

M C P S E R V E R

N O C O D E

C L O U D H O S T E D

Insurance Document Retention Plan MCP

Automate document lifecycles and regulatory compliance workflows.

Insurance Document Retention Plan MCP manages the entire lifecycle of your insurance documentation. Your AI client uses this MCP to pull retention rules, calculate when documents need to be destroyed, and build storage plans that map directly to Hot, Cold, or Ready for Purge tiers. It handles the heavy lifting of compliance monitoring so you don't have to manually track every policy date.

insurance

retention

compliance

document-lifecycle

audit



The connectivity layer between AI and the world's software.



Vinkius sits between AI and every application. All communication passes through Vinkius Cloud via the Model Context Protocol (MCP) — with governance, observability, and security at every layer.

Your AI Connections Run Through Vinkius Cloud

The world's largest
managed MCP catalog

Vinkius is the connectivity layer where AI connects to the software your business already runs. We handle the hosting, the security, the credentials, the uptime — you get agents that actually do things.

We operate the world's largest managed MCP catalog. Major SaaS platforms, CRMs, databases, and cloud providers — running, monitored, production-ready. This MCP server is hosted and maintained by the Vinkius Cloud for AI Agents.

The agent doesn't manage credentials, doesn't manage uptime, doesn't manage security. Vinkius does.

— Architecture principle

Four Pillars of the Vinkius Runtime

01 — Security by design

Credentials stay encrypted at rest via AES-256. The AI agent never touches raw keys — they're injected into a sandboxed V8 isolate at runtime. Actions are logged, and connections have an emergency kill switch.

03 — Deterministic observability

Eight immutable metrics per endpoint: request volume, p95 latency, error rate, active connections, cost attribution. A live payload feed logs every tool call with mutation detection.

02 — Built on MCP Fusion

This MCP server was built with **MCP Fusion**, the open-source framework (Apache 2.0) that powers the entire Vinkius catalog. Schema-as-firewall strips undeclared fields, compiled PII redaction runs at zero overhead, and cryptographic lockfiles produce git-diffable audit trails.

04 — Autonomous operations

Servers are deployed, monitored, and patched autonomously. New capabilities and security patches ship weekly. Zero-downtime deployments ensure continuous availability across all managed MCP servers.

AES-256

Encryption at rest

Ed25519

PKI vault signatures

24h TTL

Ephemeral session keys

V8 Isolate

Sandboxed execution

One Token. Instant Access.

Every MCP server on Vinkius is accessed through a **Connection Token**. Tokens are generated in the cloud dashboard and produce a unique MCP endpoint URL. Paste this URL into any MCP-compatible client — no SDK required.

A single token can serve **multiple AI clients simultaneously**, or you can issue separate tokens per client for granular access control. Each token tracks its own request count, last activity timestamp, and can be individually enabled or revoked.

MCP ENDPOINT`https://edge.vinkius.com/{token}/mcp`

Claude



Cursor



VS Code



Windsurf



Grok



Gemini

Security Is the Architecture

Security in Vinkius is not a feature — it's the foundation of the runtime. The gateway enforces multiple independent protection layers between AI agents and third-party APIs.

01 — Ed25519 PKI Vault

Every workspace has an Ed25519 Master Key. Session keys are generated ephemerally (24h TTL) and signed by the Master Key. Credentials never leave the vault boundary.

02 — V8 Isolate Sandboxing

Tool code runs inside isolated-vm V8 isolates with 64 MB memory caps and per-request timeouts. No filesystem access, no network access except through the SSRF-guarded fetch bridge.

03 — SSRF Guard

All outbound HTTP requests are DNS-resolved and validated before execution. Private IP ranges (10.x, 172.16-31.x, 192.168.x, AWS metadata 169.254.x) are blocked at the network layer.

05 — Cryptographic Audit Trail

Every request is signed into a SHA-256 hash chain with Ed25519 signatures. Events form a tamper-proof, SIEM-exportable forensic record.

04 — DLP & PII Redaction

A ResponseGuard pipeline intercepts every tool response. Configurable redaction patterns strip sensitive fields (emails, SSNs, card numbers) before data reaches the AI agent.

06 — Honeypot Trap System

Phantom credentials are injected into isolated environments. If a honeypot is used outside Vinkius infrastructure, the server is quarantined instantly.

Emergency Kill Switch

EU AI Act Art. 14(1)
Compliant

The kill switch is an **emergency halt** mechanism — not a simple toggle. When triggered, it executes three actions atomically:

01 — Server deactivated

The MCP server is immediately taken offline across the entire cluster.

