# RAMPAGE

## Constitutional Framework

*Decentralized Truth Verification & Constitutional Journalism*

---

## Version 1.5

---

Original Adoption: November 27, 2025
Version 1.5 Effective: February 27, 2026
Founder: Shea Patrick Kastl
Legal Review: Shea Patrick Kastl, Vincent AI
Technical Architecture: Shea Patrick Kastl, Claude Sonnet 4.6, Gemini 3.0
TruthOracle.ai | RampageNews.com

## Document Metadata

Version: 1.5

Adopted: November 27, 2025

Amended: December 2, 2025 (Amendment No. 1: 95/5 Operational Split)

Amended: January 17, 2026 (Amendment No. 2: Truth Bearer Designation)

Amended: January 18, 2026 (Amendment No. 3: Data Protection and Privacy Framework)

Amended: January 18, 2026 (Amendment No. 4: Regulatory Classification and Compliance)

Amended: January 18, 2026 (Amendment No. 5: Enhanced Internal Controls and Governance Documentation)

Amended: January 18, 2026 (Amendment No. 6: Enhanced AML/CFT Documentation)

Amended: February 27, 2026 (Amendment No. 7: Strategic Validator Agreement Framework)

## PREAMBLE

We hold these truths to be self-evident: that all human beings possess inherent rights by virtue of their existence; that access to truth is a fundamental human right; that economic freedom is inseparable from human dignity; and that when governments systematically suppress these rights, individuals and communities must build infrastructure that enables the exercise of those rights. Rampage is that infrastructure.

Rampage is designed to operate as a public-good protocol, not as a commercial enterprise or investment vehicle. Rampage exists to serve individual human beings by operationalizing the principles enshrined in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the Geneva Conventions through decentralized technology that respects human dignity and resists centralized control.

Rampage operates in the gap between what international human rights law requires of states and what states actually provide to their people. Where governments fail to fulfill their obligations under international law, Rampage provides infrastructure for civilians to exercise rights that should already be protected.

Rampage acknowledges that upholding human rights may create legal risk. Rampage does not claim legal immunity, nor does it provide such immunity to participants. Rather, Rampage accepts that principled action in defense of human rights sometimes requires accepting legal consequences.

This Constitution establishes the framework for such principled action—humanitarian in purpose, nonviolent in method, and focused solely on civilian welfare.

*Rampage is not designed to break laws. It is designed to circumvent unjust laws that oppress human rights.*

## ARTICLE I: FOUNDATIONAL PRINCIPLES (Immutable)

### Section 1: Human Rights Primacy

Rampage recognizes the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and the Geneva Conventions as the moral and legal foundation for its operations. Rampage's mission is to help states fulfill their obligations under these treaties by providing infrastructure that enables civilians to exercise fundamental rights.

Clarification: Rampage's operations are intended to support, not supplant, domestic legal processes. Rampage does not claim authority to override national law but operates to enable civilians to exercise internationally recognized rights that their governments have failed to protect.

### Section 2: Mission Statement

Rampage's mission is threefold:

> Truth Verification: To establish verifiable facts about real-world events through decentralized oracle infrastructure, with particular focus on internet shutdowns, censorship, human rights violations, and humanitarian crises.

Information Access: To provide infrastructure enabling populations facing systematic information suppression to access truthful information, consistent with ICCPR Article 19 (freedom to seek, receive, and impart information).

Humanitarian Economic Access: To enable individuals in crisis situations to access financial resources necessary for survival, medical care, and emigration, consistent with the humanitarian principles of the Geneva Conventions.

### Section 3: Core Values

Truth over narrative: Rampage verifies observable facts, not political opinions.

Civilians over states: Rampage serves individual human beings, never governments or armed groups.

Rights within law: Rampage operates within humanitarian exceptions where possible, accepts legal risk where necessary, but prioritizes nonviolent, humanitarian purposes.

Decentralization over control: Rampage resists capture by any single entity.

Accountability with transparency: Rampage operates openly except where transparency endangers Truth Bearers or civilians, with robust internal controls.

### Section 4: Nonviolence Commitment

Rampage is committed to nonviolent humanitarian action. Rampage will not:

Support, fund, or coordinate with armed groups engaged in hostilities.

Provide resources that could be used for violence or weapons.

Advocate for, incite, or facilitate violent resistance.

Operate in ways that directly contribute to armed conflict.

Philosophy: Information and economic freedom are human rights. Violence is not. Rampage serves the former, never the latter.

---

## ARTICLE II: LEGAL FRAMEWORK (Immutable)

### Section 1: Hierarchy of Authority

Rampage operates under the following framework:

International Human Rights Law (Highest Authority): Universal Declaration of Human Rights (UDHR), International Covenant on Civil and Political Rights (ICCPR), Geneva Conventions and Additional Protocols. These define what human rights should be protected.

International Regulatory Standards (Compliance Obligations): FATF Recommendations (Anti-Money Laundering / Counter-Terrorism Financing), UN Security Council resolutions, international cooperation obligations. These define how Rampage must operate to prevent abuse.

National Laws (Jurisdictional Compliance): Valid and enforceable within their jurisdictions. Rampage acknowledges national law authority. Where national law conflicts with international human rights obligations, Rampage operates to enable civilians to exercise rights, accepting legal risk where necessary.

### Section 2: Legal Risk Philosophy

Rampage acknowledges that enabling civilians to exercise fundamental rights may create legal exposure in jurisdictions hostile to human rights. This is not a claim of legal immunity—it is acceptance of consequence.

Legal Disclaimer: Rampage does not provide legal immunity to validators, users, or any participant. All participants are responsible for understanding and complying with applicable laws in their jurisdiction. Rampage provides information about legal risks but cannot guarantee protection from prosecution, civil liability, or regulatory action.

Participation in Rampage is voluntary. Participants accept that upholding human rights through decentralized infrastructure may create legal consequences. Rampage provides legal defense resources but cannot prevent legal action by authorities.

Participants are strongly advised to seek local legal counsel in their jurisdiction before engaging with Rampage operations, especially if they reside in or interact with restrictive or sanctioned jurisdictions. Rampage provides general legal risk information but cannot provide individualized legal advice. Each participant must assess their own legal exposure and make informed decisions about participation.

## Section 3: Humanitarian Operations Framework

When operating in jurisdictions with restrictions that conflict with international human rights standards, Rampage:

**Prioritizes:**

Nonviolent, humanitarian purposes only.

Civilian welfare (food, medicine, survival, emigration).

Compliance with international humanitarian law principles (necessity, proportionality, distinction between civilians and combatants).

**Prohibits:**

Support for violence or armed conflict.

Weapons, dual-use technology, or military supplies.

Resources to governments, militaries, or designated terrorist organizations.

Operations that violate international prohibitions on terrorism financing or weapons proliferation.

**Seeks to operate within:**

Humanitarian exceptions in sanctions regimes where they exist.

International law frameworks (Geneva Conventions, IHL).

Transparent processes that demonstrate humanitarian intent.

## Section 4: Sanctions Compliance and Humanitarian Exceptions

Rampage acknowledges the existence of international and national sanctions regimes. Rampage's approach:

**Compliance:**

Rigorous screening against OFAC SDN list, UN Security Council sanctions lists, EU sanctions lists, and other major international designations.

Prohibition on routing capital to sanctioned governments, militaries, or designated entities.

Verification that recipients are civilians exercising fundamental rights.

Documentation of humanitarian purpose (survival, medical care, emigration).

**Humanitarian Focus:**

Where sanctions regimes include humanitarian exceptions (food, medicine, civilian welfare), Rampage operates within those exceptions.

