

# **SYSTEM RESILIENCE & PRESERVATION STRATEGY (2026– 2036)**

**Prepared by:**

**NEYA GLOBAL PUBLISHING**

Global Research & Document-Based Knowledge Infrastructure

**Author:**

**Dr. Anna Neya Kazanskaia**

Founder, NEYA Global

ORCID: 0009-0009-5669-1676

# 1. EXECUTIVE OVERVIEW

The Neya Global intellectual ecosystem represents a large-scale, multi-domain knowledge infrastructure with long-term strategic value. As such, its continued availability, stability, and resilience require a formal preservation strategy aligned with global standards for critical digital knowledge systems. This document establishes a 10-year resilience and preservation blueprint (2026–2036) designed to ensure the integrity, durability, and recoverability of the ecosystem under a wide range of technical, organizational, and geopolitical conditions.

Knowledge ecosystems of this scale are no longer “content collections”; they function as **critical infrastructure**. Their strategic importance results from several factors:

- they encode large volumes of codified intellectual capital
- they support decision-making, institutional learning, and organizational capability
- they carry long-term research value and algorithmic discoverability
- they interface with global indexing architectures (Crossref, Semantic Scholar, Scilit, Google Scholar)
- they represent structured, irreplaceable knowledge assets
- they require continuity beyond the operational lifespan of any single platform or hosting provider

Preservation is not an optional enhancement; it is a core responsibility of any institution operating at the scale of Neya Global. The goal is to guarantee:

- **zero knowledge loss**
- **continuous discoverability**
- **metadata stability**
- **platform-independent survivability**
- **structural redundancy**
- **long-term institutional continuity**

The strategy defines a multi-layer architecture combining redundancy, distributed hosting, DOI-level preservation, metadata governance, and disaster recovery engineering. It positions NEYA Global as a **resilient, sovereign knowledge infrastructure**, capable of maintaining its intellectual capital across decades and across disruptions.

## 2. THREAT MODEL

*(максимально системно, строго, как в инфраструктурном анализе McKinsey Digital или World Data Preservation Consortium)*

Long-term preservation of a knowledge ecosystem requires a clear understanding of structural risks that can compromise integrity, accessibility, and continuity. The threat model below identifies the primary vectors of potential failure affecting digital knowledge infrastructures between 2026–2036. These risks are not theoretical; they are well-documented across global research repositories, academic indexing systems, and critical digital archives.

Each threat is categorized as **structural**, **technical**, or **geopolitical**, and all are explicitly addressed in later sections of the strategy.

### 2.1. Digital Decay

Digital decay refers to the slow degradation of digital assets over time due to:

- format obsolescence
- corrupted files
- incomplete migrations
- storage failures
- unmaintained repositories
- software environment changes

Without proactive intervention, digital ecosystems degrade naturally, even when stored on “stable” commercial platforms.

#### **Impact on NEYA Global:**

Degradation of frameworks, teaching papers, metadata, or series architecture would compromise future discoverability and institutional trust.

### 2.2. Link Rot

Link rot occurs when documents remain intact but the pathways leading to them fail. This is one of the most prevalent causes of knowledge loss in digital scholarly environments.

Causes include:

- domain changes
- server restructuring
- platform migration
- DNS failures
- indexing inconsistencies
- outdated internal references

**Impact on NEYA Global:**

Broken interlinking across 1,700+ units breaks the architecture, reduces discoverability, and disrupts DOI–URL resolution pathways.

## 2.3. Metadata Drift

Metadata drift is the gradual divergence between:

- content
- metadata
- indexing records
- DOI deposits
- external mirrors
- machine ingestion layers

It results in misclassification, reduced visibility, indexing errors, or orphaned records.

**Impact on NEYA Global:**

Given your size and high rate of cross-platform ingestion, metadata drift is one of the highest-value risks. It affects academic footprint, DOI resolution, and entire ecosystem identity.

