ARCS

Automated Record Custody Standard

Version 1.0 · April 2026

Published by Vega Commons Project, Inc.

arcsstandard.org

ARCS defines governance controls for the lifecycle, custody, retention, preservation, and deletion of interaction records generated by automated systems during human-directed operation.

92 controls across 10 control families. Applicable to operators using automated systems in contexts where interaction records may become reviewable, preservable, or producible.

> This document contains the Core Standard text. Individual control statements are maintained in the companion Controls Catalog.

Publication Notice

Automated Record Custody Standard (ARCS), Version 1.0, April 2026. Published by Vega Commons Project, Inc. This edition supersedes prior draft versions.

Trademark

ARCS and Automated Record Custody Standard are trademarks of Vega Commons Project, Inc. (USPTO Serial No. 99740988). Use of the ARCS name and mark is governed by the ARCS Trademark Policy, available at arcsstandard.org.

Document Use

This document may be reproduced and distributed subject to the ARCS Document Use Policy, available at arcsstandard.org/legal. Conformance claims referencing this standard must cite the specific version number.

Canonical Publication

The canonical publication of this standard is maintained at arcsstandard.org. In the event of any discrepancy between this document and the canonical publication, the canonical publication controls.

Contents

Rationale

Automated systems that accept natural language instructions and execute multi-step tasks generate a category of records that existing governance frameworks do not address. When an operator uses such a system to plan, research, decide, or act, the system creates logs containing the operator's initial problem framing, iterative instruction refinement, abandoned approaches, intermediate reasoning, delegated intent, authorization constraints, and tool-call execution history. These records capture not only what was done but why it was done, how alternatives were evaluated, and what was rejected.

This record category has three properties that distinguish it from conventional system logs. First, the records are generated as a condition of system operation, not as a deliberate act of publication by the operator. Second, the records reconstruct the cognitive process through which downstream actions were selected, making them functionally equivalent to work product or deliberative memoranda in contexts where no formal privilege applies. Third, the records are retained by default on centralized infrastructure controlled by the platform vendor, not the operator.

Existing governance frameworks address adjacent concerns but do not address this one. NIST SP 800-53 governs security controls for information systems. The NIST AI Risk Management Framework governs risk identification and mitigation. ISO 42001 governs AI management systems. SOC 2 governs security controls for service organizations. The EU AI Act imposes transparency and logging obligations on high-risk systems. None of these frameworks specifies controls for the retention, custody, or discoverability of records generated during automated interactions. The result is that organizations deploying automated systems have no standard against which to assess, document, or audit the record governance posture of those deployments.

The gap has operational consequences. Federal courts have treated AI interaction logs as ordinary electronically stored information subject to routine discovery. Platforms retain these records by default under terms that vary by deployment mode, subscription tier, and configuration. Enterprise customers with sufficient bargaining position negotiate contractual non-retention protections. Individual operators and smaller organizations do not. The resulting regime is structurally uneven: the same category of records receives different treatment based on the operator's commercial relationship with the platform, not on any governance principle.

ARCS addresses this gap. It defines governance controls for the lifecycle, custody, retention, preservation, and deletion of interaction records generated by automated systems. It does not require non-retention. It requires that retention decisions are explicit, documented, auditable, and architecture-aware. An implementation that retains all interaction records may conform to ARCS if the retention is documented, the custody surface is mapped, and the governance controls are operational.

The ARCS governance model is organized around five core objects: classification of interaction records by category, custody assignment identifying which entities hold records and on what surfaces, retention posture defining how long records persist and under what conditions, propagation governing how records move across system and vendor boundaries, and attestation providing verifiable evidence that governance controls were applied. These five objects constitute the minimum governance spine for any deployment.

The risk addressed by ARCS is not limited to data collection, but arises from the existence, retention, and propagation of automated interaction records across modern software systems.

1. Scope

ARCS defines governance controls for the lifecycle, custody, retention, preservation, and deletion of interaction records generated by automated systems during human-directed operation.

1.1 Covered Systems

This standard applies to AI assistants and AI agents, AI-enabled productivity software, ambient AI features embedded in enterprise software, API-based automated systems, multi-step automated pipelines, conversational AI systems, agent and toolchain-integrated systems, review and feedback and evaluation pipelines, and any other system that generates, retains, or derives artifacts from human-directed interaction where those artifacts may be subject to legal compulsion, regulatory inquiry, or preservation demand.

1.2 Applicability

ARCS obligations arise when an operator uses an automated system that generates interaction records. Applicability includes any context in which interaction records may be subject to discovery, subpoena, preservation demand, regulatory inquiry, audit, or internal investigation. An operator need not be involved in active litigation for ARCS to apply.

1.3 Non-Scope

ARCS does not govern model safety, training data, algorithm design, output quality, bias, fairness, or system behavior. Those properties are governed by separate frameworks. ARCS governs only the lifecycle and custody of records created during system use. Compliance with ARCS does not substitute for compliance with applicable data protection, security, records management, or sector-specific regulations.

2. Normative References

The key words SHALL, SHALL NOT, MUST, MUST NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL in this standard are to be interpreted as described in IETF RFC 2119 and BCP 14.

This standard may be used with, but does not replace, the following frameworks. ARCS defines a distinct governance domain for interaction records that no current framework addresses.

Framework	What It Governs	ARCS Relationship
NIST SP 800-53	Security controls for information systems	ARCS extends to lifecycle and custody of interaction records
NIST AI RMF	AI risk, bias, safety, transparency	ARCS governs records created by AI systems
ISO 27001	Information security management	ARCS complements by addressing record lifecycle
ISO 42001	AI management systems	ARCS provides record-level governance that organizational controls do not reach
GDPR / CCPA	Personal data protection	ARCS addresses custody and preservation obligations independently of data classification
EU AI Act	High-risk AI logging obligations	EU AI Act requires log creation; ARCS governs what happens to those logs after creation
SOC 2	Service organization controls	ARCS custody and lifecycle controls may inform SOC 2 evidence
MCP / A2A	Agent-to-tool and agent-to-agent protocols	MCP defines how context flows; ARCS governs records created as a result

3. Terms and Definitions

The following terms are defined for use throughout ARCS. Defined terms appear in ordinary text; no special formatting is required once defined here.