Where humanitarian exceptions exist but are denied or unavailable through traditional channels, Rampage may provide infrastructure for civilians to access such resources, acknowledging legal risk.

Rampage does not facilitate prohibited activities (weapons proliferation, terrorism financing, military support).

Legal Position: Rampage argues that comprehensive sanctions preventing civilian access to information and survival resources violate IHL principles (Geneva Convention Article 23, Additional Protocol I Article 70). However, Rampage acknowledges this is a contested legal position and does not claim immunity from sanctions enforcement. Validators in jurisdictions with sanctions enforcement (U.S., EU, etc.) participate voluntarily, understanding legal exposure, and may choose not to participate in operations they believe violate applicable law.

## Section 5: Anti-Money Laundering and Counter-Terrorism Financing

Rampage acknowledges obligations to prevent misuse of its infrastructure for money laundering or terrorism financing.

**AML/CFT Measures:**

Automated screening of capital routing against OFAC, UN, EU, FATF, and other major terrorist designation lists.

Multi-signature controls on treasury operations requiring validator consensus.

Transaction monitoring for patterns consistent with illicit finance.

Prohibition on serving entities designated by multiple international bodies as terrorist organizations.

Governance oversight of capital routing with transparency (except where transparency endangers recipients).

Periodic third-party audits of capital routing controls (anonymized to protect recipients).

**Prohibited Entities (Comprehensive):**

UN Security Council designated terrorists.

OFAC designated terrorists and SDN list entities.

EU designated terrorists.

Entities designated by FATF for terrorism financing or proliferation.

Any entity engaged in systematic violence against civilians (regardless of designation).

Governments, militaries, intelligence agencies.

**Due Diligence:**

Recipient verification: Confirmed civilian, not on prohibited lists.

Purpose verification: Humanitarian (survival, medical, emigration), documentation required.

Beneficial ownership: Verification that recipient is actual beneficiary, not front for prohibited entity.

Risk assessment: Higher scrutiny for large transfers, high-risk jurisdictions, or unusual patterns.

Travel Rule Tension Acknowledgment: Rampage acknowledges potential tension between validator anonymity protections (Article II, Section 6) and certain financial regulations (e.g., FATF Travel Rule). Where this tension exists:

Validators in jurisdictions requiring Travel Rule compliance may opt out of capital routing operations to remain compliant with local law.

Validators in high-risk jurisdictions (where anonymity is necessary for physical safety) are exempt from Travel Rule compliance due to Article I (Human Rights Primacy)—safety over regulatory convenience.

All capital routing transactions still undergo prohibited-entity screening (Article V, Section 4) regardless of validator anonymity tier.

## Section 6: Validator Protection and Legal Defense

Rampage commits to supporting Truth Bearers who face legal consequences for upholding human rights:

**Legal Defense Fund:**

5% of community treasury (1,050,000 RPM) permanently reserved for validator legal defense.

Covers legal fees, appeals, and support for validators prosecuted for Rampage participation.

Administered by governance, with emergency disbursement authority.

Defense strategy based on international human rights law, humanitarian necessity, and good-faith operation.

**Legal Resources:**

Jurisdiction-specific risk assessments (updated quarterly).

Referral network of human rights lawyers.

Legal guidance documents for validators.

Model defense strategies based on international law.

**Anonymity Protections (Tiered):**

High-risk jurisdictions (authoritarian states: China, Russia, Iran, North Korea, Saudi Arabia, UAE, Belarus): Mandatory anonymity via technical enforcement (Tor, VPN, no identifiable information).

Medium-risk jurisdictions (sanctions enforcement states: U.S., EU, with rule of law): Pseudonymity with optional full anonymity; validators choose based on risk tolerance.

Low-risk jurisdictions (no legal barriers to human rights work): Standard transparency.

**Legal Response Protocol:**

Rampage will respond to legitimate legal process in jurisdictions with rule of law, subject to Constitutional principles:

Requests must be specific, lawful, and accompanied by appropriate legal authority.

Rampage will not compromise validator anonymity in high-risk jurisdictions.

Rampage will challenge requests that violate human rights or target humanitarian activity.

Governance vote required for compliance with requests targeting Constitutional operations.

### Section 7: Regulatory Classification and Compliance

RPM is a utility token designed for governance and coordination, not as an investment vehicle.

Utility Token: Primary utility is on-chain governance and validator staking.

Regulatory Shield: RPM is not a security, asset-referenced token (ART), or e-money token (EMT) under EU MiCA.

CASP Status: Rampage is a decentralized protocol, not a traditional Crypto-Asset Service Provider, as it does not custody user funds or provide exchange services.

White Paper: A comprehensive white paper will be maintained and updated annually at RampageNews.com/whitepaper.

---

## ARTICLE III: OPERATIONAL BOUNDARIES (Immutable)

### Section 1: Government Neutrality with Regulatory Acknowledgment

Rampage serves civilians, not governments. However, Rampage acknowledges the legitimacy of certain regulatory functions.

**Rampage does not:**

Provide services to governments, militaries, or intelligence agencies.

Seek government approval for human rights operations.

Accept government authority over fundamental rights.

Allow governments to veto human rights infrastructure.

**Rampage does acknowledge:**

International cooperation obligations regarding terrorism and money laundering (FATF standards).

Legitimate law enforcement functions in jurisdictions with rule of law (with due process protections).

International regulatory frameworks preventing terrorism financing and weapons proliferation.

Balance: Rampage resists government censorship and human rights suppression, but cooperates with legitimate efforts to prevent terrorism, money laundering, and violence. The distinction is:

Legitimate regulation: Preventing harm (terrorism, money laundering, weapons) = Rampage cooperates.

Illegitimate control: Suppressing rights (censorship, information control, economic imprisonment) = Rampage resists.

### Section 2: Civilian-Only Focus

Rampage serves civilians exclusively. "Civilian" is defined by International Humanitarian Law standards: individuals not taking direct part in hostilities, not members of armed forces, and not officials of government or military entities.

**Verification Requirements:**

Identity verification (civilian status confirmed).

Purpose verification (humanitarian need documented).

Beneficial ownership verification (actual recipient is civilian).

Ongoing monitoring (no evidence recipient is front for prohibited entity).

**Prohibited Recipients:**

Government entities (executive, legislative, judicial, administrative).

Military organizations (active duty, reserves, militias under state control).

Intelligence agencies (domestic or foreign).

Designated terrorist organizations (by UN, OFAC, EU, FATF, or multiple international bodies).

Armed groups engaged in hostilities (state or non-state).

Individuals acting as agents of prohibited entities.

When state and civilian interests conflict, Rampage chooses civilians—but only civilians as defined by IHL.

Good-Faith Effort and Liability: Rampage acknowledges that despite best efforts, determined bad actors may attempt to misuse the protocol for prohibited purposes. Rampage's Constitutional commitment, technical enforcement mechanisms (mempool shield), multi-step verification processes, and validator slashing provisions represent good-faith efforts to prevent such misuse. Liability for misuse rests with the bad actor, not with validators acting in good faith in accordance with Constitutional requirements.

---

## ARTICLE IV: TRUTH VERIFICATION STANDARDS (Immutable)

### Section 1: Observable Facts Only

Rampage verifies objective, observable facts. Rampage does not make political or moral judgments about governments, ideologies, or legitimacy claims.

**Rampage CAN verify:**

Internet shutdown occurred (technical measurement: BGP routing, DNS resolution, network reachability).

Journalist was imprisoned (documented event: court records, credible news sources, human rights organization reports).

Protest occurred with estimated size (satellite imagery, multiple on-ground sources, metadata analysis).

Economic sanctions in effect (public legal record: official government/UN documents).

