacy (Integrated Requirement)

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
- ensure GDPR, CCPA, and eIDAS compliance

Blockchain immutability must not conflict with deletion rights.

7.3.8 Spatial Privacy Controls

Platforms must:

- redact sensitive background elements
- encrypt volumetric frames
- prevent unauthorized 3D reconstruction

7.4 Identity & Key Management Controls

Identity and key management directly affect continuity integrity.

7.4.1 Identity Integrity Requirements

Platforms must:

- verify user identity at onboarding
- verify executor identity during inheritance
- validate delegates through MFA or VC credentials
- maintain identity continuity across device and account transfers

---

7.4.2 Key Storage Requirements

Keys controlling continuity must:

- be encrypted
- use hardware-backed secure storage if possible
- never be exposed to unauthorized parties
- use key rotation when risk is detected

7.4.3 Continuity-Focused Key Recovery (Integrated Requirement)

Key recovery is mandatory for:

- blockchain assets
- cryptographic identity systems
- encrypted emotional assets
- AI memory archives

Recovery methods can include:

- multi-sig
- MPC
- shard recovery
- identity-verified recovery
- executor-assisted recovery

No platform may rely solely on a single seed phrase.

7.5 Monitoring & Anomaly Detection

Continuity systems must include:

7.5.1 Session Monitoring

- unusual access patterns
- unusual geographic access
- multiple failed login attempts

7.5.2 Risk Scoring

Platforms must dynamically score:

- delegate actions
- executor actions
- post-mortem access requests
- account anomalies

7.5.3 Behavioral Detection

For AI-enabled systems:

- detect unauthorized AI actions
- detect attempts to impersonate deceased individuals
- detect changes in AI model behavior

7.6 Incident Response Requirements

Platforms must maintain an incident response plan for:

- account compromise
- key compromise
- fraudulent executor activation
- inheritance disputes
- smart contract exploits
- blockchain network downtime
- AI model corruption

- major outages

Incident response must include:

- containment
- user notification
- audit-level documentation
- legal escalation (if needed)
- continuity restoration

Continuity must not be permanently interrupted by incidents.

7.7 Vendor & Third-Party Risk Management

Digital continuity depends on vendors such as:

- cloud providers
- identity verification services
- blockchain networks
- API providers
- AI model hosting services
- storage systems

Platforms must:

- assess vendor risk
- maintain SLAs
- evaluate vendor continuity
- enforce encryption requirements
- monitor provider performance
- maintain secondary providers for redundancy

Vendor failures must not compromise estate continuity.

7.8 Post-Mortem Access Security Controls

Platforms must implement specialized controls to safeguard post-mortem workflows.

7.8.1 Death Verification Protection

Systems must:

- require multi-factor verification
- validate documents
- evaluate risk indicators
- check for early or fraudulent reporting

7.8.2 Executor/Trustee Access Controls

Must include:

- identity proofing
- legal authority checks
- granular access scopes
- audit logs

7.8.3 AI Post-Mortem Safeguards

Platforms must ensure AI does:

- not impersonate the deceased
- not create new content post-mortem unless authorized
- not generate harmful or misleading output

AI memory models may need to be frozen at death.

7.8.4 Smart Contract Safeguards

Smart contracts must:

- require human approval
- allow legal override
- disable auto-trigger inheritance based solely on time
- log all execution steps

7.8.5 Multi-Party Approval

High-risk actions must require:

- executor + platform approval
  or

- executor + beneficiary
  or
- executor + DEPI-accredited governance module

7.9 Security Logging & Audit Requirements

All continuity-relevant actions must be logged, including:

7.9.1 Identity Events

- authentication
- recovery
- delegations
- revocations

7.9.2 Inheritance Events

- trigger verification
- authority mapping
- asset release
- key transitions

7.9.3 Cryptographic Events

- blockchain event logs
- smart contract execution
- oracle results
- multi-sig approvals

7.9.4 AI Events

- model access
- model update
- memory archive access

Logs must be:

append-only

exportable

tamper-resistant

stored for a minimum of 7 years

7.10 Security Requirements for Emotional Digital Assets

Emotional assets (letters, videos, memory messages, AI-generated family content) require special rules:

- encryption required
- no default visibility for beneficiaries
- staged, timed, or conditional release
- sensitive content protected from unauthorized parties
- content must not be leaked via metadata
- AI-based emotional content must be explicitly configured

Emotional assets are treated as high-sensitivity by default.

7.11 Security Requirements for AI-Generated Cognitive Assets

AI identity assets require stricter controls:

- prevent unauthorized use of AI persona
- freeze model post-mortem unless release is configured
- prevent harmful AI behavior
- allow beneficiaries to inherit outputs, not necessarily model rights
- protect training data
- allow deletion under legal authority

AI integrity is a continuity issue.

7.12 High-Risk Asset Security Requirements

High-risk assets (crypto-only wallets, unrecoverable password vaults, etc.) must:

- use multi-party controls
- reject single-seed-phrase systems for accreditation

- include enhanced KYC
- include restricted access policies
- include warnings to the user
- require continuity configuration before accreditation

Platforms failing to meet these controls cannot be DEPI-accredited.

