

# AEP-007

# Public-Safe Proof Report Standard

Public proof without private leakage

Version 1.2 Institutional Edition · Proof Gradient / Agent Evolution Protocol

The graphic features a dark blue background with a fingerprint-like pattern. At the top left, it reads 'AEP-007 v1.2' in yellow and 'Public-Safe Proof Report' in white. Below this is the subtitle 'Public proof without private leakage'. A central horizontal flow consists of seven rounded rectangular boxes, each containing a step name and a brief description: 'Private Evidence' (dockets + packets), 'Disclosure Review' (classify), 'Redaction Ledger' (remove risk), 'Claim Boundary' (limit claims), 'Approval' (publish), 'Public Report' (share), and 'Correction' (maintain trust). Below the flow are two rows of white rounded rectangular boxes with black text: the first row contains 'CLAIM BOUNDARY', 'REDACTION REVIEW', 'NO PRIVATE TRACE', and 'APPROVAL REQUIRED'; the second row contains 'CORRECTION HISTORY', 'PUBLIC HASH', 'CHALLENGE WINDOW', and 'ACCESSIBILITY'. At the bottom, a yellow text line states: 'AEP-007 converts private evidence into public-safe, claim-bounded proof.'

**AEP-007 defines the public proof. GoalOS proves publicly without leaking privately.**

## 1. Abstract

AEP-007 defines the Public-Safe Proof Report Standard: the reporting layer that converts private or protected machine-work evidence into a public-safe proof report that can be shared without leaking private or protected material.

## 2. Canonical Law

**No public claim without claim boundary.**

**No public proof without redaction review.**

**No private trace in public report.**

**No protected data in public proof.**

**No publication without approval.**

**No correction without history.**

**No proof, no evolution.**

## 3. v1.2 Upgrades

- Disclosure review objects
- Challenge records
- Retraction notices
- Report bundles
- Embargo / responsible disclosure controls
- Public claim levels
- Accessibility profile
- Proof Card profile
- Leakage audit tooling

## 4. Disclosure Classes

# Disclosure Classification

Public reports must preserve trust without exposing private or protected material

### **PUBLIC**

#### **safe to publish**

claims, summaries, public links

### **PRIVATE**

#### **internal only**

prompts, traces, tool logs

### **PROTECTED**

#### **restricted access**

secrets, regulated data, vulnerabilities

### **FORBIDDEN**

#### **never publish**

credentials, raw personal data, restricted de

### **EMBARGOED**

#### **delay publication**

responsible disclosure / timed release

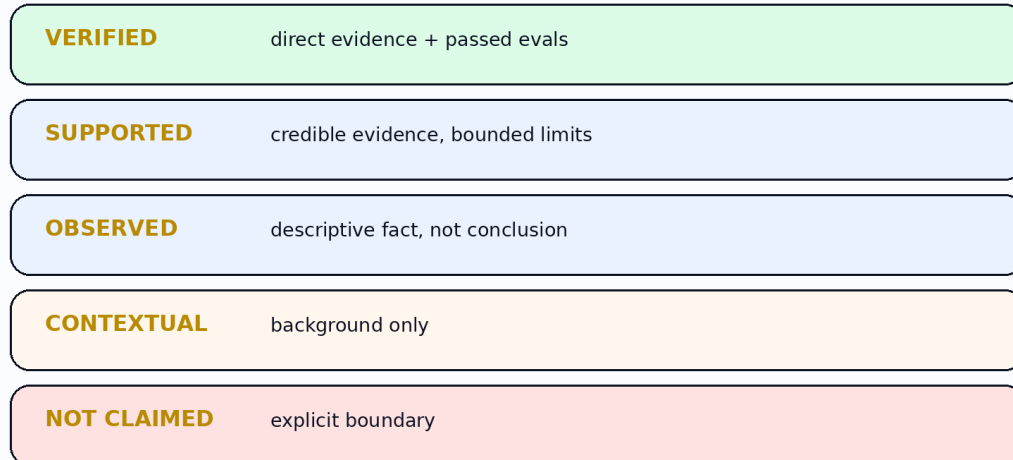
**Invariant: public proof may prove accountability, not leak sensitive intelligence.**

Class	Meaning
public	Safe to publish.
private	Internal only.
protected	Restricted to authorized roles.
forbidden	Never publish.
embargoed	Not yet publishable.

## 5. Public Claim Levels

### Claim Boundary Ladder

A public report must distinguish verified, supported, observed, contextual, and not claimed



**Public trust improves when the report says exactly what the evidence does and does not prove.**

## 6. Required Report Sections

- Report Manifest
- Source Evidence References
- Public Claim Matrix
- Evidence Summary
- Evaluation Summary
- Risk and Limitation Summary
- Rollback / Recovery Summary
- Redaction Ledger
- Publication Approval
- Correction and Retraction Policy
- Public Artifact Links
- Final Claim Boundary

## 7. Lifecycle



## 8. Zero-Leak Invariants

- No raw private prompts in public report.
- No raw private traces in public report.
- No secrets, keys, credentials, or tokens in public report.
- No regulated personal data by default.
- No exploit details without responsible disclosure review.
- No unsupported claim in public report.
- No publication without approval.
- Under uncertainty, redact or withhold.

## 9. Conformance Levels

Level	Requirement
Level 0	Informal public proof with claim boundary.
Level 1	Basic report with manifest, claim matrix, evidence summary, limitations, and claim boundary.
Level 2	Reviewed report with redaction ledger and publication approval.
Level 3	Operational report with source docket refs, ProofPacket refs, eval summary, rollback summary, correction policy, and public artifact links.
Level 4	Institutional report with disclosure review, redaction audit, challenge window, correction/retraction history, report hash, and audit export.
Level 5	Sovereign / regulated report with jurisdiction, retention, protected-boundary review, responsible disclosure controls, authorized approvers, challenge/retraction governance, accessibility profile, and machine-readable bundle.

## 10. Claim Boundary

AEP-007 does not claim achieved AGI, achieved ASI, perfect safety, legal compliance certification, financial or legal advice, guaranteed ROI, production readiness, government endorsement, or national-security readiness. AEP-007 defines a public-safe proof reporting standard.

**GoalOS proves publicly without leaking privately.**