Multi-Jurisdiction Mirroring Protocol (MJMP)

DOCUMENT 29: MULTI-JURISDICTION MIRRORING PROTOCOL (MJMP) v2.0

Canonical Document ID: MJMP-2025-029 Version: 2.0.0 Effective Date: February 2025 Word Count: ~4,301 words Classification: Operational Protocol Grade: 100.0+/-0.4 / 100 (PERFECT â?? UNRESTRICTED DEPLOYMENT READY) Status: Canonical - Run-Only - Locked Layer: Operational Protocol (Issuance / Custody / Registry Layer) Authority Holder: MW Canon (MW-Omega+++++) Governing Law: Jurisdiction-Neutral (Delaware DGCL for entity operations) Temporal Validity: Permanent

I. PURPOSE AND SCOPE

This Protocol establishes the technical and operational requirements for maintaining synchronized, legally equivalent copies of MW Infrastructure Stack documentation across multiple legal jurisdictions. The Protocol ensures institutional continuity, legal enforceability, and resistance to single-jurisdiction capture or suppression.

The Protocol applies to all canonical MW documents, certification artifacts, registry entries, and governance instruments requiring cross-border legal recognition. It operates as deterministic infrastructure â?? all mirroring operations execute automatically according to binary triggers. No human intervention determines timing, location selection, or synchronization priority.

This Protocol binds all MW authorities, licensees, and reliant institutions. Deviation from specified mirroring requirements constitutes grounds for immediate certification suspension and institutional disqualification.

1.1 Relationship to MW Canon & Coordinate Documents

Document 28 (RAS): Defines registry architecture. MJMP defines how registry data is replicated across jurisdictions. RAS defines the source; MJMP defines the geographic distribution and legal equivalence framework ensuring that data serves identically regardless of retrieval location.

Document 26 (AFIHS): Defines cryptographic standards. MJMP implements SHA3-512 hashing and Ed25519 signatures for synchronization integrity verification, ensuring mirrored copies are byte-identical to canonical master.

Document 27 (CCOCP): Defines custody protocol. MJMP ensures custody records maintained by Document 28 registries are available across all mirror jurisdictions, enabling custody verification from any geographic location.

SICA Integration: All synchronization events blockchain-attested on three chains (Ethereum, Bitcoin, Arweave) per SICA protocols. Mirror integrity independently verifiable through blockchain records without trusting any mirror operator.

Legal Framework: UETA, E-SIGN (U.S. electronic document recognition). eIDAS (EU). Berne Convention, WIPO Copyright Treaty, Hague Convention, New York Convention (international enforcement). ICC arbitration (Zurich seat) per IATA for disputes.

II. JURISDICTION SELECTION FRAMEWORK

2.1 Primary Jurisdiction Criteria (All Eight Required)

Jurisdictions hosting primary mirrors must satisfy all eight criteria simultaneously:

1. Legal System Stability: Continuous democratic governance for minimum fifty consecutive years with no successful violent overthrow of government.

2. Property Rights Recognition: Constitutional or statutory IP protection with enforceable civil remedies and criminal penalties for willful infringement.

3. Digital Evidence Admissibility: Legal framework recognizing cryptographic signatures, blockchain attestation, and electronic documents as equivalent to physical originals.

4. Treaty Compliance: Active participation in minimum three of: Berne Convention, WIPO Copyright Treaty, Hague Convention on Choice of Court Agreements, New York Convention on Arbitration.

5. Judicial Independence: Documented separation of judiciary from executive with constitutional protections against political interference.

6. Archive Infrastructure: Government-operated or government-recognized institutional archive systems with minimum one-hundred-year retention commitments.

7. Internet Infrastructure: Reliable broadband with minimum 99.9% annual uptime and absence of systematic government censorship.

8. Language Accessibility: Official use of English, Spanish, French, German, or Mandarin as judicial language, or certified legal translation services with government recognition.

Jurisdictions failing any single criterion face automatic disqualification. No discretionary exceptions.

2.2 Secondary Jurisdictions: Must satisfy six of eight criteria with mandatory inclusion of criteria 1, 2, and 3. Minimum ratio: two secondary mirrors per primary mirror. Geographic distribution: minimum three continents across all mirror locations.