02 — All tokens revoked

Every connection token is invalidated. Total lockout — reconnection blocked until new tokens are issued.

03 — WebSocket connections killed

Active connections terminated via Redis pubsub broadcast. Propagates to every runtime node in the cluster.

Full Visibility. Zero Guesswork.

The Vinkius cloud dashboard includes a full MCP Governance suite — real-time analytics and security controls for production AI operations.

Control Plane

KPI dashboard with request volume, latency, success rate, token consumption, and AI-generated operational briefings.

FinOps

Cost tracking per tool, payload compression savings, budget optimization signals, and consumption trends.

Firewall & DLP

PII redaction activity, sensitive data protection counters, and security event timeline.

Agent Activity

Which AI clients are connecting, how often, and what they're doing — real-time session tracking.

Tool Health

Slowest and most error-prone tools, with actionable root-cause insights and performance baselines.

Incident Log

Error trends, failure rates, status-code breakdowns, and forensic audit trail access.

Get started at cloud.vinkius.com — connect your AI agent in under 60 seconds.

Insurance Document Retention Plan MCP

4 tools available

Cloud-hosted on Vinkius

Managing insurance records shouldn't feel like a guessing game. This MCP gives your AI agent the logic needed to handle document lifecycles without manual oversight. You can use it to pull standard retention rules for specific document types or build out full storage plans for entire policies. It maps every document to the correct storage tier, whether that is Hot, Cold, or Ready for Purge. Instead of digging through spreadsheets to see what needs to be deleted, your agent can calculate exact disposition dates and flag potential compliance risks in your current storage strategy. It's built to keep your documentation organized and audit-ready by linking document types to their required regulatory timelines.

Core Capabilities

01 — Retention Rule Retrieval

Your agent pulls standard regulatory timelines for specific document types.

02 — Disposition Calculation

The AI calculates exactly when a document is ready for destruction or review.

03 — Storage Tier Mapping

Documents are automatically categorized into Hot, Cold, or Ready for Purge tiers.

04 — Risk Assessment

Your agent scans storage plans to find compliance vulnerabilities.

05 — Policy Planning

The MCP generates full storage and review schedules for individual policies.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/insurance-document-retention-plan — connect your AI agent in three steps.

- 01 Connect your preferred MCP-compatible client to Vinkius.
- 02 Provide your agent with policy details or document types.
- 03 The agent uses the MCP tools to calculate dates or generate plans.
- 04 Review the resulting storage tiers or compliance risk reports.

Get your insurance document lifecycle running in minutes by connecting your AI client to the Vinkius-hosted MCP.

Built For

This MCP is designed for insurance professionals who need to automate the management of document lifecycles and regulatory requirements.

Compliance Officers

They hand off the task of checking storage plans against regulatory rules to the AI.

Insurance Operations Managers

They use the agent to automate the scheduling of document reviews and purges.

Data Privacy Specialists

They rely on the agent to ensure documents are destroyed according to legal timelines.

What Changes When You Connect

- 01 Automates the calculation of document destruction dates.
- 02 Maps documents to specific storage tiers like Hot or Cold.
- 03 Identifies compliance risks within storage plans.

04 Generates structured storage schedules for insurance policies.

Real-World Applications

Automated Purging

Your agent identifies documents that have reached their disposition date so they can be safely destroyed.

Policy Onboarding

When a new policy is created, the agent generates a full storage plan based on claim and renewal dates.

Audit Preparation

Use the agent to verify that your current document storage tiers match regulatory requirements.

Regulatory Research

Quickly check the required retention period for any specific document type.

Patterns to Avoid

Manual retention rule lookup

❌ AVOID

You spend hours searching through regulatory PDFs to figure out how long to keep a specific claim file.

✓ INSTEAD

Let your agent pull the exact timelines for you using `get_retention_schedule`.

Guessing destruction dates

❌ AVOID

A manager decides to purge a folder of documents based on a gut feeling about when they are old enough.

✓ INSTEAD

Use `calculate_document_disposition` to find the precise date a document is ready for review or destruction.

Ignoring storage tier gaps

❌ AVOID

You build a new policy storage plan without checking if it actually meets legal requirements.

✓ INSTEAD

Run `evaluate_compliance_risk` to find gaps in your proposed storage plan before you implement it.