3.1 Core Record Concepts

Term	Definition
Interaction Record	Any artifact created, retained, transmitted, or derived by an automated system during or as a result of human-directed use, including artifacts held by the operator or by any vendor within the custody surface.
Record Surface	The complete set of locations where interaction records may exist. Includes provider systems, tenant systems, local storage, integrations, backups, archives, review datasets, and derived records.
Derived Record	Any artifact created outside the original system as a result of an interaction. Includes copied text, downloaded files, generated documents, stored notes, tickets, filings, emails, and database entries.
Intermediate Record	An artifact created during system processing that is not directly visible to the user. Includes agent traces, tool call logs, retrieval queries, system prompts, and runtime state.
Material Record	Any interaction record reasonably likely to be relevant in discovery, audit, or governance review.
Deliberative Content	Content that consists of, reflects, or is derived from an operator's, user's, or agent's reasoning process. Includes questions asked, options considered, arguments explored, conclusions reached or abandoned, and provisional assessments subsequently revised. Deliberative content is the governance-sensitive axis distinguishing records that require heightened lifecycle controls from operational telemetry.
Deliberative Record	An interaction record whose content is predominantly deliberative as defined in this section. Deliberative records include records where the operator's, user's, or agent's reasoning process constitutes the substantive content, as distinguished from operational telemetry, transactional metadata, or exported outputs. Deliberative records carry the highest governance sensitivity under ARCS-TAX and are the primary subject of content-telemetry separation.
Record Class	A category of interaction record distinguished by its creation trigger, content type, retention behavior, or governance treatment. Record classes include, without limitation: prompt/input text, model output, system prompt, feedback submission, review copy, training derivative, safety flag, telemetry event, agent trace, tool call artifact, and operational log. Record classes are the unit of analysis for retention configuration, non-creation claims, and taxonomy controls under ARCS-TAX. A non-creation claim under ARCS-NCR is made per record class, not per system.
Residual Artifact	Any record created by a system notwithstanding a non-creation claim for a different record class. Residual artifacts for a non-creation deployment may include session identifiers, timestamps, connection metadata, operational logs, receipt hashes, billing records, network routing metadata, and any other records generated by the interaction that are not within the non-created class. Each residual artifact class is documented and governed per its applicable retention and deletion controls.

3.2 Surface Concepts

Term	Definition
Custody Surface	The complete set of systems, vendors, and storage locations where copies of interaction records may exist, including primary stores, backups, logs, caches, safety pipelines, analytics systems, training pipelines, and vendor-held copies.
Discovery Surface	The subset of the record surface reasonably susceptible to legal production. Includes records reachable through user possession, provider logs, vendor storage, backups, review datasets, or derived documents.
Review Surface	The set of systems in which interaction records may be accessed by humans other than the user. Includes safety review, support, evaluation, moderation, and feedback review.
Unknown Surface	Any portion of the record or custody surface that cannot be conclusively documented due to architectural uncertainty, third-party opacity, or system complexity.
Record Acquisition Modality	A pathway through which interaction records may become reachable by a party other than the originating user, including civil subpoena, regulatory examination, internal review, provider safety or moderation review, government purchase through commercial intermediaries, or national security process.
Automated Record Custody Gap	The condition arising when automated processing creates interaction records that travel farther, persist longer, or become more reachable than the responsible actor understands at the time of record creation.
Surface Map	A versioned document identifying every known location where interaction records may exist (record surface map) or every entity that possesses, controls, or can access interaction records (custody surface map). Surface maps are the primary governance deliverable for ARCS-CUS and ARCS-LIF and SHALL conform to the minimum schemas defined in Standard Annexes C and D.
Backup	A copy of interaction records created for disaster recovery, business continuity, or operational resilience purposes. Backups extend the custody surface and may persist beyond the retention period applied to primary copies.
Cache	A temporary copy of interaction records or record components maintained for performance, availability, or operational efficiency. Caches extend the custody surface and may retain record content beyond the intended retention window.
Archive	A copy of interaction records placed in long-term storage for compliance, business continuity, or institutional retention purposes. Archives extend the custody surface and may persist indefinitely beyond the retention period applied to operational copies.

Term	Definition
Custody Chain	The sequence of entities through which an interaction record passes or in which copies exist, from creation through final deletion or archival. In multi-vendor and delegation contexts, the custody chain may fragment across multiple independent systems. The custody chain is distinct from the custody surface: the surface identifies who currently holds records; the chain identifies how records moved between holders over time.

3.3 Lifecycle Concepts

Term	Definition
Interaction Lifecycle	The complete sequence of record creation, transmission, storage, review, routing, export, backup, deletion, preservation, and downstream propagation.
Default Retention Posture	The record categories, retention durations, and deletion behaviors that apply in ordinary system operation, in the absence of any legal hold, preservation demand, or regulatory inquiry.
Preservation Posture	The operational state that applies when litigation is pending or anticipated, a preservation demand has been received, a regulatory inquiry has been initiated, or an internal investigation has been opened. Routine deletion may be suspended.
Feedback Routing	Any event that moves an interaction record into a different system, lifecycle, or retention regime. Includes thumbs-up/down, flagging, sampling for review, export, or forwarding to abuse monitoring.
Retention	The period during which an interaction record is preserved in accessible form, whether by default configuration, user control, or system policy.
Deletion	The removal of an interaction record from accessible storage. Does not guarantee physical erasure from all backup, cache, or archive media.
Preservation Override	A condition in which deletion or retention settings are suspended due to legal or regulatory requirements. Includes legal hold, litigation hold, and regulatory preservation notice.
Lifecycle Boundary	The point at which a runtime artifact transitions from an ephemeral operational state to a governed record subject to retention, preservation, and disposition controls. Lifecycle boundary events include: persistence to durable storage, transmission to another system or vendor, survival beyond session termination, capture by a monitoring, telemetry, or audit system, and incorporation into secondary datasets including training data, retrieval indices, vector databases, or derived analytics.
Session	A bounded period of interaction between a user or agent and an automated system. A session begins when the system is engaged and ends when the interaction terminates, times out, or is explicitly closed.
Session Boundary	The defined point at which an interaction session terminates and session-scoped state is released. In non-creation configurations, the session boundary defines when in-memory processing state ceases to exist.
Ephemeral	A retention classification applied to records that SHALL not persist beyond the session in which they are created. Ephemeral records are deleted or discarded at session termination.