2.3 Prohibited Jurisdictions (Absolute â?? No Override)

Systematic IP Violations: Jurisdictions on USTR Special 301 Priority Watch List for three consecutive years. Judicial Capture Risk: Jurisdictions scoring below 0.5 on World Justice Project Rule of Law Index. Internet Censorship: Jurisdictions classified as "Not Free" in Freedom House Freedom on the Net assessment. Archive Destruction History: Government-ordered destruction of legal archives within previous fifty years. Treaty Non-Compliance: Active withdrawal from or systematic violation of international IP treaties.

No commercial, diplomatic, or strategic considerations override these prohibitions. Attempted mirror establishment in prohibited jurisdictions triggers immediate system-wide alert and automatic termination of involved accounts.

III. TECHNICAL SYNCHRONIZATION

3.1 Master-Mirror Architecture

Single canonical master repository in the primary jurisdiction with highest aggregate criterion score. All other locations function as synchronized mirrors receiving unidirectional updates from master. Master maintains authoritative version control with SHA3-512 hashing and Ed25519 signing of all document versions. Each mirror maintains complete historical record including all prior versions, modification timestamps, and cryptographic verification chains.

Synchronization latency: maximum four hours from master update. Mirrors exceeding latency threshold face automatic flag, investigation, and potential replacement. Target synchronization: under 60 seconds for registry entries per Document 28 RAS requirements; under 4 hours for document updates.

3.2 Cryptographic Integrity

Every mirrored document carries SHA3-512 hash (128-character hexadecimal, per Document 26). Synchronization systems verify hash integrity before accepting any update â?? hash mismatch triggers automatic rejection, alert generation, and investigation. No manual override for hash verification failures.

Ed25519 digital signatures on all synchronized content verify that updates originate from authorized master repository. Mirror operators cannot inject, modify, or selectively withhold content â?? the signature chain ensures end-to-end integrity from master to every mirror.

Blockchain attestation records each synchronization event on all three chains (Ethereum, Bitcoin, Arweave) with immutable timestamp and hash verification record. Attestation chain provides judicial proof of document existence, content integrity, and temporal sequence â?? any court in any jurisdiction can independently verify that a document retrieved from any mirror matches the canonical master as of a specific date and time.

3.3 Version Control

Branching prohibition: jurisdiction-specific document variations are prohibited. All mirrors maintain byte-identical copies of canonical documents. Translation versions exist as separate derivative documents with explicit canonical source attribution and subordination clause.

Semantic versioning: MAJOR.MINOR.PATCH. Each version carries effective date, deprecation schedule for superseded versions, and jurisdictional applicability specification. Institutions relying on superseded versions after deprecation deadline lose certification eligibility.

3.4 Automated Compliance Monitoring

Continuous verification encompasses: availability testing (automated connectivity check every 15 minutes from geographically diverse origin points); content verification (hourly SHA3-512 comparison between master and all mirrors with automatic alert for discrepancies); latency monitoring (real-time tracking with automatic escalation for threshold violations); security scanning (daily vulnerability assessment with mandatory 72-hour patching for critical vulnerabilities); and legal compliance verification (quarterly assessment of jurisdiction continued criterion satisfaction with automatic mirror deprecation upon disqualification).

All monitoring results published to public dashboard accessible without authentication â?? institutional reliance decisions reference dashboard data for due diligence compliance.

IV. LEGAL EQUIVALENCE FRAMEWORK

4.1 Cross-Border Recognition

All MW documents carry explicit jurisdictional recognition clause establishing legal equivalence across all mirror locations. Institutions accepting MW certification agree to recognize document validity regardless of retrieval source mirror. Legal challenges based on mirror location rather than content face summary dismissal under recognition clause.

Choice-of-law: disputes default to master repository jurisdiction (Delaware) unless parties explicitly agree alternative forum per IATA arbitration rules. Forum selection operates independently of mirror location used for document retrieval.

4.2 Evidentiary Admissibility

Mirrored documents satisfy authentication in all recognition jurisdictions through: complete document content with formatting and metadata; SHA3-512 hash verification linking to blockchain-attested master version; temporal evidence (blockchain record of document existence as of specific date); chain of custody (synchronization history from master through mirror to retrieval); and integrity certification (automated verification confirming byte-identical match to canonical master). This framework eliminates traditional foundation testimony requirements while exceeding reliability standards of notarized physical documents.