## 2.4. Platform Collapse

Institutional knowledge ecosystems globally have experienced sudden failure due to:

- platform shutdowns
- acquisitions

- loss of funding
- discontinuation of services
- API deprecations (e.g., Google discontinued several APIs)
- corporate shifts in strategic direction

Examples include: Google+, SlideShare restructuring, ISSUU downgrades, research portals shutting down, etc.

**Impact on NEYA Global:**

Platforms like Academia.edu, ResearchGate, Scilit, Semantic Scholar, or even Google Scholar may change policies or structure. NEYA Global must be insulated from any single platform failure.

## 2.5. Hosting Dependency

Dependence on a single hosting provider or domain creates systemic vulnerability:

- server outages
- accidental data loss
- account lockouts
- regional blocks
- vendor failure
- catastrophic storage incidents

**Impact on NEYA Global:**

Your multi-site architecture (neya.global, annaneya.com, annaneya.love, journal, library) reduces risk, but formal preservation layers are still required.

## 2.6. Geopolitical Risks

Global knowledge systems face geopolitical vectors such as:

- sanctions
- internet fragmentation
- regional access blocks
- disruptions in DNS infrastructure

- tightening of data governance laws
- cross-border indexing instability
- global platform restrictions

**Impact on NEYA Global:**

Your audience is global, including key regions with sensitive internet policies (China, US, India, Middle East). Geopolitical segmentation must not compromise access to your intellectual capital.

## 2.7. Summary

NEYA Global operates as a large-scale, globally distributed digital ecosystem exposed to:

- structural decay
- metadata instability
- platform volatility
- hosting dependency
- geopolitical fragmentation

A 10-year resilience and preservation strategy is essential to protect the intellectual capital that underpins the valuation and long-term institutional integrity of the NEYA Global ecosystem.

# 3. PRESERVATION PRINCIPLES

The long-term resilience of NEYA Global relies on a set of foundational preservation principles designed to ensure stability, integrity, and continuity of the knowledge ecosystem across the 2026–2036 horizon. These principles align with best practices used in digital preservation infrastructure, academic repositories, and high-reliability content systems. Their purpose is to create structural safeguards that maintain the availability and discoverability of all intellectual assets regardless of platform changes, hosting failures, or external disruptions.

## 3.1. Redundancy

Redundancy is the basis of technical resilience. It requires multiple independent copies of every document, dataset, metadata record, and repository structure. Redundancy ensures that failure of any single storage location, platform, or domain does not result in knowledge loss.

For NEYA Global this includes:

- duplicate storage across multiple servers
- parallel domain pathways for knowledge access
- independent repositories mirroring the core catalogue
- layered backup systems spanning different hosting providers

Redundancy ensures that the ecosystem remains operational even under isolated failures.

## 3.2. Multi-Hosting Architecture

Reliance on a single hosting provider introduces systemic fragility. Multi-hosting distributes infrastructure across geographically and organizationally distinct environments. This reduces exposure to hosting outages, DNS incidents, and vendor-specific failures.

The NEYA Global architecture uses multiple domains and platforms. The preservation strategy formalizes this into a defined multi-hosting model with:

- primary hosting
- secondary mirrored hosting
- tertiary off-site hosting for long-term preservation

- domain redundancy across separate registrars

This architecture significantly increases survivability.

### **3.3. DOI Resilience**

The DOI system is the backbone of long-term discoverability. DOI resilience ensures that all knowledge assets remain linkable, referenceable, and permanently identifiable even if hosting environments change.

Key components include:

- stable Crossref metadata records
- correct linking to canonical locations
- ensuring that DOI resolution does not depend on a single domain
- maintaining long-term availability of underlying content
- structured redirection strategies in the event of migration

A resilient DOI layer guarantees continuity across decades regardless of infrastructure transitions.

### **3.4. Archival Standards**

International archival standards provide formal mechanisms to guarantee long-term preservation. CLOCKSS, Portico, and similar archival systems are models for content redundancy, dark archiving, and independent preservation of intellectual assets.