Term	Definition
Governed Persistence	A retention class applicable to agent memory stores that must survive across sessions to serve their operational purpose. A memory store classified as governed persistence is retained on operator-controlled infrastructure, subject to a defined maximum retention period with automatic purge, excluded from uncontrolled backup or synchronization, and subject to preservation override.
Legal Hold	A specific form of preservation override triggered by pending or reasonably anticipated litigation, regulatory inquiry, or internal investigation. A legal hold suspends routine deletion for records within scope.
Differential Retention	The application of different retention classes to different artifact types within a single interaction session.
Retention Class	A category of retention treatment applied to a record class or artifact class. The retention classes defined in this standard are: ephemeral, session-bounded, governed persistence, and durable.

3.4 Configuration and Deployment Concepts

Term	Definition
Deployment Mode	A distinct configuration of the system that affects record behavior. Includes consumer interface, enterprise deployment, API deployment, reduced-retention mode, non-creation configuration, agent runtime, multi-vendor workflow, and plugin or toolchain integration.
Reduced-Retention Configuration	A deployment mode intended to limit retention, logging, or review. Includes temporary mode, history-off, zero-data-retention (ZDR), or enterprise-controlled retention. A reduced-retention configuration creates records and then limits their persistence through policy, time-based deletion, or user control. An operator SHALL not describe a non-creation deployment as reduced-retention, or a reduced-retention deployment as non-creation, in any conformance statement, audit evidence, or legal submission.
Non-Creation Configuration	A deployment mode in which one or more material record classes are prevented from existing by architectural design rather than by retention policy or deletion procedure. Non-creation is a per-class architectural claim, not a system-wide absence claim.
Publish Boundary	The point at which an interaction record leaves the governed environment and is transmitted to an external recipient or system. In a non-creation configuration, the publish boundary defines the scope of the non-creation claim.
Multi-Vendor Workflow	An interaction that creates records in more than one system operated by different entities. Includes API chaining, tool integration, plugin execution, and federated agent systems.
Governance Declaration	A document provided by a vendor describing its retention behavior, preservation capability, discovery exposure, deletion verifiability, and custody surface for interaction records processed on its infrastructure.
Configuration Exposure	The set of record-behavior differences that result from changes in deployment mode, user settings, or system configuration. A configuration change may create, suppress, extend, or shorten record retention without the operator's awareness.

3.5 Agent and Runtime Concepts

Term	Definition
Agent Runtime	The execution environment in which autonomous or semi-autonomous AI agents operate. Includes multi-turn planning, tool execution, persistent memory, and delegation across models or systems.
Runtime Component	A distinct module within an agent runtime that generates, processes, or stores interaction records as part of its operation.
Autonomous Execution	AI system operation that proceeds without direct human initiation for each action. Includes scheduled tasks, continuous monitoring, multi-step workflows, and background processing.
Delegation Chain	A sequence of interactions where one AI system invokes another, either within the same provider or across vendors. Includes tool calls, API chaining, and agent-to-agent handoff.
Tool Call	An invocation by an AI system of an external function, API, database query, file operation, or integrated service during interaction processing.
Persistent Memory	Information retained by an AI system across interaction sessions and accessible in subsequent interactions. Subject to record surface mapping and discovery surface assessment. Persistent memory constitutes an interaction record regardless of whether the user can view or delete it.
Conference Runtime	An execution environment in which multiple agents participate in a shared session, coordinated runtime, or joint processing context.
Trace	A record of the sequential steps, decisions, state transitions, or reasoning paths taken by an automated system during processing. Traces are the primary artifact class through which agent runtime behavior becomes documentable.
Planning Trace	An agent's representation of its intended execution path, including task decomposition, step ordering, alternative approaches considered, and reasoning about which path to pursue. Planning traces are deliberative records and are classified as ephemeral by default under AGT-04.
Execution Trace	The sequence of steps, decisions, tool invocations, and state transitions executed by an agent during a session. Structural metadata is operational telemetry; the reasoning or content that drove each decision is deliberative.
Artifact Class	A category of agent runtime artifact defined by its function and governance characteristics. The artifact classes defined in this standard are: planning trace, tool call artifact, intermediate result, execution trace, error recovery artifact, session state artifact, and security-sensitive tool output.
System Prompt	An instruction set provided to an automated system that configures its behavior for a given deployment, session, or interaction. System prompts are identified as a record class subject to assessment and may constitute delegation artifacts.

Term	Definition
Retained Deliverable	An output of an agentic workflow expressly designated by the operator for persistent retention. Distinguished from ephemeral intermediate results by explicit designation.
Delegation Artifact	Any record encoding the scope, duration, or conditions of authority delegated to an agent. Delegation artifacts are deliberative records.
Content-Telemetry Separation	The classification principle requiring that deliberative content and operational telemetry be stored, transmitted, and governed through separate infrastructure paths.

3.6 Evidentiary Instruments

The following terms describe governance artifacts and assessment instruments that depend on the foundational concepts defined in subsections 3.1 through 3.5 and 3.7. These terms are downstream of the primitives; they identify artifacts produced by the governance process, not the governance primitives themselves.