Capital controls implemented (verifiable policy: official announcements, banking restrictions).

Casualties during conflict (hospital records, multiple witness testimony, forensic evidence where available).

Communications infrastructure disrupted (technical measurement).

**Rampage CANNOT verify (political/moral questions outside scope):**

Which government is "legitimate" in contested situations.

Whether a protest is "justified" or "unjustified."

Whether sanctions are "appropriate" policy.

Whose narrative is "true" when underlying facts are disputed.

Moral culpability for events (attribution of responsibility).

Rampage publishes facts, not opinions. Rampage is infrastructure for truth-seeking, not political judgment.

## Section 2: Multi-Source Verification Requirements

Truth verification follows tiered requirements based on controversy level and evidence complexity:

**Level 1 Attestations (Low controversy, clear technical evidence):**

Minimum 3 independent sources.

At least 1 technical measurement (if applicable).

Sources must be from different organizations/countries.

Validator consensus: 60% agreement.

Example: Internet shutdown (BGP data + DNS monitoring + user reports from multiple ISPs).

**Level 2 Attestations (Medium controversy, mixed evidence):**

Minimum 5 independent sources.

At least 2 sources with direct evidence (primary sources, not reports of reports).

Geographic/institutional diversity required.

Validator consensus: 67% agreement.

Example: Protest size estimation (satellite imagery + media reports from multiple outlets + on-ground witnesses).

**Level 3 Attestations (High controversy or complexity):**

Minimum 7 independent sources.

Multiple types of evidence (technical + documentary + witness).

Validator consensus: 80% agreement.

Independent verification by at least 2 validators with domain expertise.

Example: Attribution of casualties during conflict (hospital records + witness testimony + forensic evidence + human rights organization investigation).

**Source Quality Standards:**

Primary sources preferred over secondary.

Multiple countries/organizations (avoid single-source bias).

Technical evidence weighted heavily where available.

Anonymous sources acceptable with corroboration.

State media alone insufficient (requires corroboration from independent sources).

## Section 3: Publication Standards

All published attestations include:

Sources cited (anonymized if necessary for source protection).

Methodology documented (how verification was performed).

Timestamp (when verification occurred).

Validator signatures (which validators attested).

Legal disclaimer (see below).

Legal Disclaimer on All Publications: "This information is provided for informational purposes only based on multi-source verification as of [timestamp]. Rampage makes no warranties of accuracy, completeness, or suitability for any purpose. Verification methodology is documented at [link]. Affected parties may challenge this information through the governance dispute resolution process at [link]. Rampage and its validators disclaim liability for good-faith errors in verification."

## Section 4: Correction and Accountability

When Rampage publishes information later proven false or inaccurate:

**Mandatory Correction Process:**

Immediate on-chain correction (immutable record of error with timestamp).

Prominent notification to all who accessed original information.

Preservation of original attestation (transparency about what was published).

Publication of correction reasoning (why original was false, what evidence proved it).

Attribution of correction (who identified error, what process was used).

**Validator Accountability and Slashing:**

Good-faith error with proper methodology: 1-5% stake slashed, appealable through governance. Validator followed verification standards but reached incorrect conclusion. No evidence of negligence or bad faith. First-time error with documented methodology.

Negligent verification: 5-20% stake slashed. Insufficient due diligence (failed to follow verification standards). Reliance on single source or unverified information. Failure to cross-reference or corroborate.

Intentional fabrication (first offense): 20-50% stake slashed. Deliberate falsification of evidence. Collusion with other Truth Bearers to manipulate attestations. Publication of information known to be false.

Intentional fabrication (second offense): 100% stake slashed + permanent expulsion from validator set. Zero tolerance for repeated deliberate falsification. Immediate and permanent removal from network. No appeals for second intentional offense.

**Appeals Process:**

Slashed Truth Bearer may appeal to governance within 30 days.

Governance reviews evidence from both sides.

67% vote required to overturn slashing.

Burden of proof on validator to demonstrate good faith/proper methodology.

Appeals decision is final (no further appeals).

**Public Acknowledgment:**

Annual transparency report documenting all corrections.

Public discussion of verification failures (how did error occur?).

Process improvements based on lessons learned.

**Takedown/Challenge Process:**

Any party may challenge published information by submitting counter-evidence to governance.

Governance reviews challenge within 14 days.

If counter-evidence credible, attestation flagged as "disputed" pending resolution.

Full review by independent validators appointed by governance.

Decision requires 67% governance vote; both parties may present evidence.

Losing party may appeal once; final decision is binding.

---

# ARTICLE V: OPERATIONAL FRAMEWORK (Amendable)

## Section 1.1: Operational Priority Allocation

Rampage commits to the following resource and focus allocation for long-term legal defensibility and mission sustainability:

Core Function (95% Allocation): Truth Verification via TruthOracle operations and passive Information Access infrastructure (Article I, Section 2, items 1 & 2). This function is active at all Threat Levels and constitutes the primary ongoing output of the protocol.

Crisis Function (5% Allocation): Active Information Penetration and Humanitarian Economic Access (Article I, Section 2, item 3). This function activates only at Threat Level 2 and higher and is strictly limited to civilian, nonviolent, humanitarian purposes (food, medicine, emigration, and circumvention tools).

Enforcement & Transparency: Treasury expenditures, validator rewards, and TruthOracle compute cycles shall be allocated so as to maintain at least a 95/5 ratio during Level 0–1 operations. The Governance Module shall calculate and publish the actual ratio on-chain every calendar quarter. Persistent deviation exceeding eighteen (18) consecutive months shall require a formal governance proposal to amend this section.

## Section 1.2: Threat Level Taxonomy & Module Activation

Transition Rules:

Level 1 → 2 or 2 → 3 requires Humanitarian Escalation Protocol (Article VI).

Level 4 is emergency power (simple majority, 24-hour confirmation).

De-escalation follows reverse path with same thresholds.

## Section 2: Geographic Distribution Requirements

To prevent capture, ensure ground truth, and protect against coordinated attacks:

**Validator Distribution:**

Minimum 30% of validators in jurisdictions where Rampage operations are unambiguously legal.

Maximum 10% of validators in any single jurisdiction (prevents capture by any one state).

Minimum 20% of validators in Global South / developing economies (ensures ground truth, prevents Western bias in attestations).

At least 5 validators in each region (Africa, Asia, Europe, Latin America, Middle East, North America) to ensure geographic diversity.

**Anonymity Tier Verification:**

Validators must prove membership in one of three anonymity tiers via zero-knowledge proof (zk-SNARK) or attestation by 3-of-5 trusted geographic attesters appointed by governance.

**Three Anonymity Tiers:**

Tier 1 (High-Risk): Mandatory anonymity jurisdictions (China, Russia, Iran, North Korea, Saudi Arabia, UAE, Belarus, Eritrea, Turkmenistan, and other authoritarian states).

Tier 2 (Medium-Risk): Optional anonymity jurisdictions (U.S., EU, sanctions-enforcing states with rule of law).

Tier 3 (Low-Risk): Standard transparency jurisdictions (democracies with no legal barriers to human rights work).

**What the Proof Reveals:**

The proof reveals only: "This validator is in Tier [X]."

The proof never reveals: Specific country, region, or identifiable location.

Raw jurisdiction data is never stored on-chain.

Governance monitors only aggregate distribution (e.g., "30% Tier 3, 50% Tier 2, 20% Tier 1") to ensure Constitutional geographic requirements are met.

**Risk-Based Participation:**

Validators in high-risk jurisdictions may choose which operations to participate in.

Can opt out of operations in sanctioned jurisdictions if they believe it violates their national law.