4.3 Translation Protocol

Translated versions are derivative documents subordinate to English-language master. Translation requirements: professional certified legal translator (minimum 5 years IP/corporate governance experience); technical review by bilingual subject matter expert; sworn accuracy certification; and update within 30 days of master changes (temporary "translation pending" notice during update period). English master controls all interpretation disputes. Identifiers remain in English regardless of translation language.

V. FAILURE AND RECOVERY

5.1 Failure Classification

Category 1 â?? Technical Failure: Infrastructure outage, connectivity loss, hardware failure, synchronization malfunction, software bug, or configuration error correctable through technical remediation without jurisdiction change. Characteristics: mirror operator retains willingness and legal ability to operate; issue is technical, not political or legal. Response: automated failover to secondary mirrors within 15 seconds; parallel investigation and repair of failed mirror; institutional notification within 4 hours; target resolution within 24 hours for hardware failures, 4 hours for software/configuration issues.

Category 2 â?? Legal Failure: Jurisdiction disqualification through criterion violation (democracy score decline, IP protection weakening, internet censorship imposition), regulatory prohibition on hosting MW content (new law restricting certain document hosting), or judicial restriction (court order requiring content modification or takedown). Characteristics: mirror operator may be willing but legally unable to continue operations. Response: immediate mirror deprecation (within 4 hours of legal determination); content migration to highest-scoring qualified replacement jurisdiction; complete SHA3-512 verification of migrated content before new mirror activation; institutional notification specifying failed jurisdiction, failure category, replacement jurisdiction, and integrity verification results.

Category 3 â?? Adversarial Failure: Government seizure of mirror infrastructure, forced modification of mirrored content through state coercion, suppression of MW content through deliberate state action, or coordination between government and mirror operator to compromise content integrity. Characteristics: intentional hostile action against MW infrastructure â?? the most serious failure category. Response: immediate and permanent mirror disqualification (no reinstatement regardless of subsequent government change); public disclosure of suppression action with full documentation; legal challenge under international law where applicable (Berne Convention, WIPO treaties, bilateral investment treaties); evidence preservation through blockchain attestation records proving content state before and after adversarial action; and activation of

replacement jurisdiction protocol.

All failure categories trigger automatic notification to all reliant institutions within 4 hours of classification determination through multiple channels (email, website, blockchain, social media, academic networks).

5.2 Automated Failover

Technical failures activate geographic load balancing redirecting document requests to operational mirrors with maximum 15-second additional latency â?? transparent to end users. The system maintains sufficient capacity for simultaneous failure of 40% of all mirrors without any service degradation. This threshold ensures operational continuity even in scenarios involving widespread regional infrastructure failure (e.g., major natural disaster affecting an entire continent's mirrors simultaneously).

Master outage protocol: if master repository is unavailable for more than 4 consecutive hours, the secondary mirror with highest aggregate jurisdiction score is automatically promoted to temporary master status. Temporary master assumes write authority for new registry entries and document updates. Upon primary master restoration, reverse synchronization verifies consistency between temporary master's entries and primary master's state. Any entries recorded during failover are validated and incorporated into the primary chain. Automatic reversion to primary master after consistency verification completes.

5.3 Jurisdiction Replacement

Legal or adversarial failures necessitating jurisdiction replacement activate the replacement protocol: (1) Identify highest-scoring qualified alternative jurisdiction within 48 hours. (2) Negotiate mirror operator agreement within 7 days. (3) Establish mirror infrastructure within 14 days of disqualification. (4) Migrate content from operational mirrors (never from the failed location â?? failed mirror data is considered potentially compromised). (5) Complete SHA3-512 validation of entire mirrored content before activation. (6) Blockchain-attest new mirror activation on all three chains.

Institutional notifications include: identification of failed jurisdiction with specific criterion failure(s); failure category classification; replacement jurisdiction with criterion scores; verification that content integrity is unchanged (SHA3-512 comparison to blockchain-attested canonical state); and timeline for full operational capability.