Term	Definition
Conformance Level	The declared level of an implementation's governance posture under ARCS. ARCS defines three conformance profiles (Foundation, Minimum, Enterprise) that are operative, and six maturity levels (Level 0 through Level 5) that describe the completeness of an implementation's governance posture.
Assessor	An individual or entity responsible for evaluating conformance with this standard. May be internal (organization staff) or independent (external auditor).
Audit Evidence	Documentation, system outputs, logs, configurations, and other materials sufficient to verify conformance claims.
Conformance Statement	A written document produced by a conforming implementation containing the system name, operator, deployment mode, configuration identifier, assessment date, declared conformance level, exclusions, known non-conforming components, assessor identity, and all record-bearing components included in the assessment.
Attestation	A structured record confirming that a specific governance condition has been assessed and the result documented. Attestation records include session-level receipts, vendor compliance confirmations, and lifecycle audit attestations.
Telemetry	Operational metadata generated by an automated system during processing, including timestamps, latency measurements, error codes, resource utilization, completion status, and system health indicators.
Sovereignty Receipt	A governance artifact that records or attests to declared sovereignty-relevant conditions associated with the handling, processing, storage, or deployment context of governed records.

3.7 Entity Concepts

Term	Definition
Automated System	Any software, model, pipeline, agent, or service that processes human-directed input and generates outputs, logs, records, or derived artifacts as a condition of its operation.
Operator	The person, organization, or system that directs the use of an automated system. Distinct from the vendor that operates the underlying infrastructure.
Operator Boundary	The set of systems within the operator's control or governance responsibility for ARCS compliance.
Provider	The entity operating the AI system infrastructure. May be the same as or different from the deploying organization.
Tenant	An organization deploying an AI system for its own use or for its customers. In enterprise deployments, the tenant is typically the customer organization.
Vendor	A legal entity that operates infrastructure on which an automated system runs, stores data, or processes interaction records.
End User	The individual or automated system initiating interactions with the AI system.
Custodian	An entity that possesses, controls, or has the authority to access or delete interaction records.

3.8 Surface Class Taxonomy

The surface taxonomy in ARCS identifies six classes of automated-processing surface whose records present the custody gap condition described in this standard. The AI interaction surface is the primary domain addressed by ARCS controls. The remaining surface classes (transactional, identity, sensor, operational, and control-plane) are documented to establish that the governance gap condition is not unique to AI systems and to support future extension of the standard.

3.9 Conformance Keywords

The following conformance keywords are used throughout this standard: **shall** indicates a mandatory requirement; **should** indicates a recommendation; **may** indicates a permitted option. No alternative terminology SHALL be used in conformance documentation unless cross-mapped to the canonical term defined in this section.

4. Applicability

ARCS applies to any operator that uses an automated system in a context where interaction records are created, retained, or may be subject to legal process. Applicability is determined by record creation, not by system category.

4.1 In-Scope Systems

ARCS applies to operators using the following categories of automated system:

- AI assistants and AI agents, including consumer and enterprise interfaces, coding assistants, research assistants, and autonomous agents with tool-call or action-taking capability
- AI-enabled productivity software, including word processors, email clients, document editors, spreadsheet tools, presentation tools, and project management software where AI features are enabled by default or opt-out
- Ambient AI features embedded in enterprise software, including smart compose, smart reply, meeting transcription, search-based recommendations, and automated summarization
- API-based automated systems, including systems that process operator prompts or instructions through vendor-operated APIs and generate interaction records as a result
- Multi-step automated pipelines that direct one automated system to interact with another, where the pipeline generates, transmits, or stores interaction records
- Any other system that generates, retains, or derives artifacts from human-directed interaction where those artifacts may be subject to legal compulsion, regulatory inquiry, or preservation demand

4.2 Applicability Threshold

ARCS obligations arise when an operator uses an automated system that generates interaction records. An operator need not be involved in active litigation for ARCS to apply. The standard governs the default and preservation postures that determine whether records will exist if litigation or inquiry arises.

4.3 Non-Scope Boundaries

ARCS does not apply to system outputs consumed and immediately discarded by the operator where no record is retained in any custody location.

ARCS does not apply to automated systems that create no interaction records in any custody location, provided the operator can demonstrate non-creation under ARCS-NCR controls.

ARCS does not govern model safety, accuracy, bias, output quality, or system behavior. Those properties are governed by separate frameworks. ARCS governs only the lifecycle and custody of records created during system use.

4.4 Applicability to Vendors

ARCS obligations are placed on operators, not on vendors. Operators cannot fulfill their ARCS obligations without cooperation from vendors within the custody surface. ARCS requires operators to document vendor behavior, obtain vendor commitments where possible, and disclose limitations where vendor behavior cannot be verified or controlled.

5. Control Family Structure

ARCS controls are organized into ten control families. Each family addresses a distinct governance domain for interaction records. Controls within each family are identified by a three-letter family code and a two-digit sequence number (e.g., LIF-01, AGT-07). ARCS v1.0 contains 92 controls across 10 control families.

ARCS uses a two-layer family structure. In the Standard, each family is defined as a governance domain with a distinct scope and boundary. In the Controls catalog, each family is expressed through its constituent control statements and related operational detail.

Code	Family	Domain	Controls
ARCS-LIF	Record Lifecycle	Creation, retention, deletion, vendor deletion verifiability, and lifecycle state transitions	13
ARCS-CUS	Custody Surface	Custody identification, multi-vendor propagation, authorization-gap custody, vendor governance declarations	12
ARCS-TAX	Record Taxonomy	Record categories, classification, and category-based lifecycle rules	11
ARCS-OPB	Operator Boundary	Operator scope, vendor inclusion, responsibility boundary	5
ARCS-PUB	Publish Boundary	Export, third-party sharing, API propagation	6
ARCS-NCR	Non-Creation Posture	Non-creation declarations, memory-only processing, publish boundary verification	6
ARCS-PV	Preservation and Legal Hold	Preservation triggers, hold process, multi-vendor preservation communication	7
ARCS-VER	Verification and Audit	Lifecycle audit, custody audit, vendor compliance, cross-vendor traceability, attestation	7
ARCS-AGT	Agent Runtime	Agent runtime artifacts, tool call governance, intermediate record controls, security-relevant content, lifecycle boundaries	13
ARCS-DEL	Delegation and Memory	Governed persistence, delegation chains, autonomous execution records, emergent execution documentation	12

Each control family has a defined applicability scope. An operator satisfies the applicable families for its deployment and documents non-applicability for others.