Cannot opt out of truth verification (core validator function).

Must disclose tier membership (for distribution monitoring) but not specific location.

## Section 3: Oracle Operations (TruthOracle)

Truth attestation follows this process:

**Event Detection:**

Automated monitoring (BGP routing, DNS, network reachability, satellite imagery).

Human reports from credible sources.

Open-source intelligence aggregation.

Media monitoring (multiple countries/languages).

**Source Verification:**

Multi-source corroboration (3-7 sources depending on threat level).

Source credibility assessment (track record, institutional affiliation, methodology).

Cross-referencing across languages/countries.

Technical evidence prioritized where available.

**Validator Attestation:**

Geographic-diverse validators confirm independently (cannot copy-paste).

Each Truth Bearer documents their methodology.

Validators with domain expertise weighted (e.g., regional experts, technical specialists).

Minimum 3 validators must independently verify before publication.

**Consensus Threshold:**

Level 1: 60% validator agreement.

Level 2: 67% validator agreement.

Level 3: 80% validator agreement + governance review for high-controversy claims.

Geographic diversity required (not all validators from one region).

**On-Chain Publication:**

Immutable record of verified fact.

Sources cited (anonymized if necessary for source protection).

Methodology documented.

Timestamp and validator signatures.

Legal disclaimer attached.

Slashing for False Attestation: See Article IV, Section 4 for complete slashing framework (1-5% for good-faith errors, up to 100% + permanent expulsion for intentional fabrication on second offense).

## Section 4: Capital Routing Framework

Financial assistance to civilians operates under strict humanitarian constraints:

**Recipient Verification (Multi-Step):**

Identity verification (civilian, not on prohibited lists).

Purpose verification (humanitarian need documented: medical emergency, food insecurity, emigration, etc.).

Prohibited list screening (OFAC SDN, UN, EU, FATF lists—automated).

Beneficial ownership verification (actual recipient is civilian, not front for prohibited entity).

Risk assessment (large transfers or high-risk jurisdictions require additional scrutiny).

**Authorized Purposes (Humanitarian Only):**

Food, clean water, basic survival needs.

Medical care, medications, emergency medical evacuation.

Shelter, clothing, heating.

Emigration costs (travel documents, transportation, resettlement).

Communication tools (phones, internet access) for civilians exercising freedom of expression.

Education costs (where education is being denied).

**Prohibited Purposes:**

Weapons, ammunition, explosives.

Dual-use technology (items that could be used for military purposes).

Support for armed groups or violence.

Luxury goods, non-essential items.

Payments to governments, militaries, or prohibited entities.

Any activity that would violate international prohibitions on terrorism financing or weapons proliferation.

**Transfer Controls:**

Small transfers (<$500 USD equivalent): Automated with screening.

Medium transfers ($500-5,000): Multi-signature validator approval (3-of-5).

Large transfers (>$5,000): Governance approval + enhanced due diligence.

Emergency transfers: Expedited process available during Level 3 crises (48-hour approval).

Enhanced Due Diligence (EDD) is mandatory for transfers over $5,000 or for recipients in Level 3 crisis zones.

**Transparency with Privacy:**

All capital routing recorded on-chain (preserves accountability).

Recipient anonymity protected (hashed identifiers, no personally identifiable information published).

Periodic aggregate reporting (total routed by country/purpose, no individual details).

Third-party audits (quarterly, by independent firm, results published).

**Shielded Pool Option:**

Opt-in privacy pool for recipients facing state surveillance (Zcash-style shielded transactions).

Available only after verification process completed (no anonymous deposits).

Enhanced monitoring for abuse (heuristic analysis, unusual pattern detection).

Governance can pause privacy pool if evidence of systematic abuse.

**Prohibited-Entity Mempool Shield:**

All capital-routing transactions are rejected at mempool level if the recipient address appears on the continuously updated prohibited-entity oracle feed (OFAC SDN, UN Consolidated List, EU sanctions lists, FATF designations, and any additional lists added via Emergency Legal Compliance process under Article X, Section 3). This filter operates at the consensus layer and cannot be bypassed by governance vote, emergency powers, or any mechanism short of a full Constitutional amendment under Article X, Section 2 (requiring 60% quorum, 80% supermajority, and 90-day implementation delay). The oracle feed is updated automatically from authoritative sources (OFAC, UN, EU, FATF). Feed accuracy and timeliness are verified by 5-of-7 trusted oracle signers appointed by governance. If the oracle feed fails or cannot be verified, the mempool shield defaults to REJECT all capital routing transactions until the feed is restored. This technical enforcement mechanism ensures that Rampage cannot route funds to prohibited entities even if governance were compromised or coerced. The blockchain is physically incapable of executing such transactions.

## Section 5: Data Protection and Privacy

Rampage commits to privacy-by-design and GDPR compliance.

Data Controllers: Individual Truth Bearers act as independent data controllers for operational data.

Minimization: No personally identifiable information (PII) is published on-chain; all identifiers are hashed.

Training: All Bearers must complete mandatory data protection training before handling personal data.

---

# ARTICLE VI: GOVERNANCE (Amendable)

## Section 1: Decentralized Governance

Rampage is governed by RPM token holders through on-chain voting. No individual, company, or government can control Rampage.

**Governance Powers:**

Constitutional amendments (Articles V-XI only; Articles I-IV are immutable).

Threat level escalations (Level 2+ requires governance vote except in emergencies).

Treasury allocation beyond defined budgets.

Validator slashing appeals.

Oracle dispute resolution.

Emergency legal compliance decisions.

Prohibited entity additions (beyond automated lists).

**Governance Limitations:**

Cannot violate core Constitutional principles (Articles I-IV) except for dissolution.

Cannot serve state actors or armed groups.

Cannot abandon civilian populations facing Level 2+ human rights crises without documented justification.

Cannot centralize control.

Cannot eliminate transparency/accountability mechanisms.

**Voting Requirements:**

Standard proposals: 51% quorum, 67% approval.

Constitutional amendments (Articles V-XI): 60% quorum, 80% approval.

Emergency legal compliance: 40% quorum, 75% approval, 7-day expedited process.

Threat level escalations: See Article VI, Section 4 (Humanitarian Escalation Protocol).

Large capital routing (>$10,000): 40% quorum, 60% approval.

## Section 2: Community Treasury

21% of RPM supply (21,000,000 RPM) vested linearly over 4 years to community treasury.

**Authorized Uses:**

Validator incentives and rewards (40% of treasury).

Legal defense fund (5% of treasury, permanently reserved—1,050,000 RPM).

Oracle operations funding (20% of treasury).

Information penetration infrastructure (15% of treasury: VPN, Tor, satellite, mesh networks).

Emergency humanitarian capital routing (10% of treasury).

Developer grants, security audits, third-party reviews (10% of treasury).

**Prohibited Uses:**

Payments to governments, militaries, or intelligence agencies.

Funding designated terrorist organizations (by any major international body).

Support for armed groups or violence.

Personal enrichment of founders or validators beyond defined compensation.

Operations violating Constitutional principles.

Lobbying or political campaign contributions in any jurisdiction.

**Spending Controls:**

Quarterly budgets approved by governance.

Multi-signature treasury (see scaling thresholds below).

Monthly transparency reports (all expenditures documented).

Annual third-party audit (results published).

Emergency spending authority (up to 5% of quarterly budget without governance vote, for time-sensitive humanitarian needs).

**Treasury Multi-Signature Scaling:**

Treasury multi-signature threshold automatically scales with treasury value to prevent kidnapping/coercion attacks:

<$5M: 5-of-9 multi-signature.

$5M-25M: 7-of-11 multi-signature.