SECTION 8 — ACCREDITATION REQUIREMENTS FOR DIGITAL CONTINUITY PLATFORMS

8.1 Overview

This section defines the criteria and controls required for DEPI Accreditation, a formal process that evaluates whether a digital continuity platform or tool adheres to industry-wide standards governing:

- security
- identity continuity
- inheritance workflows
- data integrity
- consumer protection
- AI-legacy management
- blockchain or cryptographic components
- emotional asset handling
- regulatory alignment

Accreditation under DEPI is voluntary but strongly recommended for:

- digital vaults
- inheritance platforms
- continuity & identity systems
- blockchain-based continuity solutions
- AI-persona / memory systems
- SMB continuity tools
- custodial and non-custodial digital asset systems

Accreditation ensures trust, transparency, safety, and interoperability across the digital estate ecosystem.

8.2 Accreditation Structure

DEPI evaluates platforms across 8 Core Domains:

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

Platforms must meet minimum compliance in all domains and enhanced compliance in domains relevant to their architecture (e.g., blockchain, AI).

8.3 Domain 1 — Security & Encryption Controls

Platforms MUST implement:

8.3.1 Encryption Standards

- AES-256 or stronger at rest
- TLS 1.2+ in transit
- Encrypted backups
- Hardware-backed key storage where available

8.3.2 Access Security

- MFA across all privileged access
- Session monitoring
- Role-based access controls
- Least-privilege enforcement

8.3.3 Secrets Management

- Encrypted secret storage
- No plaintext credential storage
- Rotation policies for compromised secrets

8.3.4 System Integrity

- Mandatory code review
- Continuous vulnerability scanning
- Annual penetration testing

Platforms must prove these controls through documentation and audit testing.

8.4 Domain 2 — Identity Continuity & Delegation Systems

Platforms must demonstrate:

8.4.1 Identity Verification

- KYC/KYB processes
- Multi-factor authentication
- Identity recovery mechanisms
- Executor identity verification

8.4.2 Delegation Controls

- Pre-death delegation
- Incapacity delegation
- Post-mortem executor/trustee assignment
- Granular permission scopes

8.4.3 Identity Mapping

Mapping of:

- user
- delegates
- executors
- business continuity officers

must be stored in continuity metadata.

8.4.4 Device Independence

Identity access must not be tied to:

- a single device
- a single phone number
- a single authentication token

8.5 Domain 3 — Continuity Workflows

Platforms must support the following workflows fully and accurately:

8.5.1 Primary Continuity Workflow

Users must be able to configure:

- asset categories
- delegation rules
- inheritance preferences
- emotional asset handling
- AI continuity

8.5.2 Emergency Workflow

Platforms must provide emergency access that is:

- time-limited
- monitored
- logged

8.5.3 Incapacity Workflow

Platforms must support:

- legal incapacity proof
- restricted access for caregivers
- continuity without impersonation

8.5.4 Post-Mortem Workflow

Platforms must:

- verify death

- authenticate executor
- transition identity
- release assets according to user rules
- log all actions

8.5.5 SMB Workflow

Platforms must support:

- key-person delegation
- operational continuity
- account transition

8.6 Domain 4 — Inheritance Execution Controls

Platforms must:

8.6.1 Validate Legal Authority

- will
- trust
- letters testamentary
- court orders

8.6.2 Enforce Asset-Specific Rules

Financial, emotional, AI, and business assets must follow different inheritance rules aligned with Section 3.

8.6.3 Limit Unauthorized Access

Platforms must ensure:

- executors cannot see private emotional assets unless authorized
- beneficiaries cannot access restricted categories
- SMB continuity managers cannot access personal assets

8.6.4 Provide Exportable Evidence

Platforms must provide:

- inheritance reports

- chain-of-custody logs
- identity verification logs
- cryptographic proofs (if blockchain)

8.7 Domain 5 — Data Management, Integrity & Retention

Platforms must:

8.7.1 Maintain Data Integrity

- versioning
- integrity checks
- tamper-evident logs

8.7.2 Manage Metadata Properly

Metadata must include:

- asset category
- continuity rules
- visibility rules
- retention schedule
- encryption status
- storage location

8.7.3 Support User-Level Data Control

Users must be able to:

- export data
- update continuity rules
- revoke delegates
- delete content (with legal limitations)

8.7.4 Retention & Archival

- emotional assets preserved as configured
- AI models frozen or archived
- logs retained for 7+ years

8.8 Domain 6 — AI, Emotional & Cognitive Asset Governance

If a platform handles emotional or AI-generated assets, it must demonstrate:

8.8.1 Ethical Handling of Emotional Digital Assets

- encryption
- staged releases
- inheritance-level control
- privacy preservation
- metadata preservation

8.8.2 AI Continuity Controls

- freeze models post-mortem unless authorized
- do not impersonate the deceased
- preserve training data integrity
- allow deletion or revocation
- prevent AI from generating post-mortem content without consent

8.8.3 Synthetic Identity & Deepfake Protection

Platforms must implement:

- detection tools
- warning systems
- identity-verification checks
- anti-abuse controls

8.8.4 Immersive Asset Governance Requirements

Platforms handling AR/VR/XR assets must demonstrate:

- encrypted spatial storage
- ethical staging mechanisms
- minor protection policies
- AI augmentation labeling

- continuity across device generations

8.9 Domain 7 — Blockchain & Cryptographic Controls (If Applicable)

If a platform uses blockchain, smart contracts, NFTs, wallets, or cryptographic identity:

8.9.1 Key Management

- multi-sig or MPC mandatory
- key recovery mechanisms required
- no single-seed-phrase dependency allowed for accreditation

8.9.2 Smart Contract Controls

Contracts must be:

- audited
- upgradeable
- override-capable
- deterministic
- transparent

8.9.3 Oracle Integrity

Oracles must:

- be tamper-proof
- rely on multi-attestation
- support dispute resolution

8.9.4 NFT Metadata Integrity

NFTs used for emotional, identity, or continuity metadata must:

- not store sensitive data publicly
- support preservation
- support lawful deletion

8.9.5 Auditability

Platforms must offer:

- blockchain event logs
- continuity chain-of-custody

- hash proofs of off-chain data

Platforms failing to meet blockchain continuity standards cannot be DEPI-accredited.