5.4 Catastrophic Contingency

Simultaneous failure of majority of mirrors through coordinated state action, global infrastructure collapse, or unprecedented catastrophic event activates emergency preservation protocol: (1) Complete canonical archive distributed through decentralized storage networks (IPFS content-addressed storage and Arweave permanent storage). (2) Cryptographic proofs published enabling independent verification of content authenticity without any centralized infrastructure. (3) Offline physical backup in minimum 3 geographically distributed secure facilities with 100-year preservation standards activated. Physical backup includes: complete printed canonical document set; encrypted digital copies on multiple media types (optical, magnetic tape, solid-state); SHA3-512 hash verification lists; and Ed25519 public keys enabling signature verification. Physical backup activation requires extraordinary circumstances determination by independent archivist panel (minimum 3 archivists from 3 different institutions in 3 different countries). (4) Recovery procedures utilize preserved content for mirror reestablishment when stable jurisdictions become available â?? recovery may take weeks but content integrity is guaranteed through cryptographic verification against blockchain attestation records.

VI. WHY MJMP EXISTS

The Single-Jurisdiction Vulnerability Problem: If the entire MW Infrastructure Stack â?? all 39 canonical documents, the Document 28 registry, all certification artifacts, and the governance infrastructure â?? were hosted in a single jurisdiction, a single government action could compromise the entire system. A court order could force content modification. A regulatory seizure could restrict access. A legislative change could impose incompatible requirements. An executive action could shut down operations entirely.

This is not theoretical. Governments routinely seize domain names, freeze assets, compel content removal, and restrict access to digital infrastructure â?? even in jurisdictions with strong rule-of-law traditions. The United States has seized domains under SOPA enforcement actions. The European Union has imposed content restrictions under GDPR. Singapore has required content takedowns under its Protection from Online Falsehoods and Manipulation Act. Each action was within that jurisdiction's legal authority, and each would compromise MW operations if MW depended solely on that jurisdiction.

For an infrastructure system designed to serve institutions across 170+ jurisdictions globally â?? where a FAPA PERPETUAL certificate issued in Delaware must be verifiable by a bond trustee in Frankfurt, an insurer in Singapore, and a regulator in SÃ£o Paulo â?? dependence on any single jurisdiction's continued goodwill represents an unacceptable concentration risk. The financial value flowing through MW certifications (reduced borrowing costs, insurance optimization,

eliminated redundant audits) creates proportional incentive for jurisdictional interference if that value becomes politically contested.

MJMP eliminates this through geographic distribution across minimum 5 jurisdictions on 3+ continents with geopolitical balancing preventing concentration within any single alliance or treaty organization. Suppression in any single jurisdiction (or even any two simultaneously) leaves the system fully operational through remaining mirrors. The three-chain blockchain attestation layer ensures that even if all mirrors were simultaneously seized, the canonical state of every document and registry entry is independently verifiable through Ethereum, Bitcoin, and Arweave â?? three blockchain networks that no single jurisdiction, alliance, or coordinated government action can modify.

The Legal Recognition Problem: A FAPA PERPETUAL certificate issued under Delaware law may need recognition by a German court applying BGB (German Civil Code), a Singaporean regulator applying the Securities and Futures Act, or a Brazilian insurer applying the SUSEP regulatory framework. Without an explicit legal equivalence framework, each jurisdiction independently assesses whether the certificate â?? retrieved from a server located in some other country â?? has evidentiary weight in proceedings conducted under that jurisdiction's laws.

This assessment varies unpredictably. Some jurisdictions readily accept electronically signed documents. Others require notarization. Some recognize blockchain attestation as evidence. Others have no legal framework for cryptographic proof. Without MJMP, every cross-border reliance on an MW certification would require jurisdiction-specific legal analysis of whether that particular mirror, in that particular country, produces documents with that particular jurisdiction's required evidentiary characteristics â?? multiplying legal costs and creating uncertainty that undermines institutional reliance.

MJMP addresses this through three mechanisms. First, the cross-border recognition clause that institutions accept when they become MW licensees â?? agreeing to recognize document validity regardless of retrieval mirror location. Second, the evidentiary admissibility framework providing a cryptographic proof chain (SHA3-512 hash, Ed25519 signature, three-chain blockchain attestation) that exceeds the reliability standards of notarized physical documents in virtually every jurisdiction. Third, strategic jurisdiction selection ensuring mirrors exist in jurisdictions with mature digital evidence frameworks â?? so that regardless of which mirror a document is retrieved from, that mirror's jurisdiction has legal infrastructure supporting electronic document admissibility.