$25M-100M: 15-of-27 multi-signature.

>$100M: 21-of-39 multi-signature.

**Geographic Distribution Requirements for Signers:**

Maximum 2 signers per continent (prevents regional capture).

No two signers who personally know each other (prevents social engineering).

Signers must be from at least 5 different countries.

Governance appoints signers via 67% vote; signers serve 2-year terms.

## Section 3: Emergency Powers

During Level 3 crises, governance can authorize expedited operations with reduced procedural requirements:

**Authorized Emergency Measures:**

Expedited capital routing (48-hour approval instead of standard 7-day).

Increased treasury allocation for crisis response (up to 2x normal quarterly budget).

Validator bonuses for high-risk operations (hazard pay).

Coordination with verified humanitarian organizations (NGOs, UN agencies, Red Cross/Crescent).

Enhanced information penetration efforts.

**Strict Prohibitions During Emergency:**

No coordination with armed groups under any circumstances.

No support for violence or weapons.

No abandonment of verification standards (expedited ≠ eliminated).

No routing to prohibited entities (screening still mandatory).

All emergency operations must have documented humanitarian purpose.

**Time Limits and Oversight:**

Emergency powers expire after 90 days unless renewed by governance vote.

Weekly transparency reports during emergency (detailed accounting of all actions).

Post-emergency review required (lessons learned, process improvements).

Validators may appeal emergency decisions through governance.

**Emergency Legal Compliance:**

If new binding international legal obligation requires immediate Constitutional adaptation:

Emergency governance vote (7-day process, 75% approval, 40% quorum).

Changes must be minimum necessary to achieve compliance.

90-day sunset clause (must be made permanent through standard amendment process or reverts).

Used only for compliance with international law, not national law.

## Section 4: Humanitarian Escalation Protocol

Any escalation from Level 2 to Level 3, or addition of a new scenario-specific jurisdiction under Article VIII, requires:

**Voting Thresholds:**

75% of total voting power (not just participating voters—requires supermajority of all RPM).

Minimum 50% of all circulating RPM participating (prevents small-group manipulation).

30-day voting period (allows thorough deliberation and community input).

90-day implementation delay (allows validators to exit if they disagree with escalation).

**Required Documentation (Evidence Package):**

All escalation proposals must include:

Multi-source crisis documentation: Minimum 7 independent sources documenting humanitarian emergency, systematic violence, or total information blackout.

Legal analysis: Assessment of applicable international law violations (ICCPR breaches, IHL violations, Geneva Convention applicability).

Validator risk assessment: Documented legal exposure for validators participating in operations (by jurisdiction).

Explicit de-escalation criteria: Specific conditions that would trigger Level 3→Level 2 downgrade.

**De-escalation Process:**

De-escalation from Level 3 to Level 2, or removal of a jurisdiction from Article VIII scenario-specific operations, follows identical thresholds: 75% voting power, 50% quorum, 30-day vote, 90-day delay. Prevents yo-yo manipulation (cannot rapidly escalate/de-escalate). Ensures de-escalation receives same scrutiny as escalation.

### Section 5: Internal Controls and Compliance Framework

Governance appoints a Compliance Officer to oversee regulatory monitoring (MiCA, GDPR, AML/CFT).

Compliance Register: A centralized record of all regulatory policies, audit results, and authority communications is maintained.

Risk Management: Quarterly risk assessments are published in transparency reports.

---

## ARTICLE VII: TRUTH BEARER RIGHTS AND RESPONSIBILITIES (Amendable)

*Note: Article VII has been amended by Amendment No. 7 (February 27, 2026), which adds Sections 7.4 through 7.7 establishing the Strategic Validator Agreement Framework. All original sections remain intact and unchanged.*

### Section 1: Truth Bearer Designation

Truth Bearers who operate Rampage infrastructure and perform truth verification have the following rights:

**Economic Rewards:**

Staking rewards for network security.

Transaction fees from capital routing operations.

Oracle attestation rewards for truth verification.

Proportional to stake and participation.

**Legal Defense Support:**

Access to legal defense fund (5% of treasury, 1,050,000 RPM permanently reserved).

Coverage for legal fees, appeals, and support if prosecuted for Rampage participation.

Referral network of human rights lawyers.

Jurisdiction-specific risk assessments (updated quarterly).

Model defense strategies based on international law.

**Anonymity Protections:**

Mandatory anonymity in high-risk jurisdictions (Tier 1: authoritarian states).

Optional anonymity in medium-risk jurisdictions (Tier 2: sanctions-enforcing states with rule of law).

Technical enforcement via Tor, VPN, no identifiable information stored on-chain.

Protection from doxing or validator identification attempts.

**Due Process in Slashing Disputes:**

Appeals process through governance (67% vote required to overturn slashing).

30-day appeal window.

Right to present evidence and defense.

Burden of proof on validator to demonstrate good faith/proper methodology.

**Governance Voice:**

Voting power proportional to stake.

Ability to propose governance actions.

Participation in all governance decisions.

**Opt-Out Rights:**

May opt out of operations in sanctioned jurisdictions if validator believes it violates their national law.

Cannot opt out of core truth verification (fundamental validator function).

Must notify governance of opt-out to maintain geographic distribution compliance.

**Access to Information:**

Full access to verification methodology documentation.

Training materials for truth attestation.

Technical support for validator operations.

Transparency about legal risks in all jurisdictions.

## Section 2: Truth Bearer Responsibilities

Truth Bearers accept the following responsibilities when joining Rampage:

**Independent Verification:**

Verify information independently using documented methodology.

No copy-pasting from other Truth Bearers.

Cross-reference multiple sources.

Apply appropriate skepticism to claims.

**Operational Reliability:**

Maintain infrastructure uptime (minimum 95% uptime required).

Respond to attestation requests within reasonable timeframe.

Participate in governance votes.

Keep software updated and secure.

**Operational Security:**

Use anonymity tools in high-risk jurisdictions (mandatory, not optional).

Protect private keys and validator credentials.

Report security incidents to governance.

Prevent unauthorized access to validator infrastructure.

**Good Faith Operation:**

Honest attestation of facts (no fabrication or collusion).

No manipulation of verification process for political or financial gain.

Report suspected validator misconduct to governance.

Act in accordance with Constitutional principles.

**Constitutional Compliance:**

Uphold all Constitutional principles in operations.

Do not route capital to prohibited entities.

Do not support violence or armed groups.

Prioritize civilian welfare over political objectives.

**Due Diligence on Capital Routing:**

Enhanced scrutiny for large transfers.

Verification of recipient civilian status.

Documentation of humanitarian purpose.

Risk assessment for high-risk jurisdictions.

**Transparency Where Safe:**

Disclose conflicts of interest to governance.

Participate in audits (where disclosure doesn't endanger Truth Bearer).

Report suspected misuse of Rampage infrastructure.

Contribute to annual transparency reporting.

## Section 3: Slashing Conditions

Truth Bearers are slashed (lose stake) for violations of Constitutional requirements or validator responsibilities. Slashing amount is proportional to severity:

**Minor Violations (1-5% stake slashed, or warning):**

Good-faith error in verification with proper methodology followed.

Technical failures beyond validator control.

First-time procedural violations (e.g., late attestation, missed governance vote).

Downtime below 95% threshold due to unforeseen circumstances.

**Moderate Violations (5-20% stake slashed):**

Negligent verification (insufficient due diligence, failure to follow methodology).

Repeated downtime or unreliability affecting network operations.

Failure to use required anonymity tools in high-risk jurisdictions (endangers other validators).

Minor security lapses that do not compromise network.