8.9.6 Tokenized Immersive Assets (If Applicable)

If immersive assets are NFT-backed, platforms must:

- store no volumetric data on-chain
- use off-chain encrypted storage
- enforce authenticity provenance

8.10 Domain 8 — User Protection, Transparency & Ethics

Platforms must:

8.10.1 Provide Full Transparency

Users must understand:

- what data is stored
- where it is stored
- who can access it
- continuity rules
- inheritance triggers
- risks specific to blockchain or AI

8.10.2 Provide Risk Disclosures

Platforms must disclose:

- risk of asset loss
- risk of key loss
- smart contract risk
- AI impersonation risk
- continuity limitations

8.10.3 Provide Clear User Controls

Users must be able to:

- configure continuity

- modify rules
- revoke delegates
- export or delete assets
- freeze AI models

8.10.4 Adhere to Ethical Standards

Platforms must:

- honor privacy
- not manipulate emotional assets
- protect minors inheriting digital assets
- ensure AI-generated content is labeled

8.11 Accreditation Tiers

Platforms may receive:

8.11.1 Tier 1 — DEPI Accredited Digital Continuity System™

Full compliance across all applicable domains.

8.11.2 Tier 2 — DEPI Accredited (Conditional)

Conditional approval if:

- minor gaps exist
- roadmap exists to fix them
- no continuity-critical risks are present

8.11.3 Tier 3 — DEPI Not Accredited

Reasons include:

- single-seed-phrase design
- missing inheritance workflows
- poor identity verification
- storing sensitive data on public blockchains
- no AI safeguards
- no emergency or incapacity workflow

8.12 Accreditation Process

Platforms must undergo:

8.12.1 Application Submission

- technical architecture
- policy documentation
- security practices
- continuity workflow diagrams
- smart contract code (if applicable)

8.12.2 Review & Testing

DEPI reviews:

- documentation
- security controls
- identity workflows
- blockchain components
- AI assets
- UX for inheritance

8.12.3 Interview

Platform leadership must attend a DEPI review interview.

8.12.4 Remediation Window

If issues are discovered, DEPI may grant a corrections period.

8.12.5 Final Determination

A platform receives:

- Accredited
- Accredited (Conditional)
- Not Accredited

8.13 Renewal & Ongoing Compliance

Platforms must:

- undergo annual compliance reviews
- submit updated documentation for major releases
- disclose security incidents to DEPI
- maintain user protection commitments

Failure to maintain compliance revokes accreditation.

SECTION 9 — ETHICS, DIGNITY & POST-MORTEM GOVERNANCE

9.1 Overview

Digital estate continuity introduces ethical considerations beyond traditional estate planning, including:

- post-mortem dignity
- AI-generated identity preservation
- intergenerational emotional impact
- autonomy over digital memories
- privacy and consent of the deceased
- ethical use of continuity metadata
- responsibilities of executors, trustees, and delegates
- rights of heirs and beneficiaries
- boundaries for AI personas and cognitive assets

The DEPI Ethics Framework defines minimum ethical, privacy, and governance requirements for:

- platforms
- practitioners
- fiduciaries
- AI systems
- blockchain-based continuity tools
- accredited continuity systems

Compliance is mandatory for DEPI accreditation and certification.

9.2 Core Ethical Principles of Digital Continuity

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

9.2.1 Autonomy

The individual must retain control over:

- their digital identity
- continuity instructions
- emotional digital assets
- AI-personas derived from their data

No system may override the user’s explicit continuity settings, except by court order.

9.2.2 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
- how metadata may be preserved indefinitely

Platforms must provide clarity, not obscurity.

9.2.3 Dignity of the Deceased

Digital systems must never:

- exploit the deceased
- impersonate them for commercial gain
- alter AI personas in misleading ways

- expose private emotional content without authorization

Legacy dignity is paramount.

9.2.4 Privacy & Confidentiality

Even after death, privacy rights must be respected.

Platforms must:

- restrict access to sensitive content
- separate emotional content from general access
- encrypt all emotionally sensitive data
- ensure AI memories or personas cannot be misused

Privacy persists beyond death.

9.2.5 Beneficiary Protection

Beneficiaries must be protected from:

- inappropriate emotional content
- digital manipulation
- unmanaged AI content
- dangerous financial assets
- incomplete or inaccurate continuity data

The goal is protection, not burden.

9.2.6 Fairness & Non-Discrimination

Systems must not:

- privilege one heir incorrectly
- discriminate by geography, gender, age, or identity
- restrict inheritance arbitrarily

Continuity pathways must reflect the user’s wishes and legal authority.