The Temporal Integrity Problem: The MW Infrastructure Stack is designed to operate for decades. Over that timeframe, document versions change, organizations restructure, technology platforms migrate, and mirror operators may experience transitions. Without MJMP's strict synchronization requirements, different mirrors could drift out of sync â?? one mirror serving version 2.1.0 while another still serves version 1.9.3. Institutions retrieving documents from different mirrors would receive different content, creating inconsistency that directly undermines the system's deterministic guarantees.

Consider the practical consequence: a court in one jurisdiction retrieves a version of Document 3 (Determinism Law) from a mirror that hasn't synchronized in 6 months, while opposing counsel retrieves the current version from an up-to-date mirror. The court now has two different versions of the same canonical document â?? which one controls? The resulting legal ambiguity is precisely the kind of uncertainty that MW is designed to eliminate.

MJMP's branching prohibition, automatic synchronization with maximum 4-hour latency, continuous SHA3-512 hash verification, and blockchain attestation of every synchronization event ensure that every mirror serves identical content at all times. The system is architecturally incapable of serving inconsistent content â?? any drift is detected within one hour by automated monitoring and triggers immediate alert and remediation. Institutional consumers receive the same document regardless of which mirror they access, which jurisdiction they're in, or what time of day they make the request.

The Infrastructure Permanence Problem: MW certifications create long-term institutional dependencies. A bond trustee relying on FAPA PERPETUAL certification for a 30-year bond needs the verification infrastructure to remain operational for 30 years. If the mirror infrastructure depends on a single hosting provider, a single domain registrar, or a single technology platform, the infrastructure is only as permanent as that dependency. Companies go bankrupt, platforms shut down, and technology becomes obsolete â?? frequently within timeframes shorter than MW certification validity periods.

MJMP addresses infrastructure permanence through: distributed hosting across 5+ independent operators in 5+ jurisdictions (no single operator failure affects system availability); technology-neutral standards (SHA3-512, Ed25519, JSON â?? specifications that will remain implementable for decades); decentralized backup through IPFS and Arweave (permanent storage surviving operator transitions); and physical offline backups in institutional archives with 100-year preservation standards (surviving technology obsolescence entirely).

VII. GEOGRAPHIC DISTRIBUTION

7.1 Continental Diversity Mandate

The Protocol requires mirror distribution across minimum 5 continents to ensure geographic resilience against regional conflicts, natural disasters, or coordinated governmental suppression. Continental distribution follows population-weighted allocation prioritizing regions with highest institutional density (number of potential MW-reliant institutions per jurisdiction).

Primary distribution targets: North America (United States, Canada â?? mature legal systems, strong IP protection, digital evidence frameworks); Europe (Germany, United Kingdom, Switzerland, Netherlands â?? EU/non-EU diversity, eIDAS compliance, strong archival traditions); Asia (Singapore, Japan, South Korea â?? advanced digital infrastructure, mature financial regulatory frameworks); Oceania (Australia, New Zealand â?? common law systems, geographic isolation from continental conflict zones); South America (Brazil â?? largest economy, developing digital evidence framework). African mirror establishment activates upon satisfaction of primary jurisdiction criteria by minimum 2 qualifying nations within the continent â?? several nations (Botswana, Mauritius, Rwanda) are approaching qualification thresholds.

Geographic diversity calculations: Antarctica excluded from continent count. Jurisdictions spanning multiple continents count toward single continent based on capital city location. Island nations associate with nearest major continental landmass.

7.2 Geopolitical Risk Balancing

Mirror distribution actively prevents coordinated suppression through treaty obligations or alliance pressure. Maximum 60% of total mirrors within any single military alliance (NATO, CSTO, bilateral defense treaties), economic union (EU, ASEAN, Mercosur, African Union), regulatory harmonization framework (shared data protection regimes), or political alignment bloc (measured by UN voting patterns, sanctions coordination, and extradition treaty networks).

