Limits & Exclusions

What ETHRAEON is NOT—critical boundaries for institutional clarity

⚠️ Critical Disclaimer

ETHRAEON is governance infrastructure, not operational software.
Understanding what we do NOT provide is essential to avoid misalignment and ensure successful deployment.

NOT a Data Storage Platform

What ETHRAEON Does: Stores cryptographic hashes and evidence metadata (who, what, when, authority).

What ETHRAEON Does NOT Do: Store operational data like financial transaction details, full documents, or large media files.

Example (Humanitarian Aid)

- ✅ **ETHRAEON Stores:** "Aid package WFP-2026-1543 entered Lviv border at 2026-01-04T14:23Z, authorized by Customs Officer #4271, hash: a7f3c8d9..."

- ❌ **ETHRAEON Does NOT Store:** Full aid package manifest (100-page PDF), photos of supplies, customs forms

- 💡 **Reality:** Operational systems (WFP SCOPE, Customs ERP) store full data. ETHRAEON stores hash proving data integrity.

NOT a Blockchain

What ETHRAEON Does: Creates append-only evidence chains with cryptographic integrity.

What ETHRAEON Does NOT Do: Require decentralized consensus, mining, or tokens. No cryptocurrency involved.

Why This Matters

- **Trust Model:** ETHRAEON trusts authorized government actors (ministries, agencies). Blockchain assumes zero trust.

- **Performance:** ETHRAEON processes evidence nodes in milliseconds. Public blockchains are slow (minutes to hours).

- **Legal Standing:** Government signatures are legally binding. Blockchain consensus has unclear legal status in most jurisdictions.

NOT a Replacement for Existing Systems

What ETHRAEON Does: Integrates with existing systems via APIs to emit evidence nodes.

What ETHRAEON Does NOT Do: Replace ministry ERP systems, financial software, logistics platforms, or case management tools.

NOT an AI or Machine Learning System

What ETHRAEON Does: Deterministic rule-based validation (e.g., "If payment exceeds budget by >5%, flag for review").

What ETHRAEON Does NOT Do: Use AI for decision-making, predictive analytics, or pattern recognition (unless explicitly contracted as add-on).

Why No AI by Default

- **Explainability:** AI decisions are often opaque. Governance requires transparent, auditable logic.

- **Accountability:** "The AI flagged this" is not acceptable justification for government action. Humans must own decisions.

- **Bias Risk:** AI trained on historical data can perpetuate discrimination. Constitutional controls require explicit rules.

NOT a Decision-Making Tool

What ETHRAEON Does: Provides evidence for humans to make decisions (e.g., "Contractor X has failed 3 past projects").

What ETHRAEON Does NOT Do: Automatically reject bids, deny benefits, or allocate budgets. Humans retain authority.

Example (Contractor Verification)

- ✅ **ETHRAEON Action:** Flags contractor with 3 past failures, presents evidence to procurement officer

- ❌ **ETHRAEON Does NOT:** Automatically reject contractor's bid (officer must review and decide)

- 💡 **Accountability Preserved:** Officer is responsible for decision, ETHRAEON proves what evidence was available at decision time

NOT a Real-Time Operational System

What ETHRAEON Does: Processes evidence nodes typically within seconds to minutes.

What ETHRAEON Does NOT Do: Operate at millisecond latency required for high-frequency trading or emergency dispatch systems.

⚠️ Performance Expectations

If your use case requires sub-100ms response times (e.g., border gate opens/closes based on instant verification), ETHRAEON's evidence emission happens *after* the operational decision, not during. We document what happened, we don't control real-time gates.

NOT a Cyber Defense System

What ETHRAEON Does: Detects unauthorized changes to evidence after-the-fact (tamper-evidence).

What ETHRAEON Does NOT Do: Prevent cyberattacks, block malware, or secure networks. Standard cybersecurity measures still required.

Security Responsibility

- **ETHRAEON Provides:** Cryptographic integrity of evidence (proves if data was altered)

- **Client Provides:** Network security, access controls, firewall, intrusion detection

- **Shared Responsibility:** ETHRAEON secures evidence layer, client secures infrastructure layer

NOT a Legal Compliance Guarantee

What ETHRAEON Does: Provides tools to document compliance (evidence chains, audit trails, constitutional controls).

What ETHRAEON Does NOT Do: Guarantee legal compliance—clients remain responsible for following applicable laws.

🔴 Legal Disclaimer

ETHRAEON evidence infrastructure supports compliance efforts but does not constitute legal advice or replace legal review. Clients must ensure their use of ETHRAEON aligns with national laws, donor agreements, and international obligations.

NOT Infinitely Scalable (Yet)

Current Capacity: Designed for government-scale operations (millions of evidence nodes per year).

Known Limits: Systems handling billions of transactions per day (e.g., payment networks) may require custom architecture.

Scalability Benchmarks

- ✅ **Well-Suited:** National procurement systems, humanitarian aid tracking, reconstruction oversight (10K-1M nodes/month)

- ⚠️ **Requires Planning:** Cross-border trade (100M+ shipments/year), high-volume financial transactions

- ❌ **Not Suitable:** Consumer IoT (billions of sensor readings/day), social media (billions of posts/day)

NOT a Magic Solution

Reality Check: ETHRAEON makes governance violations *evident*, not impossible. Determined bad actors can still commit fraud—but they cannot hide it.

What ETHRAEON Changes

- **Before ETHRAEON:** Fraud is discovered months/years later (if ever), evidence destroyed or altered, accountability unclear

- **With ETHRAEON:** Fraud leaves cryptographic traces, evidence is tamper-evident, investigators have clear audit trails

- **Net Effect:** Increased deterrence (bad actors know they'll leave evidence) +

faster detection + stronger prosecution

Excluded Use Cases

ETHRAEON is **intentionally NOT designed for:**

- Consumer-facing applications (use Diia, not ETHRAEON)

- Private sector internal operations (unless government oversight involved)

- Military operational systems (command & control, targeting—requires different security model)

- Intelligence gathering (ETHRAEON creates audit trails, incompatible with covert operations)

- Personal data storage (ETHRAEON stores hashes, not raw personal data)

When to Choose ETHRAEON

ETHRAEON is the right solution when:

- Institutional accountability is critical (government procurement, aid distribution, fund oversight)

- Evidence must survive years of scrutiny (war crimes, reconstruction audits, donor reporting)

- Multiple agencies must trust shared data (cross-agency synchronization)

- Transparency is required WITHOUT exposing operational details (public accountability, privacy protection)

- Constitutional rules must be enforced computationally (T3-T5 constraints)

Contact for Boundary Questions

If your use case is unclear (might be in scope, might not), contact us at **inquiry@ethraeon.systems** with:

1. Brief description of operational context (which agencies, what processes)

2. Governance challenge you're trying to solve

3. Why existing systems are insufficient

4. Expected evidence volume (nodes per month/year)

We'll provide honest assessment within 48 hours: "ETHRAEON fits" / "Alternate solution recommended" / "Requires custom architecture discussion"

Disclaimer: This document outlines technical and operational boundaries. It does not constitute legal advice or warranty. Consult legal counsel for compliance questions.