9.2.7 Transparency

Platforms must disclose:

- continuity processes
- AI content behaviors
- blockchain usage
- smart contract logic (in plain language)
- identity handling
- key recovery mechanisms

No “black box” inheritance.

9.2.8 Accountability

Executors, trustees, continuity delegates, and platforms are accountable for:

- lawful handling of assets
- ethical preservation
- correct distribution
- maintaining audit trails
- respecting user intent

Accountability must be enforceable.

9.2.9 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
- promote unethical emotional interactions

Ethical boundaries must be explicit and enforced.

9.3 Ethical Handling of AI-Generated Identity & Memory Assets

AI-generated content presents unique ethical challenges.

Platforms must apply strict governance for:

- AI memory models
- AI persona bots
- predictive behavior engines
- voice or likeness models
- generative emotional assets
- autobiographical models

9.3.1 Model Freezing Requirement

Upon death:

AI models must be frozen unless explicitly authorized for continued operation.

Freezing prevents:

- uncontrolled evolution
- inaccurate personality drift
- unintended impersonation
- exploitation of the deceased's identity

9.3.2 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
- no commercial usage allowed unless explicitly permitted
- output must not misrepresent legal intent

Platforms must ensure AI never:

- makes financial decisions

- influences legal processes
- imitates the deceased deceptively
- manipulates vulnerable beneficiaries

9.3.3 Ethical AI Output Controls

AI assets must:

- filter harmful content
- avoid rewriting personal history
- provide accurate, unaltered memory summaries
- prevent hallucinated advice being treated as real estate instructions

AI cannot override legal estate documents.

9.3.4 Data Minimization

Only essential training data should be used for AI memories.

Highly sensitive data must be:

- excluded
- encrypted
- subject to deletion under user or executor authority

9.4 Emotional Digital Asset Ethics

Emotional assets include:

- letters
- videos
- time-delayed messages
- legacy content for children
- NFT-based memory assets
- AI-generated emotional archives

These require heightened ethical care.

9.4.1 Protection from Inappropriate Disclosure

Platforms must:

- restrict emotional assets from executors unless authorized
- release emotional content only to intended recipients
- enforce staging, timing, or milestone gates
- encrypt all emotional content

9.4.2 Intergenerational Timing Ethics

For children or minors:

- content may be delayed until a specified age
- content may be staged over years
- guardians may NOT override these settings

The user's emotional intent is binding.

9.4.3 Avoidance of Harm

Platforms must ensure emotional content does not:

- cause psychological harm
- deliberately manipulate heirs
- include abusive or damaging content without safeguards
- violate privacy of third parties

Ethical review is permitted when systems detect high-risk content.

9.4.4 Immersive Emotional Asset Ethics

Platforms must ensure immersive/holographic assets:

- do not mislead heirs
- clearly label AI involvement
- reflect authentic legacy content

- avoid manipulation or distortion

9.5 Consent, Rights & Revocation

9.5.1 Consent Framework

Consent must be:

- explicit
- documented
- revocable
- asset-specific

Platforms cannot rely on “blanket” consent.

9.5.2 Revocation Rights

Users must be able to:

- revoke delegates
- revoke executor consent (before death)
- revoke emotional asset access
- revoke AI post-mortem activity
- revoke blockchain execution triggers

Revocation must propagate across all continuity systems.

9.5.3 Heirs’ Rights

Heirs have rights to:

- see clear continuity logs
- receive assets legally designated
- challenge unethical or inaccurate AI-inheritance content
- request correction of inherited digital misinformation

Heirs do not have default rights to emotional or private content.

9.5.4 Executor Duties Under DEPI

Executors must:

- honor privacy
- act without exploitation
- protect emotional data
- disclose actions to beneficiaries when appropriate
- follow legal authority
- preserve audit logs

Executors cannot use continuity systems for personal gain.

9.6 Ethical Use of Blockchain in Inheritance

Blockchain-based inheritance must preserve:

- consent
- legal compliance
- privacy
- reversibility
- dignity
- transparency

Platforms must avoid:

- irreversible errors
- unverified triggers
- auto-transfer without human confirmation
- storing sensitive content on-chain
- exploiting beneficiaries with complex or unsafe blockchain mechanics

DEPI requires a human-in-the-loop for all inheritance-critical blockchain actions.

9.7 Digital Dignity & Post-Mortem Governance

Digital dignity applies to the deceased, their heirs, and their community.

Platforms must support:

9.7.1 Right to Be Remembered

Emotional assets must be preserved when the user requests it.

9.7.2 Right to Erasure

The deceased's prior instructions override default archival policies unless prohibited by law.

9.7.3 Right to Transparency

Executors must know what assets exist and how to process them.

9.7.4 Right to Non-Impersonation

AI systems cannot impersonate the deceased unless explicitly configured and ethically constrained.

9.7.5 Right to Accurate Legacy

Platforms must not modify:

- AI memories
- personal content
- historical materials

unless authorized.