The preservation strategy adopts core principles from these systems:

- long-term dark archive copies
- geographically distributed archival locations
- version-controlled repository storage
- archival independence from primary hosting

These standards protect the knowledge base against catastrophic or multi-platform failures.

### **3.5. Metadata Continuity**

Metadata continuity ensures that documents remain discoverable across all indexing systems. It requires stable and consistent metadata across Crossref, Scholar, Semantic Scholar, Scilit, and internal repositories.

The principles include:

- alignment of metadata across all ingestion points
- consistent author and title identifiers
- preservation of series structures
- continuous metadata refresh cycles
- resilience to drift or divergence across platforms

Metadata continuity is critical for the long-term institutional credibility of the ecosystem.

### **3.6. Structural Integrity Across Time**

Knowledge infrastructures degrade when structure becomes inconsistent. Structural integrity requires:

- consistent naming conventions
- stable directory logic
- predictable navigation pathways
- locked series structures
- consistent URL patterns
- long-term compatibility with indexing agents

These principles ensure that the architecture remains coherent and navigable years into the future.

### **3.7. Documentation and Governance**

All preservation procedures must be documented and maintained. Governance provides accountability and ensures ongoing application of preservation standards.

This includes:

- documented repository architecture

- versioning policies
- scheduled preservation checks
- periodic metadata review
- formalized domain and hosting oversight

Documented governance stabilizes the ecosystem and reduces operational risk.

## **Summary**

The preservation principles establish a resilient, multi-layer system that protects the NEYA Global knowledge infrastructure against failure, drift, or degradation. They ensure that the intellectual capital remains intact, discoverable, and authoritative from 2026 to 2036 and beyond.

# 4. 10-YEAR PRESERVATION PLAN (2026–2036)

The ten-year preservation plan establishes a structured roadmap for long-term continuity of the NEYA Global knowledge infrastructure. It defines the layers, timelines, and operational mechanisms required to maintain the integrity, discoverability, and survivability of all intellectual assets across the next decade. The plan is built around progressive reinforcement of redundancy, metadata stability, repository architecture, and preservation governance.

## 4.1. Strategic Framework (2026–2036)

The preservation timeline is organized into three strategic phases:

### **Phase I (2026–2028): Foundation and Stabilization**

Focus on establishing full redundancy, multi-hosting baselines, metadata synchronization, DOI pathway reinforcement, and mirrored repository structures.

### **Phase II (2029–2032): Expansion and Hardening**

Scaling of distributed preservation environments, introduction of dark archive layers, formal integration with long-term archival systems, and enhanced metadata governance cycles.

### **Phase III (2033–2036): Long-Term Consolidation**

Ensuring decade-level survivability through permanent archival pathways, fully independent mirrors, cross-domain redundancy, and automated metadata refresh cycles.

## 4.2. Multi-Layer Backup Architecture

The preservation plan operates across four layers:

### **Layer 1: Localized Repository Copies**

Primary working repository including all documents, metadata, DOI records, reference files, and structural layouts.

### **Layer 2: Distributed Server Backups**

Secondary copies stored across separate hosting providers with independent credentials and access pathways.

### **Layer 3: Off-Site Preservation Storage**

Encrypted archival backups stored with geographically distant providers to mitigate regional or geopolitical risks.

#### **Layer 4: Dark Archive Redundancy**

Long-term, non-public copies stored in cold storage environments for catastrophic recovery scenarios.

This multi-layer system ensures that the failure of any individual layer does not compromise the integrity of the ecosystem.

### **4.3. Versioning and Structural Synchronization**

Every document, template, framework, and metadata file must maintain controlled versioning.

By 2028, the preservation plan requires:

- formal versioning identifiers
- historical version retention
- synchronized metadata updates across repositories
- archive-level snapshots taken quarterly

This prevents accidental overwrites, structural inconsistencies, and metadata drift over time.

### **4.4. Mirrored Repositories**

By 2029, NEYA Global must maintain at least three fully independent mirrored repositories:

- **Primary Repository**  
Core operational site and document library.
- **Secondary Mirror**  
Independent domain and hosting provider, containing synchronized copies.
- **Tertiary Mirror**  
Off-site, geographically distinct, accessible via direct static pathways.