The base families (ARCS-LIF through ARCS-VER) apply to all deployments subject to ARCS. ARCS-NCR applies only where non-creation or non-retention is claimed. ARCS-AGT applies to any deployment in which an automated system operates across multiple steps, invokes external tools, or maintains state across steps within a session. ARCS-DEL applies to any deployment in which an agent maintains state across sessions, operates with delegated authority, or executes autonomous action sequences without synchronous human review.

6. ARCS-LIF: Record Lifecycle

Purpose

ARCS-LIF defines the governance domain applicable to the lifecycle of interaction records. This family establishes requirements for creation, classification, retention, deletion, purge execution, and lifecycle-state transition. It applies wherever a record enters, persists within, or exits a governed environment, and ensures that lifecycle treatment is explicit, verifiable, and capable of review. The purpose of this family is to prevent lifecycle treatment from remaining implicit, discretionary, or dependent on undocumented system behavior.

Governance focus

- Conditions under which governed records are created or recognized
- Classification states relevant to retention and deletion treatment
- Declared retention periods and lifecycle-state transition
- Deletion and purge execution as governed actions rather than background assumptions
- Evidentiary record of lifecycle treatment where review is required

Boundary

ARCS-LIF applies at every point where a record is created, retained, reclassified, deleted, or otherwise subjected to lifecycle treatment within the governed environment. It governs the operator's handling of record persistence over time and distinguishes declared lifecycle treatment from mere system behavior. This family does not depend on publication, transfer, or legal hold in order to apply. It establishes the baseline lifecycle posture against which those later conditions may modify or suspend ordinary treatment.

The corresponding control statements for this family are maintained in the Controls catalog.

7. ARCS-CUS: Custody Surface

Purpose

ARCS-CUS defines the governance domain applicable to the identification and declaration of record custody. This family establishes requirements for identifying custodians, documenting propagation across vendor and system boundaries, and maintaining visibility into the surfaces through which records are held, processed, retransmitted, or otherwise made materially available. Its purpose is to ensure that custody is declared as an observable governance condition rather than inferred only from architecture diagrams, procurement records, or post hoc investigation.

Governance focus

- Identification of record custodians and materially relevant subprocessors
- Declaration of vendor and system surfaces through which records move
- Distinction between primary custody, delegated custody, and retransmission surface
- Visibility into multi-system propagation and boundary crossing
- Maintenance of custody declarations sufficient for review and audit

Boundary

ARCS-CUS applies wherever custody is distributed, shared, delegated, or extended beyond a single system boundary. It governs the visibility of holding and propagation conditions, whether persistent or transient, where those conditions are relevant to record treatment. This family is concerned with the existence and declaration of custody surface, not merely with contractual relationship or infrastructure ownership. Where records pass through systems that materially affect retention, access, transmission, or exposure, this family applies.

The corresponding control statements for this family are maintained in the Controls catalog.

8. ARCS-TAX: Record Taxonomy

Purpose

ARCS-TAX defines the governance domain applicable to the classification of interaction records. This family establishes requirements for assigning records to categories that determine lifecycle treatment, custody significance, boundary conditions, preservation posture, and downstream obligations. Its purpose is to ensure that governance treatment is attached to record type through declared taxonomy rather than through informal naming, application convention, or unexamined default behavior.

Governance focus

- Assignment of records to policy-relevant categories
- Taxonomy attributes that affect retention, deletion, preservation, or publication
- Distinction among transient, persistent, derivative, evidentiary, and other governed record classes
- Classification logic sufficient to support downstream governance decisions
- Consistency between taxonomy and declared lifecycle or custody treatment

Boundary

ARCS-TAX applies wherever differences in record type affect governance treatment. It governs the classification layer by which records are distinguished for policy purposes, including where similar technical artifacts carry different governance significance. This family does not require that every record class receive identical treatment. It requires that treatment-relevant distinctions be declared and maintainable. Where record handling turns on type, this family applies.

The corresponding control statements for this family are maintained in the Controls catalog.

9. ARCS-OPB: Operator Boundary

Purpose

ARCS-OPB defines the governance domain applicable to the boundary of operator responsibility. This family establishes requirements for determining which records, systems, vendors, and processing contexts fall within the operator's declared governance scope. Its purpose is to ensure that statements about retention, deletion, custody, verification, and publication are made against a clearly defined perimeter rather than an indeterminate collection of adjacent technical dependencies.

Governance focus

- Declaration of the operator-governed perimeter
- Distinction between in-scope and out-of-scope systems or processing contexts
- Treatment of vendor services, delegated functions, and adjacent environments
- Consistency between governance claims and actual boundary definition
- Exclusion logic where systems or records are not governed by the operator

Boundary

ARCS-OPB applies wherever responsibility must be distinguished from downstream, inherited, external, or third-party processing conditions. It governs the perimeter within which the operator claims governance effect and outside of which separate custody or responsibility conditions apply. This family is concerned not with whether external systems exist, but with whether the boundary between operator responsibility and adjacent environments is declared sufficiently to support meaningful governance claims.

The corresponding control statements for this family are maintained in the Controls catalog.

10. ARCS-PUB: Publish Boundary

Purpose

ARCS-PUB defines the governance domain applicable when interaction records cross from a governed environment into a published, exported, transferred, or externally accessible state. This family establishes the requirements that attach at the publish boundary, including boundary declaration, downstream lifecycle continuity, and the treatment of records that remain discoverable, retrievable, or propagable after transfer. Its purpose is to ensure that external release is governed as a distinct condition rather than treated as the end of record responsibility by implication.

Governance focus

- Declaration of publication, export, or external release conditions
- Treatment of records that remain discoverable or accessible after transfer
- Continuity of lifecycle obligation across publish-boundary events
- Distinction between internal persistence and external circulation
- Release conditions involving APIs, syndication, downstream delivery, or third-party exposure

Boundary

ARCS-PUB applies where records are made available beyond the operator's direct environment through publication, export, API delivery, syndication, transmission, or similar release mechanisms. It governs the transition from internal custody to wider circulation where the record may continue to exist, propagate, or be relied upon after crossing the original system boundary. This family applies whenever release alters the governance condition of the record by extending its accessibility beyond the governed environment.