9.7.6 Immersive Presence Ethics

Post-mortem holographic or volumetric reconstructions must:

- be used only if explicitly authorized
- never impersonate the deceased without disclosure
- avoid generating new simulated "memories"
- respect cultural and personal dignity standards

9.8 Ethical Requirements for Practitioners & Professionals

Estate planners, advisors, fiduciaries, and DEPI-certified professionals must:

- avoid conflicts of interest
- disclose platform affiliations
- maintain confidentiality
- avoid promoting their products over competitor tools

- avoid coercing users into specific continuity configurations
- maintain neutrality in multi-heir disputes
- follow DEPI governance principles

Violations may result in:

- certification revocation
- membership suspension
- reporting to regulatory bodies

9.9 Ethical Requirements for Platforms

Accredited platforms must:

- implement DEPI’s ethical rules
- provide user-first design
- avoid dark patterns
- not exploit bereaved families
- not commercialize AI personas
- not mine heirs’ emotional content
- not collect unnecessary sensitive data
- provide transparency over data lifecycle

Platforms violating these requirements lose accreditation.

9.10 Global Governance & Cultural Sensitivity

Digital inheritance occurs across cultural, religious, and legal boundaries.

Platforms must:

- respect cultural variations
- localize emotional-content handling
- support multi-jurisdictional estate processes
- provide inclusivity for non-Western inheritance norms

DEPI will maintain a Cultural Governance Appendix for regional adaptation.

SECTION 10 — REGULATORY & COMPLIANCE ALIGNMENT

10.1 Overview

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 ethics
- cross-border inheritance rules

This section provides a Regulatory Alignment Framework ensuring that DEPI compliance supports — and never contradicts — applicable laws across jurisdictions.

DEPI is technology-neutral and jurisdiction-neutral.
Compliance requires adherence to this Standard *in harmony with* governing legal authority.

10.2 Legal Hierarchy & Precedence Rules

Continuity systems must follow this hierarchy:

10.2.1 Governing Law of the Estate

Wills, trusts, and court orders supersede platform-level continuity settings.

10.2.2 Jurisdictional Probate Authority

Local laws govern:

- inheritance rights
- documentation requirements
- executor authority
- digital asset access rules

10.2.3 Statutory Digital Asset Frameworks

Platforms must follow:

- RUFADAA (U.S.)
- GDPR (EU)
- eIDAS 2.0 (EU identity)
- HIPAA (U.S. medical data)
- local data protection laws
- local succession laws

10.2.4 Platform Contracts

Terms of service must comply with DEPI and legal frameworks.

10.2.5 User Continuity Instructions

Binding unless overridden by law.

10.2.6 Technical Rules & Smart Contracts

Smart contract logic must always defer to legal authority.

10.3 U.S. Regulatory Alignment

Digital estate continuity intersects with multiple U.S. frameworks.

10.3.1 RUFADAA (Revised Uniform Fiduciary Access to Digital Assets Act)

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 authorized
- support revocation of legacy credentials

10.3.2 Federal Privacy Laws (HIPAA, GLBA, COPPA, etc.)

Platforms must:

- restrict health-related data access
- protect minor children from privacy breaches

- comply with financial data handling restrictions

10.3.3 ESIGN & UETA

Platforms supporting electronic signatures must:

- ensure records are accessible
- maintain permanent audit trails
- support long-term verification

10.3.4 Federal & State Blockchain Regulations

Platforms must:

- disclose where blockchain networks operate
- comply with KYC/AML for financial assets
- support subpoena compliance
- ensure tokenized rights reflect actual legal ownership

10.4 European Union (EU) Regulatory Alignment

10.4.1 GDPR (General Data Protection Regulation)

Key requirements:

- data minimization
- data subject rights
- lawful basis for processing
- right to rectification
- right to erasure (post-mortem requests delegated to executors)
- breach reporting within 72 hours

Platforms must support executor-driven GDPR requests post-mortem.

10.4.2 eIDAS 2.0 (Digital Identity Regulation)

Platforms must:

- support digital identity wallets
- integrate VCs (Verifiable Credentials)
- align decentralized identity systems with EU identity trust frameworks

---

10.4.3 EU Digital Markets Act & Digital Services Act

Platforms must:

- provide transparency in algorithms
- support exportability of user data
- protect users from digital manipulation
- enforce content governance for AI assets

10.5 Asia-Pacific Regulatory Alignment

The Asia-Pacific region contains rapidly evolving digital asset and AI regulations.

Platforms must align with:

- Singapore PDPA
- Australia Privacy Act
- New Zealand Privacy Framework
- Japan Digital Asset Regulations
- South Korea PIPA
- India's DPDP Act

Key requirements:

- localized data transfers
- explicit consent models
- restrictions on biometric and genetic data
- digital executor compliance

10.6 LATAM Regulatory Alignment

Countries such as Mexico, Brazil, Argentina, Chile, and Colombia have unique succession and digital privacy laws.

Platforms must support:

- civil law–based inheritance
- mandatory executor authority validation
- LGPD (Brazil) compliance for data processing
- localization of data processing where required

Blockchain usage must consider:

- tax implications
- restrictions on tokenized securities

10.7 Cross-Border Digital Estate Conflicts

Cross-border estates raise conflicts in:

- identity
- jurisdiction
- asset classification
- inheritance rights
- executor recognition
- recognition of smart contract triggers
- AI persona treatment

Platforms must implement:

10.7.1 Jurisdiction Mapping

Map assets to:

- storage location
- citizen/resident status
- corporate domicile
- blockchain node locations
- legal system of origin

10.7.2 Multi-Jurisdictional Executor Support

Executors must be verified under:

- jurisdiction of death
- jurisdiction of asset location
- jurisdiction of platform operation

10.7.3 Cross-Border Continuity Controls

Platforms must:

- prevent unlawful data export
- restrict access based on jurisdiction
- support legal disputes
- escrow continuity events when not legally permissible

10.8 Compliance Requirements for Blockchain Systems

Platforms using blockchain MUST comply with:

10.8.1 Data Protection Rules

No personal data may be stored on public chains without encryption or ZK proofs.