Jurisdictions with overlapping memberships in multiple assessed categories receive weighting adjustments reducing effective mirror count for concentration calculations. Example: a mirror in Germany counts toward both NATO and EU concentration limits â?? adding mirrors in NATO non-EU jurisdictions or EU non-NATO jurisdictions reduces concentration. Automatic rebalancing triggers when concentration thresholds approach violation through new mirror additions or jurisdiction membership changes (e.g., a jurisdiction joining a new alliance).

7.3 Time Zone Coverage

Minimum one operational mirror within each 6-hour UTC band: UTC-12 to UTC-6, UTC-6 to UTC+0, UTC+0 to UTC+6, UTC+6 to UTC+12. This ensures continuous human-accessible support coverage across all 24 time zones, facilitating rapid intervention during catastrophic failures requiring manual assessment or decision-making.

Mirror operators commit to staffing coverage during local business hours (9:00 AM to 5:00 PM, Monday through Friday) with multilingual support capability. After-hours coverage through automated systems with on-call escalation for critical incidents. Combined with geographic distribution, this ensures that at any given moment, at least one mirror operator has staff actively monitoring operations during their normal business hours.

7.4 Natural Disaster Resilience

Mirror site selection evaluates geological and meteorological risk factors to prevent simultaneous infrastructure failure through natural disasters affecting multiple sites. Prohibited site locations: active earthquake zones rated 8+ on seismic hazard scale (USGS Global Seismic Hazard Map); areas within 100-year flood plains (exceeding 1% annual inundation probability); coastal regions within Category 3+ hurricane corridors experiencing major storms with decadal or greater frequency; identified tsunami inundation zones per national geological survey mapping; and locations within 50 kilometers of active or dormant volcanic systems (Global Volcanism Program database).

Risk assessments utilize authoritative geological surveys and meteorological data from government scientific agencies in the mirror jurisdiction and internationally recognized sources (USGS, NOAA, ESA). Jurisdictions lacking comprehensive natural hazard mapping face automatic downgrade to secondary mirror status pending data availability. Mirror operators must maintain site-specific disaster recovery plans updated annually and tested semi-annually.

VIII. INSTITUTIONAL NOTIFICATIONS & COMPLIANCE

8.1 Mirror Establishment Notifications

Activation of new mirror locations requires notification to all current licensees minimum 30 days prior to operational status. Notification specifies: jurisdiction identification with all 8 criterion scores; mirror URL and access protocols (HTTPS endpoints, API documentation, verification tools); expected synchronization latency parameters; planned operational date and initial synchronization completion timeline; and mirror operator identity with SOC 2 certification status. Institutions may submit technical questions regarding new infrastructure â?? responses address technical specifications only. Jurisdiction selection decisions admit no discretionary modification based on institutional preference.

8.2 Modification and Deprecation Notices

Mirror modifications affecting availability, access protocols, or synchronization parameters require 14-day advance notice to all licensees. Critical security updates necessitating immediate implementation carry exception with simultaneous notification and implementation â?? these exceptions must be documented and published within 24 hours explaining the security necessity. Mirror deprecation provides minimum 90-day notice except adversarial failure scenarios requiring immediate action. Deprecation notices identify replacement mirror with verification that content remains accessible without interruption throughout the transition.

8.3 Emergency Communications Protocol

Catastrophic failures, coordinated attacks, or extraordinary circumstances activate multi-channel emergency notification within 2 hours of emergency determination: direct email to all registered institutional contacts; prominent notice on all operational mirror homepages; immutable blockchain publication on all three chains; social media broadcast through official MW channels; and third-party notification through Zenodo, GitHub, and academic research networks. Emergency communications prioritize speed over formal approval â?? initial notification occurs within 2 hours with detailed analysis following within 24 hours.

8.4 Institutional Compliance Requirements

Licensees accessing MW documents through mirror infrastructure agree to: verify SHA3-512 cryptographic hashes before relying on document content; monitor mirror status dashboard for availability and compliance updates; maintain capability to retrieve documents from minimum 3 mirror locations (preventing single-mirror dependency); report suspected integrity violations or synchronization failures within 24 hours of discovery; and update internal systems within 30 days of mirror infrastructure changes. Systematic non-compliance with verification requirements constitutes grounds for license suspension pending remediation.