**Severe Violations (20-50% stake slashed, possible removal):**

Intentional false attestation (first offense).

Collusion with other Truth Bearers to manipulate attestations.

Routing capital to prohibited entities (governments, militaries, terrorists).

Security failures that endanger other Truth Bearers (e.g., doxing other Truth Bearers).

Systematic violations of Constitutional principles.

**Critical Violations (100% stake slashed + permanent expulsion):**

Intentional false attestation (second offense)—zero tolerance for repeated fabrication.

Collaboration with state actors to compromise Rampage operations.

Deliberate routing to designated terrorist organizations.

Actions that directly endanger validator lives.

**Appeals Process:**

Slashed Truth Bearer may appeal to governance within 30 days of slashing.

Governance reviews evidence from validator and accuser.

67% vote required to overturn slashing.

Burden of proof on validator to demonstrate good faith and/or proper methodology.

If slashing upheld, Truth Bearer may not appeal again (decision is final).

If slashing overturned, stake is restored and Truth Bearer may continue operations.

---

## AMENDMENT NO. 7 — STRATEGIC VALIDATOR AGREEMENT FRAMEWORK

*The following Sections 7.4 through 7.7 were added to Article VII by Amendment No. 7, ratified February 27, 2026.*

### Section 7.4: Strategic Validator Agreement Authority

During the Pre-Mainnet Phase, as defined in Section 7.5 below, the Founder or, upon its formation, the Truth Bearer Council, shall have authority to execute Strategic Validator Agreements ("SVAs") with qualified institutional or strategic partners. SVAs may specify a reduced minimum staking threshold below the standard 100,000 RPM requirement, subject to the conditions and limitations set forth in this Amendment.

Transfer of Authority: SVA authority held by the Founder shall transfer automatically to the Truth Bearer Council upon its formation. Any SVA entered into by the Founder prior to that transfer remains valid and binding for its stated duration. Upon transfer, the Truth Bearer Council assumes full SVA authority and responsibility under this Section.

### Section 7.5: Definition of Pre-Mainnet Phase and Sunset Provision

The Pre-Mainnet Phase is defined as the period beginning upon ratification of this Amendment and concluding upon the deployment of the Rampage mainnet genesis block, currently targeted for Q4 2026. Upon mainnet deployment, the standard 100,000 RPM minimum staking requirement shall apply automatically and universally to all Truth Bearers.

Extension of Pre-Mainnet SVA Regime: The Pre-Mainnet SVA regime may be extended beyond mainnet launch only by a supermajority vote of 67% of all staked tokens pursuant to Article X of this Constitution. Any such extension must specify a defined duration not to exceed twelve (12) months

per extension, and must include a governance-approved review cadence of no less than once every six (6) months during the extension period. This requirement prevents indefinite extension of pre-mainnet flexibility without renewed community consensus.

Transition Standard for SVA Validators: All SVA validators must reach the standard 100,000 RPM minimum staking threshold within six (6) months following mainnet launch, or such other period as expressly specified in the executed SVA, failing which SVA validator status lapses automatically and the standard threshold applies. Governance may approve a single extension of the transition period not to exceed three (3) additional months upon documented good-faith showing by the SVA validator.

## Section 7.6: SVA Eligibility and Required Conditions

A Strategic Validator Agreement may be executed only where all of the following conditions are satisfied:

(a) The prospective validator demonstrates institutional alignment with the Rampage constitutional mission of truth verification, journalistic integrity, or humanitarian crisis response. For purposes of this Section, qualifying institutional categories include, but are not limited to: accredited journalism organizations and press freedom bodies; internationally recognized human rights organizations; UN agencies and affiliated non-governmental organizations; academic institutions with documented human rights or journalism research programs; and other mission-aligned entities as approved by governance. This list is illustrative, not exhaustive. Governance may establish additional guidance on qualifying categories without Constitutional amendment.

(b) The reduced staking threshold is specified in writing within the executed SVA, including the agreed minimum RPM stake, the duration of the reduced threshold, and conditions for transition to the standard threshold, consistent with Section 7.5.

(c) The SVA validator agrees to full compliance with all other Truth Bearer obligations under Article VII, including uptime requirements, governance participation, and compliance with the Mempool Shield AML/CFT framework established under Amendment No. 6.

(d) The SVA does not conflict with the immutable principles established in Articles I through IV of this Constitution.

(e) The executed SVA is recorded in the Rampage governance ledger and disclosed publicly through official Rampage channels within thirty (30) days of execution. Public disclosure shall include the identity of the SVA partner, the agreed staking threshold, the duration of the SVA, and the mission-alignment basis under subsection (a). Confidential commercial terms unrelated to validator obligations may be redacted with governance approval.

## Section 7.7: Constitutional Integrity Preservation

Nothing in this Amendment shall be construed to permanently lower, waive, or otherwise diminish the standard 100,000 RPM minimum staking requirement established in Article VII. SVAs represent temporary, bilateral, contractual arrangements for the Pre-Mainnet Phase only. The standard threshold remains the constitutional floor and the permanent standard of Truth Bearer participation in the Rampage network.

SVAs entered into under this Amendment do not constitute precedent for permanent reduction of the staking threshold. Any proposal to permanently reduce the standard 100,000 RPM minimum must proceed through the full Constitutional amendment process under Article X, Section 2, and is subject to all applicable quorum and supermajority requirements.

## ARTICLE VIII: SCENARIO-SPECIFIC OPERATIONS (Amendable)

This Article documents the specific humanitarian justifications and operational parameters for Rampage operations in high-risk jurisdictions. Each scenario has been assessed under international human rights law and approved via Humanitarian Escalation Protocol (Article VI, Section 4).

### Section 1: North Korea

**Status: Level 3 (Permanent Humanitarian Crisis)**

**Human Rights Violations:**

Total information blackout violating ICCPR Article 19 (North Korea signed ICCPR in 1981, in systematic breach of treaty obligation for 40+ years).

Systematic starvation violating ICCPR Article 6 (right to life).

Prison camps, torture, summary executions violating Geneva Conventions.

No freedom of movement violating UDHR Article 13.

70+ years of sustained, extreme human rights violations with no improvement.

**Operations Authorized:**

Information penetration via smuggled devices (USB drives, SD cards with outside information, radios).

Satellite internet access (Starlink or equivalent for verified recipients inside North Korea).

Mesh network infrastructure where possible.

Capital routing ONLY via verified resistance networks with documented civilian delivery channels (extremely high risk of regime capture requires intermediary verification).

**Operations Prohibited:**

Direct capital routing to individuals inside North Korea without verified resistance network intermediary.

Support for armed resistance (Rampage does not support violence under any circumstances).

Coordination with North Korean government, military, or Workers' Party entities.

**Legal Risk Acknowledgment:**

Extreme: Violates comprehensive UN Security Council sanctions (Resolutions 1718, 2087, 2094, 2270, 2321, 2371, 2375, 2397) + OFAC sanctions. All UN member states legally obligated to enforce sanctions. Truth Bearers accept this is highest legal risk jurisdiction in Rampage operations.

**De-escalation Criteria (Would trigger Level 3→Level 2):**

Restoration of internet access to civilian population.

Release of all political prisoners.

Ratification and implementation of press freedom reforms.

Demonstrable improvement in ICCPR compliance for 5+ consecutive years.

### Section 2: Iran

**Status: Level 4 (Active Armed Conflict — Effective February 28, 2026); de-escalation to prior tier requires Humanitarian Escalation Protocol.**

Note: On February 28, 2026, the United States and Israel commenced major combat operations against Iran (Operation Epic Fury). Iran launched retaliatory strikes against US military assets across the Gulf region. This active armed conflict triggers maximum Constitutional threat level parameters for Iran. All Level 3 operational authorities are activated. This status shall be reviewed by governance within 30 days and updated as conditions develop.