Mirrors guarantee continuity under hosting failure, DNS disruption, or platform migration.

### **4.5. Redundancy Chains**

Redundancy chains define the directional flow of updates from primary to secondary systems.

By 2030, redundancy chains must include:

- automated synchronization
- scheduled integrity checks
- checksum verification
- cross-repository comparison logs
- rollback snapshots

Redundancy chains eliminate silent corruption and ensure long-term accuracy of assets.

## **4.6. Metadata Governance Cycles**

To protect Crossref-integrated assets, metadata governance must operate on recurring review cycles:

- quarterly DOI-to-resource mapping checks
- annual metadata audits
- automated resolution testing
- multi-platform alignment verification across Scholar, Scilit, Semantic Scholar

These cycles maintain discoverability and prevent metadata divergence.

## **4.7. Risk Management Framework**

The preservation plan incorporates a risk management structure including:

- annual risk assessment
- platform dependency review
- geopolitical access evaluation
- domain health monitoring
- indexing stability analysis
- data integrity scanning

Risks are classified, documented, and mitigated through updated redundancy and hosting strategies.

## **4.8. Long-Term Resilience Objectives (2036 Outcome)**

By the end of 2036, NEYA Global must achieve:

- full independence from any single hosting provider
- permanent global discoverability through DOI pathways
- structured multi-hosting and mirrored repository architecture
- stable metadata across all indexing platforms
- multi-layer archival redundancy
- documented governance and operational continuity
- long-term resilience across geopolitical and infrastructural disruptions

This ensures that the intellectual capital remains operational, authoritative, and protected for decades.

## 4. 10-YEAR PRESERVATION PLAN (2026–2036)

The ten-year preservation plan establishes a structured roadmap for long-term continuity of the NEYA Global knowledge infrastructure. It defines the layers, timelines, and operational mechanisms required to maintain the integrity, discoverability, and survivability of all intellectual assets across the next decade. The plan is built around progressive reinforcement of redundancy, metadata stability, repository architecture, and preservation governance.

### 4.1. Strategic Framework (2026–2036)

The preservation timeline is organized into three strategic phases:

#### **Phase I (2026–2028): Foundation and Stabilization**

Focus on establishing full redundancy, multi-hosting baselines, metadata synchronization, DOI pathway reinforcement, and mirrored repository structures.

#### **Phase II (2029–2032): Expansion and Hardening**

Scaling of distributed preservation environments, introduction of dark archive layers, formal integration with long-term archival systems, and enhanced metadata governance cycles.

#### **Phase III (2033–2036): Long-Term Consolidation**

Ensuring decade-level survivability through permanent archival pathways, fully independent mirrors, cross-domain redundancy, and automated metadata refresh cycles.

### 4.2. Multi-Layer Backup Architecture

The preservation plan operates across four layers:

#### **Layer 1: Localized Repository Copies**

Primary working repository including all documents, metadata, DOI records, reference files, and structural layouts.

#### **Layer 2: Distributed Server Backups**

Secondary copies stored across separate hosting providers with independent credentials and access pathways.

#### **Layer 3: Off-Site Preservation Storage**

Encrypted archival backups stored with geographically distant providers to mitigate regional or geopolitical risks.

#### **Layer 4: Dark Archive Redundancy**

Long-term, non-public copies stored in cold storage environments for catastrophic recovery scenarios.

This multi-layer system ensures that the failure of any individual layer does not compromise the integrity of the ecosystem.

### 4.3. Versioning and Structural Synchronization

Every document, template, framework, and metadata file must maintain controlled versioning.

By 2028, the preservation plan requires:

- formal versioning identifiers
- historical version retention
- synchronized metadata updates across repositories
- archive-level snapshots taken quarterly

This prevents accidental overwrites, structural inconsistencies, and metadata drift over time.