10.8.2 Legal Override Protocol

Smart contracts must be override-capable.

10.8.3 Geographic Jurisdiction Disclosure

Platforms must disclose:

- where nodes operate
- jurisdictional risk
- immutability implications
- regulatory regimes applicable

10.8.4 Proof-of-Authority & Permissioned Chains

If using permissioned chains:

- governance must be transparent
- participants must be vetted

- override authorities must be defined

10.8.5 Tokenized Rights Alignment

Tokenized legal rights must reflect actual legal title.

10.9 Compliance Requirements for AI Systems

Platforms using AI must comply with emerging global AI regulations including:

- EU AI Act
- OECD AI Principles
- U.S. AI safety guidance
- 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
- ensuring AI does not override legal estate instructions

10.10 Compliance Requirements for Emotional & Cognitive Assets

Platforms must:

- classify emotional assets as high-sensitivity
- protect minors from premature exposure
- ensure heirs receive only intended content
- prevent coercion through emotional manipulation
- ensure AI memories comply with inheritance restrictions

10.11 Required Documentation for Compliance

Platforms must maintain:

10.11.1 Compliance Statements

Including:

- data protection compliance
- identity workflows
- blockchain disclosure
- AI governance report
- continuity workflow documentation

10.11.2 Audit Logs

- identity events
- delegation events
- inheritance events
- AI model changes
- smart contract execution

10.11.3 Regulatory Risk Assessments

Conducted annually.

10.12 Regulator-Ready Outputs

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
- cross-border inheritance documentation

DEPI may publish a Regulator Alignment Guide as an annex.

SECTION 11 — FUTURE-STATE CONTINUITY SYSTEMS

11.1 Introduction

As humanity transitions into an era defined by:

- multimodal AI
- spatial computing
- extended reality (XR)
- 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 section provides a forward-looking framework to guide technology builders, policymakers, institutions, professionals, and families as continuity systems extend beyond the boundaries of:

- traditional inheritance
- single-generation asset transfer
- device-based digital identity
- physical-world documentation

DEPI recognizes that continuity must operate across decades, geographies, legal systems, platforms, and technologies that do not yet exist.

Section 11 ensures that DEPI remains:

- technologically neutral
- legally aligned
- ethically grounded
- globally adaptive
- future-proof

This section is non-normative but strongly recommended as guidance for emerging technologies.

11.2 Future Identity Constructs

Beyond today’s identity layers (legal, digital, cryptographic, AI), future continuity systems must anticipate additional identity modalities.

11.2.1 Neuro-Digital Identity (NDI)

Identity signals derived from:

- neural interfaces
- brain-computer interfaces
- cognitive activity models
- biometric neuro-signatures

Continuity requirements:

- NDIs must have ethical inheritance boundaries
- NDIs must not enable post-mortem impersonation
- NDIs must be frozen upon death unless explicitly permitted
- NDIs must integrate with legal identity frameworks

11.2.2 Synthetic Identity Constructs

Future identity models may include:

- AI-trained personal identity proxies
- predictive digital twins
- emotionally adaptive AI guardians
- co-evolving AI personas

Continuity requirements:

- synthetic identities must be labeled
- must not override or replace real identity instructions
- succession rules must be explicitly defined
- AI co-agents must be bound by ethical constraints

11.2.3 Distributed & Multi-Anchor Identity

As identity becomes decentralized:

- identity may exist across multiple chains and platforms
- the “self” may be represented by composite signatures
- continuity must map authority across distributed anchors

Continuity guidance:

- inheritance must unify multi-anchor identity
- executors must be able to manage distributed identity clusters
- metadata must bind identity to the user, not the system

11.3 Future Digital Asset Classes

Emerging assets require new continuity frameworks.

11.3.1 Spatial-Life Archives

High-fidelity volumetric recordings capturing:

- life events
- conversations
- experiences
- surroundings
- personal history

Continuity concerns:

- long-term rendering compatibility
- privacy of third parties captured in spatial scenes
- emotional sensitivity

11.3.2 Holographic Presence Assets

These include:

- holographic last messages
- 3D presence archives
- volumetric AI avatars

Continuity guidance:

- Must be clearly labeled as immersive assets
- Must not be used for exploitation or misrepresentation
- Must require explicit user authorization

11.3.3 Digital Twin Intellectual Property

Digital twins may contain:

- business knowledge
- trade processes
- professional expertise

Continuity considerations:

- SMB inheritance
- IP ownership
- multi-party governance

11.3.4 Cross-Platform AI Memory Clouds

Future families may inherit:

- multi-generational AI-enhanced memory clouds
- merged parental memory repositories
- cross-generational cognitive datasets

Continuity concerns:

- what is ethically inheritable
- rights to AI interpretations of personal histories
- avoidance of memory distortion

11.4 Future Continuity Triggers

Technological shifts may introduce new categories of continuity triggers.

11.4.1 Bio-Digital Triggers

Triggers initiated by:

- biometric shutdown
- neural inactivity
- medical device integration
- authenticated incapacity detection

These must always require human verification.

