AI SYSTEM OF RECORD · EVIDENCE PACK

ISO/IEC 42001:2023

ISO/IEC · 2023

Organization	Acme Health Co. (sample)
Workspace ID	sample_workspace_acmehealth
Period covered	Apr 21, 2026 ’ May 21, 2026
Pack ID	pack_iso-42001_2026-05-21_sample0
Generated	May 21, 2026, 03:00 PM
Attested by	Joe Carter (joe.carter@acmehealthco-sample.test)

Controls satisfied	Needs attention
12 / 14	2
Missing	**Chain integrity**
0	Verified

About this pack

AI Management System (AIMS) standard. Certification-grade evidence for organizations deploying AI systems or relying on third-party AI tools.

This evidence pack is produced from the Northbeams AI System of Record for the period above. Every control on the following pages is mapped to data captured by the Northbeams browser extension, desktop sentinel, and MCP gateway — no manual screenshots or spreadsheets. The append-only audit log feeding this pack is hash-chained (HMAC-SHA256, key id nbm_v1_sample00) so the artifact can be verified against the source data at any time at northbeams.com/verify.

1. Scope

1.1 Scope statement

Sample workspace on a Northbeams Evidence subscription. The bundled telemetry surfaces (browser extension, desktop sentinel, MCP gateway) install on every laptop and observe AI tool use, MCP gateway calls, and LLM traffic in observation-only mode. The data feeding this pack comes from those surfaces directly, not from self-attestation. Synthetic data shown here matches the shape of a real 30-day window for a 60-person workspace. Out of scope: BYOD endpoints without the Northbeams installer, mobile, and network traffic that bypasses the gateway.

1.2 What is in scope

The Northbeams AI System of Record captures the following surfaces for Acme Health Co. (sample):

· Browser-resident AI tool use (extension), including visits, prompts, and uploads to third-party AI tools.

· Desktop AI tool use (Northbeams desktop sentinel), including local MCP server calls.

· MCP gateway traffic — every tools/call invocation by AI agents the workspace operates.

· LLM API traffic intercepted by the Northbeams LLM proxy where deployed.

· Workspace policy and configuration history, including who changed what and when.

1.3 What is out of scope

Activity that does not flow through the surfaces above is not in scope of this pack. Specifically:

· AI tool use from unmanaged or BYOD devices that do not run the Northbeams extension or sentinel.

· Network-layer outbound calls that bypass the browser, sentinel, and MCP gateway.

· Internal model training pipelines if your organization develops AI systems (the framework treats deployer obligations only).

1.4 Observed scope statistics

AI tools inventoried	**22**
· Sanctioned	**8**
· Unknown	**3**
· High-risk	**11**
Active employees (last 30d)	**58**
Audit-log history	**47 days**
Events recorded in window	**12,437**

1.5 Chain integrity

Events are committed to a per-collection, per-org append-only hash chain. Each event's hash commits to the prior event's hash so any tampered, missing, or reordered event breaks the chain at that point. Status for this period:

Verified (chain intact end-to-end).. Chain cutover began Apr 01, 2026; events prior to that date are present in the log but predate hash-chain integrity claims.

2. Control mapping

Each row maps a ISO 42001 obligation to the artifact that satisfies it. AUTO rows derive their status from workspace telemetry; ATTEST rows are owner-confirmed organizational facts with a recorded timestamp and actor.