The corresponding control statements for this family are maintained in the Controls catalog.

11. ARCS-NCR: Non-Creation Posture

Purpose

ARCS-NCR defines the governance domain applicable to systems and workflows that are declared not to create governed interaction records, or to create only bounded transient artifacts that do not persist as governed records. This family establishes requirements for such declarations, the operating conditions under which they remain true, and the verification criteria necessary to distinguish non-creation from undeclared persistence. Its purpose is to ensure that non-creation is treated as a governed posture rather than as an informal assertion about system design.

Governance focus

- Declaration of non-creation posture
- Conditions under which transient processing does not become governed persistence
- Distinction between absence of record creation and unexamined record generation
- Identification and governance of residual artifacts that persist notwithstanding a non-creation claim
- Operating assumptions necessary to sustain a non-creation claim
- Evidence sufficient to review or verify that posture

Boundary

ARCS-NCR applies wherever an operator claims that governed records are not created, or are created only in bounded transient form that does not persist as a governed record. It governs the conditions under which such claims remain valid. This family does not apply merely because a system is lightweight, ephemeral in intent, or low-retention by design. It applies where the absence of governed record creation is itself being asserted as a meaningful governance condition.

The corresponding control statements for this family are maintained in the Controls catalog.

12. ARCS-PV: Preservation and Legal Hold

Purpose

ARCS-PV defines the governance domain applicable to preservation obligation, hold state, and suspension of ordinary deletion or purge treatment. This family establishes requirements for hold triggers, preservation scope, hold communication, and the treatment of records whose ordinary lifecycle must be interrupted for legal, regulatory, investigatory, or other declared reasons. Its purpose is to ensure that preservation conditions are governable, reviewable, and capable of overriding ordinary lifecycle automation where required.

Governance focus

- Initiation of preservation or legal hold state
- Definition of scope for affected records, systems, or custodians
- Suspension of ordinary deletion or purge treatment
- Communication and maintenance of hold condition
- Documentation sufficient to support later review of preservation posture

Boundary

ARCS-PV applies wherever ordinary lifecycle treatment must be suspended because a preservation obligation has attached. It governs the change in record posture that occurs when deletion, purge, or other routine lifecycle action can no longer proceed as scheduled. This family applies to the existence and maintenance of hold state, including its scope and operational effect, rather than to the substantive merits of the underlying dispute, inquiry, or proceeding giving rise to preservation.

The corresponding control statements for this family are maintained in the Controls catalog.

13. ARCS-VER: Verification and Audit

Purpose

ARCS-VER defines the governance domain applicable to the verification of declared record treatment. This family establishes requirements for evidentiary support, auditability, traceability, attestation, and the means by which lifecycle, custody, publication, preservation, and related governance claims may be tested against observable record. Its purpose is to ensure that declared posture can be substantiated through reviewable evidence rather than resting solely on policy language or interface-level assertion.

Governance focus

- Evidentiary support for declared governance claims
- Traceability between stated treatment and observable artifact
- Auditability of lifecycle, custody, publication, and hold conditions
- Attestation and verification mechanisms
- Record of governance events sufficient for independent examination

Boundary

ARCS-VER applies wherever governance claims must be substantiated rather than merely stated. It governs the evidentiary and review conditions under which an operator may demonstrate that declared treatment has actually occurred, or that declared boundaries and obligations are materially reflected in system behavior and retained record. This family applies across other domains of the Standard where proof, traceability, or independent review is required.

The corresponding control statements for this family are maintained in the Controls catalog.

14. ARCS-AGT: Agent Runtime

Purpose

ARCS-AGT defines the governance domain applicable to agent-mediated execution and runtime-generated record conditions. This family establishes requirements for records arising from autonomous or semi-autonomous processing, including execution context, tool invocation, intermediate artifacts, runtime decision surfaces, and other record-bearing conditions specific to agentic operation. Its purpose is to ensure that records produced through delegated computational action are governed as first-order record conditions rather than treated as incidental byproducts of application behavior.

Governance focus

- Execution context associated with agent-mediated action
- Record-bearing consequences of tool invocation and delegated processing
- Treatment of intermediate artifacts, runtime traces, and execution-linked outputs
- Distinction between user-originated input, runtime transformation, and agent-generated artifact
- Governance significance of autonomous or semi-autonomous execution state

Boundary

ARCS-AGT applies wherever agent-mediated execution creates, transforms, carries forward, or materially conditions interaction records within the governed environment. It governs runtime-specific record conditions that arise from delegated computational action, including where those conditions are not fully captured by ordinary user-input or static application-state models. This family applies when execution flow, runtime context, or agent-linked artifact formation bears on lifecycle, custody, verification, or other governance treatment.

Agent runtime artifact taxonomy

The following artifact classes are defined for purposes of ARCS-AGT controls. Operators must classify all agent runtime artifacts into one or more of these classes.

Planning trace. The agent's representation of its intended execution path, including task decomposition, step ordering, alternative approaches considered, and reasoning about which path to pursue. Planning traces are deliberative records and SHALL be classified as ephemeral by default.

Tool call artifact. Any record created by or resulting from the agent's invocation of an external tool. Tool call metadata (tool name, timestamp, completion status, latency, error codes) is operational telemetry. Tool call content (arguments passed, responses received, content derived from operator prompts) is deliberative. These components SHALL be governed separately.

Intermediate result. The output of any step in a multi-step workflow that is not the final deliverable. Intermediate results are deliberative records and SHALL be classified as ephemeral unless the operator designates a specific output as a retained deliverable.

Execution trace. The sequence of steps, decisions, tool invocations, and state transitions executed during a session. Structural metadata is operational telemetry. Reasoning content is deliberative. These components SHALL be governed separately.

Error recovery artifact. Any record generated when the agent encounters a failure condition and adapts its execution. Error recovery artifacts are deliberative records. Error metadata (error codes, retry counts, affected tool) is operational telemetry and may be retained separately.