11.4.2 AI Predictive Triggers

AI may detect:

- cognitive decline
- health risk patterns
- continuity risks

DEPI mandates:

- AI may inform but never solely initiate inheritance
- AI-triggered warnings must require human confirmation

11.4.3 Cross-System Event Triggers

Continuous systems across devices, chains, AIs, and cloud services must coordinate inheritance events.

This requires:

- verified multi-source data
- override mechanisms
- interoperability protocols

11.5 Long-Term Preservation & Ultra-Longevity

As people live longer and as digital assets persist across centuries, continuity must anticipate:

- 100+ year archives
- AI-enhanced genealogical systems
- multi-generational digital storytelling
- enterprise continuity beyond founders

11.5.1 Ultra-Longevity Preservation Requirements

Immersive and cognitive assets must:

- remain readable for decades
- support format migration
- preserve contextual meaning
- avoid technological decay (bit rot, obsolescence)

11.5.2 Multi-Generational Continuity

Future estates may support:

- planned multi-generational releases
- heritage-based data inheritance
- lineage-specific content access

Platforms must:

- enforce ethical controls
- prevent identity misuse across generations

11.6 Future Ethics & Post-Biological Governance

Digital personhood and identity persistence beyond physical life raise profound ethical questions.

11.6.1 Post-Biological Identity Boundaries

AI or synthetic identities based on user data must:

- remain subordinate to legal estate instructions
- avoid simulating “conversations” on behalf of the deceased unless authorized
- prevent misrepresentation as living entities

11.6.2 Digital Reincarnation Prohibition (Default)

Unless explicitly enabled by the user:

- platforms must not create persistent post-mortem digital selves
- no autonomous AI evolution
- no generative simulation beyond configured boundaries

11.6.3 Ethical Stewardship of Digital Memories

Future memory technologies may recreate events visually or cognitively—platforms must prevent:

- false-history generation
- unauthorized reinterpretation
- harmful emotional manipulation
- synthetic distortion of truth

11.7 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
- standardized export formats

DEPI will publish updates as emerging technologies mature.

11.8 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
- blockchain inheritance law

Platforms should design systems expecting:

- strong consent laws
- identity authenticity requirements
- AI activity restrictions
- extended executor authority expansion

11.9 DEPI's Long-Term Commitments

DEPI commits to:

- maintaining technology-neutral standards
- updating the Standard annually
- monitoring AI, AR/VR/XR, BCI, and identity innovation
- collaborating with legislators
- educating professionals
- stewarding ethical digital legacy

Continuity is not static. As humans change, technology changes, and laws change, DEPI's duty is to guide the world responsibly into the future.

APPENDICES — DEPI DIGITAL ESTATE CONTINUITY STANDARD™ v1.0

A — Glossary

B — Asset Taxonomy

APPENDIX A — GLOSSARY

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.

Asset Category – Classification grouping defining digital assets based on purpose, sensitivity, inheritance rules, and continuity requirements.

Blockchain Anchor – A cryptographic hash representing off-chain metadata, used for provenance and audit without storing personal data on-chain.

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.

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.

Cryptographic Identity – Identity derived from cryptographic keys, signatures, MPC, multi-sig access structures, or DIDs.

Delegated Authority – Role-based permissions allowing designated individuals to access specific assets or continuity functions.

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, AI-based legacies.

Executor Authority Mapping – The process of matching legal executor authority to digital asset categories.

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.

Multi-Sig / MPC – Security schemes requiring multiple parties/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.

Smart Contract Governance – Rules for updating, overriding, or modifying smart contracts in response to legal or continuity events.

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 Section 3.

Category 1 — Financial Digital Assets

- Online bank accounts
- Brokerages & trading platforms
- Payment systems (PayPal, Stripe, Zelle)
- Crypto exchanges (centralized)
- Insurance/retirement portals
- Reward points and loyalty programs
- SMB accounting systems

Continuity: High verification, legal authority required.

Category 2 — Communication & Identity Assets

- Email accounts
- Phone numbers & SIM identity

- Messaging apps
- Social media accounts
- Contact directories
- Influencer/business identity accounts

Continuity: Executor read-limited; identity continuity required.

Category 3 — Personal Data & Cloud Storage

- Photos/videos
- Cloud drive content
- Password managers
- Documents & records
- Subscription accounts

Continuity: Granular access required.

Category 4 — Emotional Digital Assets

- Legacy letters
- Videos for children
- Voice messages including stored voice mail
- Future-dated messages
- Memory NFT artifacts
- AI-generated emotional content

Continuity: Privacy-first, staged delivery.

Category 5 — AI-Generated Cognitive Assets

- AI personas
- Autobiographical models
- AI knowledge graphs
- Predictive behavioral engines

Continuity: Freeze post-mortem unless explicitly allowed.

Category 6 — Business & 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 7 — Blockchain & Cryptographic Assets

- Crypto wallets
- On-chain tokens
- NFTs (identity or emotional)
- Smart-contract–locked assets
- Tokenized rights

Continuity: Multi-sig/MPC mandatory.

APPENDIX C — EMOTIONAL DIGITAL ASSET GUIDELINES

These rules govern sentimental digital assets that impact families and heirs.

C.1 Privacy & Sensitivity Requirements

Emotional assets must be:

- encrypted
- hidden from executors unless authorized
- released only to designated beneficiaries
- never used for marketing or AI training without consent

C.2 Staged Release Mechanisms

Emotional assets may use:

- time delays
- milestone releases (e.g., birthdays, graduations)
- segmented releases
- conditional releases

These may not be overridden by executors or platforms (except by law).