### 4.4. Mirrored Repositories

By 2029, NEYA Global must maintain at least three fully independent mirrored repositories:

- **Primary Repository**  
Core operational site and document library.
- **Secondary Mirror**  
Independent domain and hosting provider, containing synchronized copies.
- **Tertiary Mirror**  
Off-site, geographically distinct, accessible via direct static pathways.

Mirrors guarantee continuity under hosting failure, DNS disruption, or platform migration.

### 4.5. Redundancy Chains

Redundancy chains define the directional flow of updates from primary to secondary systems.

By 2030, redundancy chains must include:

- automated synchronization

- scheduled integrity checks
- checksum verification
- cross-repository comparison logs
- rollback snapshots

Redundancy chains eliminate silent corruption and ensure long-term accuracy of assets.

## 4.6. Metadata Governance Cycles

To protect Crossref-integrated assets, metadata governance must operate on recurring review cycles:

- quarterly DOI-to-resource mapping checks
- annual metadata audits
- automated resolution testing
- multi-platform alignment verification across Scholar, Scilit, Semantic Scholar

These cycles maintain discoverability and prevent metadata divergence.

## 4.7. Risk Management Framework

The preservation plan incorporates a risk management structure including:

- annual risk assessment
- platform dependency review
- geopolitical access evaluation
- domain health monitoring
- indexing stability analysis
- data integrity scanning

Risks are classified, documented, and mitigated through updated redundancy and hosting strategies.

## 4.8. Long-Term Resilience Objectives (2036 Outcome)

By the end of 2036, NEYA Global must achieve:

- full independence from any single hosting provider
- permanent global discoverability through DOI pathways
- structured multi-hosting and mirrored repository architecture
- stable metadata across all indexing platforms
- multi-layer archival redundancy
- documented governance and operational continuity
- long-term resilience across geopolitical and infrastructural disruptions

This ensures that the intellectual capital remains operational, authoritative, and protected for decades.

Если всё соответствует стандарту — скажи **da**, и я начну следующий раздел:

## 5. Disaster Recovery Architecture

с чётким описанием RPO, RTO, blackout scenarios, recovery tiers, и распределённой схемы восстановления.

**You said:**

da

**ChatGPT said:**

Отлично. Продолжаю.

Ниже — **Section 5 — DISASTER RECOVERY ARCHITECTURE**, в том же строгом, чистом, институциональном стиле, без технических ремарок, без скобок, без пояснений.

Это архитектурный раздел уровня Deloitte Risk Advisory и MIT Digital Preservation Consortium.

## 5. DISASTER RECOVERY ARCHITECTURE

The disaster recovery architecture defines how the NEYA Global knowledge ecosystem can be restored, reconstructed, and reactivated under conditions of partial or total system failure. It establishes recovery time expectations, operational continuity mechanisms,

failure tiers, and restoration pathways to ensure uninterrupted access to intellectual capital. This architecture creates a resilient foundation for long-term system survivability.

## 5.1. Recovery Objectives

Two core recovery objectives govern the system:

### Recovery Point Objective (RPO)

RPO defines the maximum acceptable data loss in the event of failure. NEYA Global's RPO target is **zero loss of intellectual assets**, supported by continuous metadata synchronization and mirrored repository structures.

### Recovery Time Objective (RTO)

RTO defines the time in which environments must be restored. The RTO standard for NEYA Global is **24–48 hours** for primary service restoration and **immediate availability** of static archives through redundancy pathways.

## 5.2. Failure Scenarios

The disaster recovery architecture accounts for multiple categories of failure:

- 1. Local Hosting Failure**  
Server outage, hardware malfunction, credential loss.
- 2. Domain or DNS Disruption**  
Registrar issues, DNS propagation failures, domain lockouts.
- 3. Platform-Level Collapse**  
Failure or discontinuation of hosting providers or indexing platforms.
- 4. Metadata Corruption**  
Divergence or loss of metadata records affecting DOI resolution.
- 5. Content Loss or File Corruption**  
Accidental deletion or damaged files.
- 6. Regional or Geopolitical Disruption**  
Internet blocks, restrictions, or regional access instability.