Session state artifact. Any record used to maintain continuity within a single agent session. Session state artifacts are ephemeral and SHALL not persist beyond session termination.

Security-sensitive tool output. Tool output whose content is operationally sensitive independent of its deliberative character. Requires decomposition: the final deliverable is persistent, deliberative intermediates are ephemeral, operational telemetry is retainable.

The corresponding control statements for this family are maintained in the Controls catalog.

15. ARCS-DEL: Delegation and Memory

Purpose

ARCS-DEL defines the governance domain applicable to delegated execution, persistent memory, and continuity of record across handoff, reuse, or retained contextual state. This family establishes requirements for documenting delegation chains, memory-bearing artifacts, execution inheritance, and other conditions in which record significance persists through autonomous continuation or retained state. Its purpose is to ensure that governance remains attached not only to a single interaction event, but also to the continuity of state carried forward across later action.

Governance focus

- Delegation chains through which action or responsibility continues beyond an initial interaction
- Persistent memory and retained contextual state with governance significance
- Continuity of record across reuse, inheritance, or resumed execution
- Distinction between isolated interaction output and state carried forward into later processing
- Responsibility conditions attached to memory-bearing artifacts and delegated continuation

Boundary

ARCS-DEL applies wherever records or materially significant state persist through delegation, memory, or continued execution beyond a single immediate interaction. It governs conditions under which retained context, inherited state, or delegated continuation carry governance effect forward across time or process boundary. This family applies when what matters is not only the initial record event, but the persistence and later use of state that continues to shape action, interpretation, or responsibility.

Governed persistence

Persistent agent memory is deliberative in content but requires persistence to function. The standard three-class retention model (ephemeral, session-bounded, persistent) does not adequately address this condition. ARCS-DEL introduces governed persistence as a fourth retention class.

A memory store classified as governed persistence SHALL satisfy all of the following: (a) retained on operator-controlled infrastructure or in a storage environment subject to the operator's deletion authority; (b) subject to a defined maximum retention period with automatic purge; (c) excluded from backup systems or synchronization that would create uncontrolled copies; (d) subject to preservation posture under ARCS-PV; and (e) not transmitted to governance infrastructure or third parties as part of receipt generation.

Delegation

An agent operating with delegated authority executes on behalf of the operator or user and may interact with external systems, commit resources, transmit data, or take consequential actions within the scope of its delegation. The record of what the agent was authorized to do, and by whom, is a governance artifact. Delegation artifacts are deliberative records.

Multi-agent and cross-operator considerations

Where a deployment involves multiple agents, each agent-to-agent interaction may generate its own artifact classes. The operator of the orchestrating system is responsible for documenting the custody surface of agent-to-agent communication records. Each agent in a multi-agent deployment SHALL have its artifact classes, retention posture, and custody surface documented independently.

The corresponding control statements for this family are maintained in the Controls catalog.

16. Conformance

A system conforms to ARCS if all applicable controls for the declared conformance profile are implemented, required documentation exists, lifecycle posture is defined, custody surface is disclosed, preservation posture is supported, and non-creation claims are auditable where asserted. Conformance is evaluated per deployment, not per organization.

16.1 Scoping

A conformance claim may be scoped to a defined subset of the operator's AI systems, provided:

1. the scope is explicitly stated in the conformance statement;
2. the scoped systems are independently identifiable and assessable; and
3. any material interaction between scoped systems and systems outside the declared scope is disclosed in the conformance statement.

Scoping does not permit exclusion of material record surfaces. A system that transmits records to an out-of-scope system must disclose that transmission as a custody event, even if the receiving system is not itself assessed.

16.2 Conformance profiles

ARCS defines three conformance profiles:

Foundation Profile. Requires implementation of ARCS-LIF, ARCS-CUS, and ARCS-TAX, with ARCS-NCR required only if non-creation or non-retention is claimed. The Foundation Profile establishes baseline record identification and surface mapping sufficient to begin governance. Organizations may declare Foundation conformance while implementing remaining families.

Minimum Profile. Requires implementation of all controls in ARCS-LIF, ARCS-CUS, ARCS-TAX, ARCS-OPB, ARCS-PUB, ARCS-PV, and ARCS-VER, with ARCS-NCR required only if non-creation or non-retention is claimed. The Minimum Profile constitutes the institutional minimum for ARCS conformance.

Enterprise Profile. Requires all Minimum Profile controls plus Enterprise Enhanced controls. Enterprise Enhanced controls are defined in the Enterprise Implementation Profile. Universal Enhanced controls apply to all Enterprise Profile declarations. Conditional Enhanced controls apply based on the operator's declared risk factors as specified in the Enterprise Profile document.

16.3 Maturity levels

ARCS defines six maturity levels describing the completeness of an implementation's governance posture. Maturity levels are descriptive; conformance profiles are operative. An operator claiming a maturity level should also declare the corresponding conformance profile.

Level 0 - Undocumented record governance. Interaction records exist, but the implementation has not independently identified, mapped, or documented the record, custody, discovery, and review surfaces. Most organizations deploying AI systems are at Level 0 upon initial assessment. Level 0 reflects reliance on vendor

policy statements without independent documentation, not the absence of all data governance.

Level 1 - Record identification. The implementation has identified the interaction records created by its operation. Record surfaces, custody, retention, and routing may remain undocumented. Corresponds approximately to ARCS-TAX and basic ARCS-LIF inventory.

Level 2 - Surface mapping and disclosure. The implementation has mapped where records exist, who holds them, and what review and routing conditions apply. Retention and deletion documentation may remain incomplete. Corresponds approximately to ARCS-CUS, ARCS-TAX, and ARCS-LIF, with review and routing disclosure.

Level 3 - Documented lifecycle governance. The implementation has documented how records move, persist, and are removed across the interaction lifecycle, including retention and deletion controls. Corresponds approximately to ARCS-LIF, ARCS-PUB, and deletion/routing controls.

Level 4 - Governance-grade implementation. The implementation has achieved governance-grade control of interaction records across the normal operating surfaces of the system. Level 4 marks the transition from internal documentation to externally reviewable governance. A Level 4 implementation can demonstrate where interaction records exist, who holds them, and how long they persist, for all normal deployment modes, in a form reviewable by an auditor, procurement officer, or legal counsel. Corresponds to the Minimum Profile.