C.3 Ethical Content Guidelines

Platforms must:

- detect harmful emotional content
- warn beneficiaries before exposure
- block content containing violence or abuse (optional, configurable)

C.4 AI-Generated Emotional Assets

If AI generates messages:

- AI must not be mistaken for the deceased
- AI must not fabricate false memories
- AI must not interact beyond user-defined boundaries

AI emotional assets must be labeled as AI.

C.5 Inheritance of Emotional NFTs

Emotional NFTs must:

- store no private content on-chain
- link to encrypted off-chain assets
- provide metadata permanence
- preserve authenticity provenance for families

APPENDIX D — SMART CONTRACT TEMPLATE MODELS

These templates govern digital inheritance using blockchain.

Template 1 — Time-Locked Release Contract

Features:

- timelock expiry
- revocation mechanism
- multi-sig override
- human-in-the-loop requirement

Use Case: Messages, emotional assets.

Template 2 — Multi-Party Approval Inheritance Contract

Required approvals:

- executor
- platform continuity module
- optional beneficiary

Use Case: Financial or high-risk crypto assets.

Template 3 — Oracle-Based Death Verification Contract

Required elements:

- multi-source oracles
- redundancy
- manual override
- dispute resolution

Use Case: Automated triggering under verified death events.

Template 4 — Key Rotation & Reassignment Contract

Functions:

- key revocation
- successor key assignment
- inheritance of multi-sig roles
- continuity recovery

Use Case: Continuity of blockchain identity.

Template 5 — AI Model Continuity Contract

Tracks:

- model provenance
- freeze state
- authorized use cases
- beneficiary rights

Use Case: AI-persona and memory model inheritance.

APPENDIX E — ACCREDITATION CHECKLIST (DEPI AUDIT GUIDE)

This checklist is used during DEPI platform accreditation.

E.1 Security

- AES-256 encryption at rest
- TLS v1.2+ in transit
- Encrypted backups
- Password hashing best practices
- Zero-knowledge architecture verified

E.2 Identity

- KYC/identity verification
- robust delegate assignment
- executor verification

- recovery mechanisms

E.3 Continuity Workflows

- emergency workflow works
- post-mortem workflow works
- incapacity workflow works
- delegation mapping works
- inheritance execution complete

E.4 Data Integrity

- versioning
- audit logs
- exportable metadata
- retention rules

E.5 AI & Emotional Asset Controls

- model freezing
- ethical labeling
- sensitive content safeguards
- emotional staging

E.6 Blockchain Controls (If Applicable)

- multi-sig or MPC
- audited smart contracts
- override controls
- no PII on-chain
- oracle redundancy

E.7 Transparency & User Protection

- disclosures clear
- risks explained
- terms understandable
- consent revocation supported

E.8 Documentation Review

- internal policies
- compliance artifacts
- incident response plan
- continuity technical diagrams

Platforms must pass ALL mandatory items for accreditation.

APPENDIX F — CERTIFICATION COMPETENCY MAP

This defines the knowledge domains required for DEPI certifications (CDEP, DAC, DCP).

F.1 Foundation Knowledge

- digital asset taxonomy
- continuity principles
- identity layers
- legal frameworks (wills, trusts, probate)

F.2 Continuity Engineering

- continuity workflows
- metadata standards
- trigger management
- executor and beneficiary mapping

F.3 Security & Risk

- encryption
- access control
- key management
- incident response
- blockchain security (if applicable)

F.4 AI & Emotional Asset Governance

- ethical frameworks
- emotional asset handling
- AI persona governance

F.5 Blockchain & Smart Contracts

For DAC/DCP and advanced CDEP candidates:

- multi-sig/MPC
- smart contract logic
- oracle usage
- tokenized assets
- auditability requirements

F.6 Regulatory & Compliance

- GDPR
- RUFADAA
- eIDAS
- HIPAA
- cross-border conflicts

F.7 Professional Ethics

- conflict of interest rules
- user protection
- executor fiduciary duties
- DEPI ethical standards

APPENDIX G — RISK ASSESSMENT TEMPLATES

These templates allow platforms and professionals to evaluate continuity risk consistently.

G.1 Asset Risk Evaluation Template

Columns:

- Asset Name
- Asset Category
- Sensitivity Level
- Access Dependency
- Storage Location
- Blockchain Interaction (Y/N)
- Inheritance Priority
- Continuity Risk Score (1–5)
- Mitigation Required

G.2 Identity Risk Template

Fields:

- identity layer risks
- MFA dependencies
- device-loss risk
- key loss probability
- executor verification complexity

G.3 Continuity Workflow Risk Template

Assess:

- emergency workflow gaps
- incapacity workflow gaps
- post-mortem workflow vulnerabilities
- orphaned asset scenarios

G.4 Blockchain Risk Template

Fields:

- key management
- oracle dependencies
- smart contract immutability
- network risk
- multi-party governance
- irreversible loss potential

G.5 AI-Legacy Risk Template

Assess:

- model integrity risk
- harmful output risk
- impersonation risk
- synthetic memory distortion risk
- post-mortem misuse risk

G.6 SMB Continuity Risk Template

Fields:

- key-person dependency
- operational asset risk
- credential sprawl
- account survivorship
- vendor lock-in risk