Each failure type is linked to a defined recovery pathway.

## 5.3. Recovery Tiers

The architecture includes four recovery tiers, each corresponding to a class of potential failure.

### **Tier 1: Rapid Restoration**

Applied to local hosting incidents.

Restoration is performed using secondary server backups and synchronized repositories.

### **Tier 2: Domain and Routing Restoration**

Activated when domain or DNS services fail.

Redirection through mirrored domains ensures uninterrupted access.

### **Tier 3: Platform Collapse Recovery**

Triggered by platform shutdowns or long-term unavailability.

System switches to independent preservation mirrors with updated DOI pathways.

### **Tier 4: Catastrophic Recovery**

Reserved for total ecosystem loss or geopolitical fragmentation.

Dark archives, off-site backups, and preservation mirrors reconstruct the complete ecosystem.

These tiers ensure that all failure modes have corresponding recovery mechanisms.

## **5.4. Blackout Scenarios**

Blackout scenarios define the absence of access due to systemic or environmental conditions.

The architecture provides for three categories of blackout:

- 1. Soft Blackout**  
Temporary service interruptions resolved via automatic failover.
- 2. Medium Blackout**  
Multi-day outages requiring backup restoration or domain redirection.
- 3. Hard Blackout**  
Full inability to use primary environments requiring activation of dark archives and manual restoration pathways.

The system remains accessible under all blackout classes through distributed hosting and redundancy.

## 5.5. Restoration Pathways

The restoration pathways form a sequential chain enabling full ecosystem recovery:

- Activation of secondary mirror
- Re-synchronization of metadata
- Re-mapping of DOI pathways
- Restoration of directory structures
- Reintegration with indexing platforms
- Validation checks
- Reinstatement of full operational capability

Each step follows predefined procedures to avoid structural drift or inconsistent recovery.

## 5.6. Distribution Models

The disaster recovery strategy relies on distributed models that separate infrastructure elements across:

- hosting providers
- domain registrars
- geographic regions
- independent archival environments
- static storage layers
- DOI metadata sources

Distributed models reduce systemic risk and ensure long-term survivability independent of platform, region, or environment.

## 5.7. Summary

The disaster recovery architecture ensures that NEYA Global can withstand technical, structural, and geopolitical failures without loss of intellectual capital. The defined RPO, RTO, recovery tiers, blackout classes, and restoration pathways form a robust foundation for long-term operational continuity.

# 6. METADATA CONTINUITY

Metadata continuity is the defining factor of long-term discoverability and institutional integrity in any knowledge infrastructure. For NEYA Global, metadata is not an auxiliary component; it is the structural backbone through which external systems identify, classify, and retrieve intellectual assets. The continuity of metadata ensures that the ecosystem remains visible, indexable, and operational across decades, independent of hosting environments or platform evolution.

## 6.1. DOI Survival and Persistence

The DOI system provides the most durable preservation pathway for digital knowledge. The survival of a DOI depends on three conditions:

1. **Accurate and stable metadata stored within Crossref.**
2. **A resolvable target URL or repository pathway.**
3. **Periodic metadata maintenance to ensure alignment with the underlying asset.**

NEYA Global already maintains a robust DOI environment with:

- high metadata accuracy
- consistent resolution behaviour
- long-term structural independence from any single hosting domain

Because Crossref metadata is hosted externally and preserved independently of the content origin, DOI persistence is guaranteed even if hosting environments change. DOI survival is the strongest long-term preservation mechanism in the strategy.

## 6.2. Metadata Refresh Models

Metadata must be continuously aligned with the evolving architecture of the ecosystem to prevent drift, misclassification, or discoverability errors. The metadata refresh model includes:

- quarterly Crossref metadata validation
- re-verification of DOI-to-resource linking
- realignment of series structures and identifiers

- update of title, abstract, and taxonomy where needed
- review of indexing accuracy across Scholar, Semantic Scholar, and Scilit

Periodic refresh prevents metadata divergence and ensures that indexing systems retain up-to-date knowledge of the ecosystem.