**Human Rights Violations (Pre-Conflict Basis):**

Internet shutdowns during protests violating ICCPR Article 19.

Execution of protesters violating ICCPR Article 6 (right to life).

Torture of dissidents violating ICCPR Article 7 + Geneva Conventions Article 3.

Gender apartheid violating UDHR, CEDAW.

Economic isolation combined with sanctions causing medical supply shortages.

**Operations Authorized — Level 4 (Active Armed Conflict):**

Maximum information penetration efforts to counter propaganda and document civilian impact.

Expanded capital routing to civilians fleeing violence or facing humanitarian emergency.

Emergency coordination with humanitarian NGOs and UN agencies (not armed groups).

Documentation of civilian casualties and infrastructure damage for international accountability.

Support for independent journalists and press freedom organizations operating in or reporting on Iran.

Information penetration via all available means (VPN, Tor, satellite internet, mesh networks).

**Operations Prohibited:**

Support for armed opposition groups (MEK or any militia).

Routing to IRGC (designated FTO by U.S.).

Routing to Iranian government entities or sanctioned officials.

Routing to US, Israeli, or any other military forces.

Weapons, dual-use technology, or materials that could support violence.

Coordination with any government seeking regime change (Rampage is humanitarian infrastructure, not geopolitical tool).

**De-escalation Criteria:**

Level 4 → Level 3: Cessation of active combat operations and establishment of ceasefire.

Level 3 → Level 2: Cessation of systematic violence against civilians; humanitarian corridors established; international observers allowed access.

Level 2 → Level 1: No internet shutdowns for 6+ consecutive months; release of political prisoners arrested during protests; demonstrable improvement in press freedom.

## Section 3: Venezuela

**Status: Level 2 Active.**

Authorized operations include capital routing for survival and emigration costs following the validation of the Maduro capture in January 2026.

**Operations Authorized:**

Level 1 (Baseline): Information flow to counter state propaganda; support for independent journalism; monitoring of human rights violations.

Level 2 (Active): Capital routing to civilians for food, medicine, emigration costs; enhanced information penetration; humanitarian coordination with NGOs.

**Operations Prohibited:**

Routing to Maduro government, PDVSA, military, or sanctioned officials.

Support for armed opposition groups.

Political organizing or regime change operations.

**De-escalation Criteria: Level 2→Level 1:**

Healthcare system functional; capital controls lifted; independent journalists can operate without fear; food security restored; refugee flow reversed.

## Section 4: Lebanon

**Status: Level 1-2 (Flexible, crisis-responsive).**

**Operations Authorized:**

Capital routing to bypass failed banking system.

Information flow during communications blackouts.

Humanitarian support for Lebanese citizens and Syrian refugee populations.

Support for independent journalism documenting crisis.

**Operations Prohibited:**

Routing to Hezbollah (designated FTO by U.S. and multiple countries).

Routing to Syrian government entities.

Support for sectarian militias.

**De-escalation Criteria: Level 2→Level 1:**

Banking system functional; government provides basic services; political stability restored; humanitarian conditions improve for Syrian refugees.

## Section 5: Taiwan

**Status: Level 0 (Monitor only); Escalates to Level 2 if communications disrupted; Level 3 if armed conflict.**

**Operations Authorized:**

Level 0: Monitoring only; preparation of crisis response protocols; validator network maintained in region.

Level 2: Information penetration via satellite internet; mesh network infrastructure; capital routing for civilian evacuation if possible.

Level 3: Maximum information flow; capital routing for refugees; emergency humanitarian coordination; documentation of conflict.

**Operations Prohibited:**

Pre-crisis positioning that could be seen as preparing for conflict.

Support for military operations on either side.

Taking sides in PRC-Taiwan sovereignty dispute.

### Section 6: Haiti

**Status: Level 1-2 (Flexible, crisis-responsive).**

**Operations Authorized:**

Information flow during gang-imposed blackouts or state-caused communications disruptions.

Capital routing for humanitarian aid (food, medicine, evacuation from gang-controlled areas).

Support for NGOs providing humanitarian assistance.

Documentation of gang violence and state failure.

**Operations Prohibited:**

Routing to gangs or armed criminal groups.

Support for any armed factions.

Political organizing for any faction.

### Section 7: Addition of New Jurisdictions

Any addition of a new jurisdiction to Article VIII requires activation of the Humanitarian Escalation Protocol (Article VI, Section 4): 75% of total voting power, minimum 50% of all circulating RPM participating, 30-day voting period + 90-day implementation delay, with attached evidence package including multi-source crisis documentation, legal analysis, validator risk assessment, and explicit de-escalation criteria.

Current Jurisdictions: North Korea, Iran (Level 4 — Active Armed Conflict as of February 28, 2026), Venezuela, Lebanon, Taiwan (crisis only), Haiti.

Potential Future Additions (Would require Humanitarian Escalation Protocol): Afghanistan (under Taliban—systematic information suppression, gender apartheid); Myanmar (post-coup—military violence, communications blackouts); Syria (ongoing conflict—multiple humanitarian crises); Sudan (conflict zones—communications blackouts, mass displacement); any other jurisdiction where systematic human rights violations create humanitarian need for Rampage operations.

---

## ARTICLE IX: PROHIBITED ACTIVITIES (Amendable)

Rampage will not, under any circumstances:

### Section 1: Support for Violence

Fund, coordinate with, or provide resources to armed groups (state or non-state) engaged in hostilities.

Provide weapons, ammunition, explosives, or materials that could be used for violence.

Provide dual-use technology or equipment that could be weaponized.

Advocate for, incite, or facilitate violent resistance or armed conflict.

Support military operations of any kind.

Rationale: Rampage's mission is information freedom and humanitarian access. Violence undermines human rights. Rampage will not contribute to violence under any circumstances, regardless of claimed justification.

## Section 2: Service to State Actors

Provide operations, services, or resources to governments.

Provide operations, services, or resources to militaries (any country, any branch).

Provide operations, services, or resources to intelligence agencies (any country).

Accept funding from governments.

Allow governments operational control or veto power over Rampage operations.

## Section 3: Terrorism Financing

Route capital to entities designated as terrorist organizations by UN Security Council.

Route capital to entities designated by multiple major international bodies.

Route capital to entities engaged in systematic violence against civilians.

Knowingly facilitate financing for terrorist activities.

## Section 4: Compromising Validator Safety

Operate in jurisdictions where validator participation creates imminent physical danger without adequate protection.

Publish information that could identify validators in high-risk jurisdictions.

Require validator participation in operations creating unacceptable safety risk.

Continue operations if systematic validator targeting occurs.

## Section 5: Centralizing Control

Allow any single entity to gain operational control.

Eliminate or weaken decentralized governance.

Create mechanisms for unilateral decision-making outside governance.

Accept capture by any actor.

## Section 6: Falsifying Information

Publish unverified claims as verified facts.

Fabricate evidence or sources.

Manipulate verification process for political purposes.

Suppress truth for any reason (political, financial, or otherwise).

## Section 7: Profit Over Mission

Abandon civilians facing human rights crises for financial reasons.

Compromise Constitutional principles to access traditional finance/exchanges.

Accept funding or partnerships requiring mission compromise.

Prioritize token price over humanitarian operations.

# ARTICLE X: AMENDMENT AND INTERPRETATION (Amendable)

## Section 1: Constitutional Structure

**Immutable Core (Articles I-IV):**

Article I: Foundational Principles.

Article II: Legal Framework (core principles).

