ARCS Automated Record Custody Standard

Positioning Quick Reference

v1.0 | arcsstandard.org

Vega Commons Project, Inc.
info@arcsstandard.org

AI interaction records are a distinct governance object class requiring lifecycle governance: custody chain, retention, deletion, and production readiness. ARCS occupies a layer beneath all existing frameworks (privacy, security, safety, content standards) by asking the prior question every other framework assumes away: does the record exist, who controls it, and can it be compelled?

Where ARCS Sits: The Governance Stack

Layer	Scope	Current Coverage
A	Runtime and model security	Active development
B	Authorization, delegation, identity	Active development
C	Verifiable execution proofs	Active development
D	**Interaction record lifecycle**	**ARCS (sole published standard)**

A lifecycle boundary exists at the point where ephemeral runtime artifacts become persistent records. After that transition, record governance questions arise independently of the runtime protocol that produced the artifact.

Custody vs. Privacy

Privacy governs who may access existing records. Custody governs whether records exist on reachable infrastructure in retained form and under what lifecycle controls. Enterprise terms, access controls, encryption, and data classification govern access. They do not determine whether records are created, how long they persist, where copies propagate, or what production posture attaches once they do.

Record existence Which interaction records are retained on reachable infrastructure

Custody posture Which entities hold records, under what authority, and with what obligations

Preservation state What retention, hold, or deletion requirements apply at each custody node

Production readiness Whether records can be identified, collected, reviewed, and produced if required

The Protocol Stack

MCP governs action.

x402 governs value.

ARCS governs the records.

Doctrinal Anchor

United States v. Heppner, No. 25 Cr. 503 (JSR)

(S.D.N.Y. Feb. 2026, Judge Rakoff)

Federal criminal matter in which the defendant used consumer Claude after receiving a grand jury subpoena. The court denied privilege and work product protection for the resulting interaction records. Establishes the floor: AI interaction records are discoverable electronically stored information. No privilege protection attaches merely because the operator used an AI system to reason through a problem.

Adjacent Frameworks: What Each Governs

Domain	What It Governs
Privacy (GDPR, CCPA)	Access controls, consent, and processing restrictions for existing data
Security (800-53, ISO 27001)	Protection of systems, networks, infrastructure, and accounts from unauthorized access or misuse
Safety (AI RMF, EU AI Act)	Model behavior, output quality, alignment, and harm mitigation
Content Provenance (C2PA)	Authentication and attribution of media and generated outputs
Records Management (ISO 15489)	General records lifecycle; does not address automated interaction records or multi-vendor custody fragmentation
AI Management (ISO 42001)	Organizational controls for AI systems; does not reach record-level governance
SOC 2	Service organization controls; does not address interaction record lifecycle
MCP / A2A	Runtime interaction among models, tools, resources, and services; does not govern records after creation
ARCS	**Lifecycle governance for interaction records: existence, custody, preservation, deletion, transfer, and production readiness**

An organization may be fully compliant with every framework listed here and still have no governance posture for interaction records. ARCS addresses that gap.

What ARCS Does Not Govern

- Model safety, training data, algorithm design, output quality, bias, or fairness
- Privacy law compliance, data protection impact assessments, or consent management
- Information security certification, red-teaming, or adversarial testing
- Privilege doctrine, substantive discovery law, or insurance coverage terms
- Content moderation policy or model documentation requirements

What ARCS Requires

- That retention decisions are explicit, documented, auditable, and architecture-aware
- That the custody surface is mapped: every entity that holds records, under what authority
- That preservation posture can override routine deletion when required
- That non-creation or non-retention claims are auditable, not assumed
- That governance treatment is disclosed, not inferred from vendor policy language

Regulatory Record

VCP filed formal comments on NIST Docket NIST-2025-0035 (March 9, 2026) and the NCCoE AI Agent Identity and Authorization concept paper (April 2, 2026). Among 529 reviewed comments on the CAISI docket, VCP is the sole commenter addressing interaction-record lifecycle governance as a distinct governance layer.