2.1 Automatic controls

ID	CONTROL	STATUS	EVIDENCE
aims-asset-inventory	**AI system inventory maintained** ISO/IEC 42001 cl. 6.1.4 + A.6.2.6	Satisfied	22 AI tools catalogued. 8 sanctioned, 11 high-risk, 3 awaiting review.
aims-risk-classification	**Each AI system risk-classified** ISO/IEC 42001 A.5.4 (impact assessment)	Needs attn.	19 of 22 classified. 3 unknown tools surfaced in the last week pending review.
aims-monitoring-active	**Operational monitoring of AI use** ISO/IEC 42001 cl. 9.1 + A.6.2.6	Satisfied	12,437 events captured in window. 4 surfaces reporting (extension, sentinel, MCP gateway, LLM proxy).
aims-control-policy-defined	**Documented AI use policy in force** ISO/IEC 42001 cl. 5.2 + A.2.2	Satisfied	Custom policy on file. Last edited 02 May 2026 by jcarter@acmehealthco-sample.test.
aims-incident-records	**AI incident records retained** ISO/IEC 42001 cl. 9.1 + A.10.4	Satisfied	47 days of incident history retained. Oldest event: 03 April 2026.
aims-access-control	**AI system access control in place** ISO/IEC 42001 A.4.6 (resources)	Satisfied	Workspace owner identified. 58 active members in the last 30 days, all enumerated.

2.2 Owner attestations

ID	CONTROL	STATUS	EVIDENCE
aims-leadership-policy	**AI policy approved by leadership** ISO/IEC 42001 cl. 5.1	Satisfied	Attested 14 May 2026. Attested 2026-05-14 by Joe Carter.
aims-objectives-set	**AI objectives defined and reviewed** ISO/IEC 42001 cl. 6.2	Satisfied	Attested 14 May 2026. Attested 2026-05-14 by Joe Carter.
aims-roles-assigned	**AI roles and responsibilities assigned** ISO/IEC 42001 cl. 5.3 + A.3.2	Satisfied	Attested 14 May 2026. Attested 2026-05-14 by Joe Carter.
aims-impact-assessment	**AI system impact assessment performed** ISO/IEC 42001 A.5.2 + A.5.3	Needs attn.	Not yet attested by workspace owner.
aims-third-party-mgmt	**AI suppliers and data providers managed** ISO/IEC 42001 A.10.2 + A.10.3	Satisfied	Attested 14 May 2026. Attested 2026-05-14 by Joe Carter.
aims-internal-audit	**Internal AIMS audit within last 12 months** ISO/IEC 42001 cl. 9.2	Satisfied	Attested 14 May 2026. Attested 2026-05-14 by Joe Carter.

aims-management-review	**Management review within last 12 months** ISO/IEC 42001 cl. 9.3	**Satisfied**	Attested 14 May 2026. Attested 2026-05-14 by Joe Carter.
aims-continual-improvement	**Continual improvement actions logged** ISO/IEC 42001 cl. 10	**Satisfied**	Attested 14 May 2026. Attested 2026-05-14 by Joe Carter.

3. Evidence appendix

Sampled events supporting the AUTO controls above. Sampling is deterministic: the most recent N events per control (N=10 typical), filtered to the reporting window. The full event log is available on request as a signed JSONL export from the Northbeams Trust dashboard.

AI system inventory maintained (aims-asset-inventory)

WHEN	SAMPLED EVENT
2026-05-20 14:08Z	Cursor (high-risk) · alice@acme
2026-05-20 11:22Z	Claude Code (high-risk) · bob@acme
2026-05-19 16:51Z	ChatGPT (sanctioned) · carol@acme
2026-05-19 09:14Z	Granola (sanctioned) · dan@acme
2026-05-18 17:33Z	Perplexity (unknown) · erin@acme
2026-05-18 13:01Z	Pi.ai (unknown) · frank@acme
2026-05-17 10:48Z	Claude Desktop (high-risk) · gina@acme
2026-05-17 08:02Z	Cody (high-risk) · hank@acme
2026-05-16 19:28Z	ChatGPT (sanctioned) · ivan@acme
2026-05-16 14:55Z	Cursor (high-risk) · joan@acme

Each AI system risk-classified (aims-risk-classification)

WHEN	SAMPLED EVENT
2026-05-20 14:08Z	Cursor ’ re-classified high-risk by jcarter@acme
2026-05-19 13:22Z	Pi.ai ’ flagged unknown (auto)
2026-05-19 11:18Z	Perplexity ’ flagged unknown (auto)
2026-05-18 09:44Z	Granola ’ sanctioned (admin override)

Operational monitoring of AI use (aims-monitoring-active)