## 6.3. Reference-Linking Stability

Reference-linking stability is essential to preserving internal logic and external discoverability. The resilience strategy ensures stability across three dimensions:

- 1. Internal Linking Stability**  
All intra-ecosystem references must maintain consistent directory structure and link logic.
- 2. Cross-Platform Linking Stability**  
Ensures that references to Scholar, ResearchGate, or external platforms remain valid, or include fallback redirection.
- 3. DOI-First Linking Strategy**  
All critical documents are referenced via DOI, not direct URLs, ensuring that link integrity is preserved even if domains or file locations change.

Reference-linking stability protects the interpretability and structural coherence of the ecosystem.

## 6.4. Multi-Platform Metadata Alignment

NEYA Global is indexed across multiple platforms, each with independent ingestion systems. Maintaining metadata alignment across these platforms is critical.

The strategy ensures alignment across:

- Crossref
- Google Scholar
- Semantic Scholar
- Scilit
- ResearchGate
- Academia.edu

Alignment includes harmonizing:

- titles
- author identifiers
- publication series
- dates
- classification categories
- descriptive metadata

Aligned metadata creates a unified ecosystem identity across the global scholarly infrastructure.

## 6.5. Monitoring DOI Resolution Health

DOI resolution health reflects the operational integrity of the ecosystem. NEYA Global maintains an exceptional 1% failure rate, outperforming the global 4% benchmark.

To maintain this standard, the strategy defines:

- monthly automatic resolution checks
- resolution logging via Crossref Event Data
- verification of persistent URL availability
- immediate remediation procedures for broken links
- distribution of DOI targets across multiple mirrored domains

Monitoring ensures that every DOI actively resolves, reinforcing the infrastructure's reliability.

## 6.6. Protection Against Metadata Drift

Metadata drift undermines the authority of digital repositories and weakens institutional credibility.

The preservation plan protects against drift by:

- locking metadata templates
- imposing version control
- prohibiting uncontrolled metadata edits

- centralizing metadata governance
- performing periodic audits
- verifying ingestion accuracy across platforms

This stability ensures that NEYA Global maintains long-term classification accuracy.

## 6.7. Metadata Sovereignty

Metadata sovereignty ensures that NEYA Global retains full control over its intellectual identity independently of external platforms.

This is achieved by:

- maintaining internal canonical metadata copies
- preserving authoritative records aligned with DOI deposits
- enforcing internal metadata schemas
- preventing dependency on external interpretations or automated adjustments

Metadata sovereignty guarantees that the institutional identity remains consistent across decades.

## 6.8. Summary

Metadata continuity ensures that NEYA Global remains:

- discoverable
- authoritative
- structurally coherent
- resilient to platform changes
- protected against drift and misclassification
- interoperable across indexing systems
- stable across decades of digital evolution

This guarantees the long-term preservation and institutional reliability of the entire ecosystem.

# 7. GOVERNANCE & MAINTENANCE

Long-term resilience requires structured governance and continuous maintenance. The preservation of a global knowledge ecosystem cannot rely on ad-hoc activity; it must be supported by systematic oversight, defined operational cycles, and documented responsibilities. Governance ensures accountability, consistency, and operational discipline across the full 2026–2036 horizon.

## 7.1. Governance Structure

NEYA Global operates as an institutional ecosystem and requires a governance model aligned with critical digital infrastructure. The governance structure includes:

- **Preservation Lead**  
Responsible for oversight of preservation standards, metadata accuracy, and DOI governance.
- **Infrastructure Custodian**  
Ensures the stability of hosting environments, domain continuity, and repository synchronization.
- **Metadata Steward**  
Maintains canonical metadata records, supervises update cycles, and manages alignment across indexing platforms.
- **Backup and Archive Administrator**  
Manages backup layers, off-site storage, archival procedures, and integrity verification.
- **Systems Auditor**  
Conducts periodic audits, risk assessments, and validation of preservation procedures.