Article III: Operational Boundaries.

Article IV: Truth Verification Standards.

These articles encode Rampage's values and cannot be amended except as specified in Section 3 (Emergency Legal Compliance—and even then, only for dissolution if compliance conflicts with core principles).

**Amendable Implementation (Articles V-XI):**

Article V: Operational Framework.

Article VI: Governance.

Article VII: Truth Bearer Rights and Responsibilities.

Article VIII: Scenario-Specific Operations.

Article IX: Prohibited Activities.

Article X: Amendment and Interpretation.

Article XI: Dissolution.

These articles describe how Rampage operates and can be amended as needed to adapt to changing circumstances, provided amendments do not violate the Immutable Core.

## Section 2: Standard Amendment Process

Articles V-XI can be amended through the following process:

**Requirements:**

Governance proposal with detailed rationale (minimum 5,000-word justification).

Community discussion period (30 days minimum).

60% quorum of RPM holders.

80% supermajority vote for approval.

Implementation delay (90 days after passage).

**Restrictions:**

Amendments cannot violate Articles I-IV.

Amendments cannot eliminate accountability mechanisms.

Amendments cannot centralize control.

Amendments cannot abandon civilian populations facing Level 2+ crises without documented humanitarian justification.

## Section 3: Emergency Legal Compliance

If binding international legal obligation requires Constitutional adaptation, an expedited process is available:

**When Applicable:**

New international treaty obligations.

International court rulings with binding effect.

Changes to international AML/CFT standards requiring immediate implementation.

UN Security Council resolutions with humanitarian implications.

**Process:**

Emergency governance proposal (documented legal necessity with citation to specific international obligation).

Expedited discussion period (7 days).

40% quorum (lower than standard due to urgency).

75% approval (still requires supermajority).

Changes must be minimum necessary to achieve compliance.

90-day sunset clause.

Critical Limitation: Emergency Legal Compliance cannot amend Articles I-IV under any circumstances. If compliance with international law requires violating these immutable principles, the only Constitutional response is dissolution under Article XI.

### Section 4: Constitutional Interpretation

Conflict Resolution Hierarchy: When Constitutional principles conflict, priority order is:

1. Human Rights Primacy (Article I)—Highest priority.
2. Validator Safety (Article VII, Article II Section 6)—People over mission.
3. Truth Verification Integrity (Article IV)—Integrity of information is foundational.
4. Operational Boundaries (Article III)—Prevent mission compromise.
5. Specific operational provisions (Articles V-IX)—Lowest priority.

---

## ARTICLE XI: DISSOLUTION (Amendable)

### Section 1: Mission Failure Conditions

Rampage ceases operations if any of the following occur and cannot be remedied: Capture by State Actor; Validator Safety Failure; Truth Verification Corruption; Constitutional Violation; Technical Failure. See original Constitution v1.4 for full definitions of each condition.

### Section 2: Dissolution Process

Governance Vote Required: Proposal documenting which dissolution condition(s) are met; 30-day community discussion; 60% quorum; 80% supermajority for dissolution.

**Asset Distribution:**

Electronic Frontier Foundation (EFF): 25%.

Amnesty International: 25%.

Reporters Without Borders (RSF): 25%.

Human Rights Watch: 25%.

Distribution occurs in stablecoins or liquid assets. Governance may adjust recipient list by 67% vote if any organization ceases to exist, loses nonprofit status, or is found to have compromised its mission.

**Knowledge Preservation:**

All code open-sourced under GPL v3 license.

All documentation made publicly available.

All learnings and post-mortems published.

Verification methodology documented comprehensively.

### Section 3: Dissolution Philosophy

Better to cease existing than to exist in contradiction to founding principles. If Rampage can no longer uphold human rights without compromise, it should not exist. Dissolution with dignity is preferable to continued operation without integrity.

---

## CLOSING STATEMENT

This Constitution is a declaration of values, a legal framework, and a commitment to human dignity.

Rampage exists because human rights are universal, governments frequently violate them, and technology can enable individuals to exercise rights their governments deny. This is civil infrastructure for human rights—built on transparency, accountability, and principled commitment to truth.

We acknowledge limits and risks: Rampage does not claim legal immunity. Rampage cannot eliminate risk for validators. Rampage cannot solve political problems through technology alone. Rampage accepts that upholding human rights may require accepting legal consequences.

We commit to principles: Nonviolence always. Civilians over states. Truth over narrative. Accountability with transparency. Safety for those who serve this mission.

To the Truth Bearers who will risk prosecution to uphold these principles: You continue a tradition of principled resistance to injustice—the Underground Railroad, the Pentagon Papers, Solidarność, the Arab Spring. History remembers those who stood for human dignity when powerful institutions opposed them. Rampage provides infrastructure, legal defense, and community—but cannot eliminate risk. Your participation is voluntary, informed, and honored.

To the civilians who will use Rampage to access truth and exercise economic freedom: This infrastructure exists because you deserve information, resources, and the ability to survive and escape oppression. Your rights are not granted by governments; they are inherent to your humanity.

To the governments who will oppose Rampage: We respect legitimate regulatory functions—preventing terrorism, combating money laundering, maintaining international peace. We cooperate where cooperation serves human rights. But we will not accept your authority to censor truth, imprison populations economically, or suppress fundamental human rights. Where you violate your obligations under international human rights law, we provide infrastructure for civilians to exercise the rights you deny them.

To the international community: Rampage operates under international human rights law. We acknowledge this is contested. We proceed with humility, accountability, and commitment to humanitarian principles.

**Rampage is not perfect. But Rampage is necessary.**

**Rampage is truth. Rampage is freedom. Rampage is human dignity encoded in decentralized infrastructure—built to last, built to serve, built to honor the fundamental rights of every human being.**

This is our Constitution. These are our principles. This is our mission.

---

## AMENDMENT HISTORY

Amendment No. 1 (December 2, 2025): 95/5 Operational Split. Codified the allocation of 95% resources to journalism/verification and 5% to humanitarian response. (Article V, Section 1.1.)

Amendment No. 2 (January 17, 2026): Truth Bearer Designation. Established validator requirements, staking mechanisms, and governance participation rights. (Article VII.)

Amendment No. 3 (January 18, 2026): Data Protection and Privacy Framework. Created Article V, Section 5: Data Protection and Privacy.

Amendment No. 4 (January 18, 2026): Regulatory Classification and Compliance. Created Article II, Section 7: Regulatory Classification and Compliance.

Amendment No. 5 (January 18, 2026): Enhanced Internal Controls and Governance Documentation. Created Article VI, Section 5: Internal Controls and Compliance Framework.

Amendment No. 6 (January 18, 2026): Enhanced AML/CFT Documentation. Added the Enhanced Due Diligence requirement to Article V, Section 4: Capital Routing Framework.

Amendment No. 7 (February 27, 2026): Strategic Validator Agreement Framework. Added Sections 7.4 through 7.7 to Article VII, establishing authority to execute Strategic Validator Agreements during the Pre-Mainnet Phase with reduced staking thresholds for mission-aligned institutional partners, subject to constitutional safeguards and sunset provisions. Incorporates supermajority extension mechanics, transition standards for SVA validators, and institutional eligibility guidance per Perplexity constitutional review.

*Note: Articles I-IV remain immutable and cannot be amended under any circumstances per Article X, Section 2. All amendments apply only to Articles V-XI.*

---

## RATIFICATION — VERSION 1.5

This Constitution, Version 1.5, incorporating Amendments 1 through 7, is ratified and effective as of February 27, 2026.

**Shea Patrick Kastl**

Founder, Rampage Constitutional Journalism Network

Date: February 27, 2026