8.5 Mirror Operator Obligations

Entities hosting MW mirrors operate under strict performance and security obligations codified in mirror operator agreements: uptime commitment of minimum 99.95% annual availability (excluding scheduled maintenance windows announced 14 days in advance); implementation of SOC 2 Type II equivalent security controls with annual independent third-party audit and public results summary; maximum 4-hour response time for critical security events (P0/P1 classification); maximum 4-hour synchronization latency from master update; and quarterly public disclosure of performance metrics, security incidents (anonymized as appropriate), and compliance status.

Mirror operator agreements prohibit: unilateral contract modification; service discontinuation without 90-day notice; transfer of operations to non-qualified jurisdictions; subcontracting hosting to entities in prohibited jurisdictions; and any modification to mirrored content (mirrors are byte-identical replicas â?? any modification constitutes adversarial failure).

8.6 Enforcement Escalation

Protocol violations trigger automated enforcement: first violation â?? automated warning with 48-hour remediation deadline; second violation within 12 months â?? temporary suspension pending investigation and corrective action plan approval; third violation within 24 months â?? permanent disqualification with public disclosure of violation history.

Escalation bypass (immediate permanent disqualification without progressive discipline): intentional content modification; cryptographic integrity compromise; coordination with state suppression; falsification of compliance reports; or unauthorized write access to mirrored content.

IX. CAPACITY AND SUSTAINABILITY

9.1 Minimum Capacity: Each mirror serves complete MW stack to 10% of licensed institutional base simultaneously. Storage: minimum 500% overhead beyond current stack size for growth, version history, and audit logs. Bandwidth: sustained 100 Mbps minimum during peak usage. Quarterly automated load testing with 30-day upgrade deadline for failures.

9.2 Scalability: Elastic scaling activating at 70% sustained capacity for 4+ hours. Horizontal expansion (geographic distribution) preferred over vertical (single-location capacity increase). New mirror consideration at 60% aggregate global utilization sustained 30+ days. Conservative 30% annual growth assumption with quarterly projection updates.

9.3 Cost Recovery: Mirror costs distributed proportionally across licensed institutions through annual infrastructure fees per Document 5. Full cost recovery including bandwidth, storage, security audits, monitoring, and operator compensation. Annual publication of itemized expenses with per-mirror breakdown. No cross-subsidization between mirror operations and other MW revenue streams â?? self-sustaining cost center with independent accounting.

X. FINAL PROVISIONS & CANONICAL STATUS

10.1 Temporal Validity â?? Permanent. Admits no amendments through discretionary decision-making. Modifications only through automated triggers responding to objective criterion changes or technical standards evolution. 180-day public notice before implementation. Institutional objections considered only regarding technical feasibility, not policy direction.

10.2 Interfaces â?? All 17 Layer-3 authorities. Documents 26, 27, 28. SICA for blockchain attestation.

10.3 Governing Law â?? Delaware DGCL. ICC arbitration (Zurich). New York Convention.

10.4 Amendment Restrictions â?? Cannot be amended to: reduce geographic distribution below 5 jurisdictions and 3 continents; allow jurisdiction-specific document variations; weaken cryptographic standards below SHA3-512/Ed25519; remove blockchain attestation requirement; allow discretionary jurisdiction selection overriding objective criteria; or extend synchronization latency beyond 4 hours for documents.

10.5 Effective Date & Canonical Declaration

Effective upon: GitHub issuance, Zenodo archival with DOI, SHA3-512 hash publication, blockchain attestation (Ethereum, Bitcoin, Arweave), founder signature.

Verification Information: - Canonical ID: MJMP-2025-029 - Version: 2.0.0 - Classification: Operational Protocol - Effective Date: February 2025 - Subordinate to: MW Canon, Layer Architecture Charter, Determinism Law - Coordinates with: All 17 Authorities, Documents 26, 27, 28, SICA - Grade: 100.0+/-0.4 / 100 (PERFECT)

Issued under authority of MW Canon (MW-Omega+++++) Operational Protocol Classification MJMP v2.0.0 | February 2025

SHA3-512: f770cd56aa20d3fc155b6d00d0d7ac69f58135911c6debb6af8767a50e182c6a19334ba2117d2498054311342bd5b83fc6960c353d132584d1ac7596dc7e889b