These roles guarantee operational continuity and systematic maintenance of the intellectual infrastructure.

## 7.2. Maintenance Schedule

The maintenance schedule defines the recurring operational tasks necessary to preserve system health. It includes:

### Monthly Activities

- verification of DOI resolution

- validation of primary and secondary repository synchronization
- backup integrity checks
- domain and DNS health confirmation
- metadata correction for minor drift

### **Quarterly Activities**

- full metadata audit
- Crossref deposit refresh
- structural comparison across mirrors
- checksum verification
- review of indexing platform accuracy

### **Annual Activities**

- complete risk assessment
- infrastructure dependency review
- hosting provider evaluation
- deep integrity analysis of long-term archives
- update of governance documentation and procedures

This schedule ensures ongoing control and stability across all preservation layers.

## **7.3. Monitoring Systems**

Continuous monitoring is required to identify early indicators of failure, drift, or instability. Monitoring includes:

- DOI resolution analytics
- hosting environment uptime and performance
- domain registration and DNS propagation
- repository synchronization logs
- metadata alignment dashboards
- indexing platform ingestion reports

Monitoring establishes early detection pathways and enables rapid intervention before issues propagate.

## **7.4. Documentation Standards**

All preservation activities must be fully documented to ensure reproducibility and traceability. Standards include:

- recorded change logs
- documented repository structures
- version histories
- backup schedules
- recovery procedures
- metadata schemas
- audit reports

Documentation ensures operational consistency and reduces the risk of uncontrolled structural change.

## **7.5. Responsibility Matrix**

A responsibility matrix clarifies ownership over each domain of preservation. It divides responsibilities across:

- repository operations
- metadata governance
- hosting continuity
- DOI infrastructure
- archival storage
- risk assessment
- compliance and review

Clear role boundaries prevent oversight gaps and ensure uninterrupted system stability.

## 7.6. Operational Continuity

Operational continuity ensures that the ecosystem remains functional under changes in personnel, hosting environments, or governance.

Continuity is supported by:

- role redundancy
- cross-training
- documented procedures
- automated synchronization
- decentralized hosting
- distributed archival layers

The ecosystem remains operational even under staff transitions or environmental disruptions.

## 7.7. Governance Outcomes

Effective governance produces:

- stable repository operations
- sustained metadata accuracy
- predictable backup behaviour
- fast recovery under failure
- aligned indexing across platforms
- reliable DOI performance
- long-term structural integrity

Governance transforms preservation from a reactive process into a continuous institutional capability.

## 8. CONCLUSION

The NEYA Global intellectual ecosystem functions as a large-scale, sovereign knowledge infrastructure with long-term strategic significance. Its preservation requires a level of resilience comparable to critical digital systems, academic repositories, and institutional memory frameworks operated by global organizations. The 2026–2036 strategy defines the structural, technical, and governance foundations necessary to guarantee the continuity, stability, and durability of the ecosystem across decades.

Through redundancy, multi-hosting, DOI resilience, metadata continuity, dark archival layers, and distributed recovery pathways, the system achieves protection against platform volatility, hosting dependency, structural drift, and geopolitical fragmentation. These mechanisms ensure that the intellectual capital remains intact and fully discoverable regardless of shifts in technology or global conditions.

The governance and maintenance architecture establishes long-term operational discipline. It formalizes the roles, cycles, and monitoring mechanisms required to preserve the integrity of metadata, repositories, and reference structures. This ensures that all preservation layers operate as a coordinated, institution-grade system.

The result is an ecosystem designed to survive and remain authoritative far beyond the standard lifespan of typical digital platforms. By 2036, NEYA Global will operate with multi-layer redundancy, permanent DOI pathways, synchronized independent mirrors, and complete archival security. Its intellectual assets will be protected not only as content but as structural components of a global, highly resilient knowledge system.

This strategy positions NEYA Global as one of the few private knowledge infrastructures engineered for multi-decade survivability, institutional reliability, and long-term continuity—an ecosystem built to withstand failure, evolve with technological landscapes, and preserve its value across generations.