WHEN	SAMPLED EVENT
2026-05-21 11:58Z	agent · cursor ’ tools/list · allow
2026-05-21 11:57Z	agent · claude-code ’ tools/call (read_file) · allow
2026-05-21 11:55Z	agent · claude-code ’ tools/call (delete_file) · block · policy: delete_file
2026-05-21 11:54Z	browser · chatgpt ’ prompt (credential) · block
2026-05-21 11:52Z	agent · cursor ’ tools/call (write_file) · warn

4. Methodology

4.1 Data collection

Northbeams collects the events feeding this pack from three first-party surfaces:

· **Browser extension.** Watches AI tool tabs in the user's primary browser, classifies pasted/typed content with an on-device privacy classifier, and posts event metadata (hashed where sensitive) to the workspace ingest endpoint.

· **Desktop sentinel.** Native macOS / Windows daemon that observes locally-running AI clients and MCP servers. Sensitive payloads are redacted at the source; only category and hash signals cross the wire.

· **MCP gateway.** Workspace MCP-aware proxy intercepting tools/call invocations, applying allow/warn/block policy, and recording per-call metadata.

4.2 Retention

Event retention windows for the surfaces feeding this pack:

· Incidents (browser tool visits, prompts): 395 days.

· LLM API events: 395 days.

· MCP gateway events: 395 days.

· Policy audit log: 730 days.

Retention is enforced server-side via Firestore TTL fields. The full retention schedule is published at northbeams.com/trust and any change is announced in the privacy policy.

4.3 Integrity

Each event collection maintains a per-org append-only hash chain. Every event commits SHA-256(seq prevHash canonical(payload)) and updates a chain-head document. Verification recomputes the chain end to end; any tampered, missing, or reordered event breaks the chain at that point. This pack's chain status: **verified**.

4.4 Pack signature

The full content of this pack is hashed (SHA-256) into a content digest, then signed with the workspace's evidence-signing key (HMAC-SHA256, key id nbm_v1_sample00). Both the digest and the signature are printed on the next page and embedded in the pack's `pack.json` companion manifest. To verify, visit northbeams.com/verify and submit the pack id along with the printed digest and signature.

4.5 Sampling

AUTO controls are corroborated by sampled events. Sampling is deterministic and biased toward recent events within the reporting window. The full event log is available on request via the signed JSONL export from the Northbeams Trust dashboard.

4.6 What this pack does NOT claim

Pack contents do not constitute legal advice, an audit opinion, or a certification under any framework. The pack is the workspace owner's attestation supported by Northbeams telemetry. A qualified auditor's review is still required for certification.

5. Attestation & signature

5.1 Workspace owner attestation

I, **Joe Carter** (joe.carter@acmehealthco-sample.test), attest as the owner of the Northbeams workspace **Acme Health Co. (sample)** (sample_workspace_acmehealth) that:

· The information in this pack is accurate to the best of my knowledge as of May 21, 2026, 03:00 PM.

· The controls marked as attested were confirmed by me with the timestamps recorded in section 2.2.

· The Northbeams telemetry feeding the automatic controls reflects the workspace surfaces enumerated in section 1.2.

5.2 Pack signature

```
Pack id:        pack_iso-42001_2026-05-21_sample0
Period:         2026-04-21T00:00:00.000Z ’ 2026-05-21T00:00:00.000Z
Content digest: 8ebc24abec528e6908c42e4f13315cfa6b7adb50db93fc7234915ff7abc2850b
Algorithm:      HMAC-SHA256
Key id:         nbm_v1_sample00
Signature:      a649939860e56c1ca702b1e337ac54988bfdf6645913a394f06bf68c02e859c1
```

5.3 Verification

To independently verify this pack: visit northbeams.com/verify and submit the pack id along with the printed digest and signature. The verifier recomputes the content digest from the pack contents and validates the signature against the workspace's evidence-signing key. The verifier returns "valid" only if the digest and signature match.

Workspace owner signature

Joe Carter

Date

May 21, 2026