Level 5 - Full-surface governance. The implementation has governed all known record surfaces, including advanced runtime, derivative, and autonomous execution artifacts. No known material record surface remains undocumented. Level 5 claims SHALL identify the scope of agent runtime, delegation, memory, and derivative-record governance applied, including any material runtime conditions not fully specified by the current version of this standard. Corresponds approximately to the Enterprise Profile with agent runtime coverage.

16.4 Partial conformance

An implementation may declare partial conformance by listing the control families satisfied, provided partial conformance is not represented as Foundation, Minimum, or Enterprise Profile conformance. Partial conformance declarations should identify families satisfied, families in progress, and families not yet addressed.

16.5 Conformance statement requirements

A conformance statement SHALL identify:

1. system name and operator;
2. declared conformance profile (Foundation, Minimum, or Enterprise) and maturity level where applicable;
3. scope of the assessment, including any scoping exclusions;
4. deployment mode(s) included;
5. date of assessment;
6. excluded components with justification;
7. known non-conforming components;
8. responsible assessor and assessment type (self-attestation, internal audit, or third-party assessment).

16.6 Reference implementation

At least one reference implementation of ARCS lifecycle controls, including record classification, retention posture enforcement, sovereignty receipt generation, automated purge scheduling, and legal hold override, exists in production code as of the date of this publication. Reference implementations do not confer conformance on other deployments.

17. Limitations and Non-Claims

Conformance to ARCS does not by itself establish privilege, confidentiality, immunity from discovery, immunity from preservation, immunity from liability, legal sufficiency under any specific jurisdiction, insurance coverage, or zero-record operation.

ARCS governs record architecture and disclosure. It does not govern legal outcomes. Legal advice regarding discovery, privilege, and compliance obligations should be obtained from qualified counsel.

ARCS does not define model quality requirements, privacy law compliance in general, information security certification in general, privilege doctrine, substantive discovery law, insurance coverage terms, product performance requirements, AI safety evaluation methodology, red-teaming or adversarial testing methodology, content moderation policy, data protection impact assessment methodology, or model documentation requirements. Where ARCS governs records created by such activities (safety review logs, evaluation datasets, moderation artifacts), the governance applies to the records, not to the activities that generated them.

ARCS does not require non-retention. It requires that retention decisions are explicit, documented, auditable, and architecture-aware. An implementation that retains all interaction records may conform to ARCS if the retention is documented, the custody surface is mapped, and the governance controls are operational.

ARCS does not require any specific retention duration, any specific architecture, any specific vendor, any specific security model, or any specific legal theory. ARCS requires disclosure, mapping, and documentation.

Conformance to ARCS does not establish compliance with any external regulatory framework, including GDPR, CCPA, HIPAA, the EU AI Act, NIST SP 800-53, ISO 27001, or SOC 2. ARCS may be used alongside those frameworks, and an implementation may satisfy overlapping requirements, but ARCS conformance and external regulatory compliance are independently evaluated.

18. Relationship to Other Frameworks

ARCS is complementary to existing security, privacy, and records management frameworks. It addresses a distinct governance layer: the lifecycle and custody of interaction records created during automated system use.

Framework	What It Governs	ARCS Relationship
NIST SP 800-53	Security and privacy controls for information systems	ARCS extends to lifecycle and custody of interaction records, which 800-53 does not address. Maps to AU-3, MP-6, SI-7, AC-3.
NIST AI RMF	AI risk, bias, safety, transparency	ARCS governs records created by AI systems. AI RMF governs system behavior and outputs.
ISO 42001	AI management systems	ARCS provides record-level governance that organizational controls do not reach.
EU AI Act	High-risk AI logging obligations	EU AI Act requires log creation. ARCS governs what happens to those logs after creation.
SOC 2	Service organization controls	ARCS custody and lifecycle controls may inform SOC 2 evidence.
MCP / A2A	Agent-to-tool and agent-to-agent protocols	MCP defines how context flows. ARCS governs what happens to records after they flow.

ARCS does not duplicate, replace, or supersede any of these frameworks. An organization may be fully compliant with every framework listed here and still have no governance posture for interaction records. ARCS addresses that gap.

19. Versioning and Amendment Control

19.1 Version numbering

ARCS uses a major.minor version scheme. A major version increment (e.g., v1 to v2) denotes structural changes to control families, conformance levels, or the surface model that may require reassessment. A minor version increment (e.g., v1.3 to v1.4) denotes additions, clarifications, or expanded coverage that do not invalidate prior conformance claims but may introduce new requirements for higher conformance levels. Errata corrections that do not change normative requirements are denoted by a patch identifier and do not constitute a new version for conformance purposes.

19.2 Transition period

Conformance claims issued under a prior version remain valid for 12 months after publication of a new major version, provided the assessor documents a gap analysis identifying new requirements introduced by the current version. Claims older than 24 months without renewal or gap analysis are considered stale and SHALL not be cited as current conformance evidence.

Minor version increments do not trigger the transition period. An implementation conforming to v1.3 remains conforming through v1.x unless the implementation's declared conformance level requires controls introduced in a later minor version.

19.3 Amendment authority

Amendments to ARCS are published by Vega Commons Project, Inc. The amendment process includes public notice of proposed changes, a comment period for adopters and assessors, and a reconciliation review before publication. Emergency errata affecting the correctness of normative text may be published without a comment period, provided they are documented in the version history with the rationale for expedited publication.

19.4 Backward compatibility

New versions of ARCS SHALL not retroactively invalidate conformance that satisfied all requirements of the prior version at the time of assessment. Where a new version introduces requirements that would change the conformance status of an existing implementation, the transition period in Section 19.2 applies.

19.5 Conformance statement version reference

All conformance statements, attestation artifacts, and assessment reports SHALL reference a specific ARCS version number. Conformance claims that do not reference a version are non-conforming. Where an implementation undergoes reassessment, the new assessment SHALL reference the current version.