The Right Fit

Insurance compliance officers and operations managers should connect this MCP to automate document lifecycles. If your team manages document storage through manual spreadsheets and lacks strict regulatory timelines, this MCP is for you. Avoid this if you do not have defined document types or specific retention requirements to follow.

Insurance Document Retention Plan MCP Tools

These tools handle the heavy lifting of document lifecycles, from calculating destruction dates to mapping storage tiers.

#	TOOL	DESCRIPTION
01	evaluate_compliance_risk	Use this tool to have your agent identify potential compliance gaps within a proposed storage plan.
02	generate_storage_plan	This tool builds a complete storage and review schedule for a specific insurance policy.
03	get_retention_schedule	This tool retrieves the standard regulatory retention rules for any given document type.
04	calculate_document_disposition	This tool determines the exact date a specific document is due for review or destruction.

See It in Action

Real prompts you can use once this MCP is connected to your AI agent through Vinkius Cloud.

- U** Generate a storage plan for policy ID POL-998 with these claim dates: 2023-01-15 and 2023-06-20, and renewal dates: 2024-01-01.



The storage plan for policy POL-998 includes 2 claims in Hot storage and the renewal record in Hot storage, with a review scheduled for 2025-01-01.

- U** What is the retention rule for a 'claim' document type?



Claims must be retained for 7 years from the trigger date according to the Standard regulatory tier.

- U** Check if there are any compliance risks for this storage plan: {"documents": [{"documentId": "DOC-1", "storageTier": "Ready for Purge", "reviewDate": "2023-01-01"}]} under the 'Standard' tier.



No high-level compliance risks were identified for the provided storage plan under the Standard tier.

Frequently Asked Questions

01 What kind of storage tiers does this MCP use?

The MCP maps documents to Hot, Cold, or Ready for Purge tiers based on their lifecycle stage.

02 Can I use this with Claude or Cursor?

Yes, you can connect this MCP to any MCP-compatible client including Claude, Cursor, and Windsurf.

03 How does the MCP handle document destruction?

The MCP uses the `calculate_document_disposition` tool to determine exactly when a document is due for destruction.

04 Does this MCP help with regulatory compliance?

Yes, it includes a tool to evaluate compliance risks and another to retrieve standard retention rules.

05 Do I need to host the MCP myself?

No, Vinkius hosts and manages the MCP for you, so it is ready to use immediately after connection.

06 How does the retention period get calculated?

The retention period is determined by the intersection of the document type and the regulatory tier, or by a user-provided override via ``calculate_document_disposition``.

07 What are the different storage tiers?

Documents are assigned to Hot storage if active, Cold storage if nearing their end date, or marked Ready for Purge if they have passed their retention date.

08 Can I override standard retention rules?

Yes, you can use the ``calculate_document_disposition`` tool with the ``userOverrideYears`` parameter to extend the retention of a specific document.

Go Live in 60 Seconds

Get your connection token from cloud.vinkius.com, then paste the endpoint URL into any MCP-compatible client.

YOUR MCP ENDPOINT

`https://edge.vinkius.com/[TOKEN]/mcp`

CLIENT	WHERE TO CONFIGURE
 Claude AI	Profile → Customize → Connectors → "+" → Add custom connector → Paste endpoint
 Cursor	Settings → Features → MCP Servers → "+ Add New MCP Server" → Type: SSE → Paste endpoint
 VS Code	Ctrl/Cmd+Shift+P → "MCP: Add Server" → add <code>"insurance-document-retention-plan": { "url": "..." }</code>
 Windsurf	MCP Settings → <code>mcp_settings.json</code> → Add endpoint URL
 ChatGPT	Settings → Tools & plugins → Add MCP server → Paste endpoint
 Gemini	Extensions → Add MCP Server → Paste endpoint URL

ASK AN AI ABOUT THIS

Let your preferred AI explain this MCP server

-  Ask ChatGPT 
-  Ask Claude 
-  Ask Perplexity 
-  Ask Gemini 
-  Ask Grok 

READY TO CONNECT

Insurance Document Retention Plan is live on Vinkius Cloud.

Get your connection token, paste it into your AI agent, and
start building. No SDK. No deployment. Just results.

Start at cloud.vinkius.com →

vinkius.com · support@vinkius.com

INDEPENDENT PLATFORM DISCLAIMER

Vinkius is an independent platform and is not affiliated with, endorsed by, sponsored by, verified by, or otherwise authorized by Insurance Document Retention Plan. All third-party trademarks, logos, and brand names are the property of their respective owners. Their use in this document is strictly for informational purposes to identify service compatibility and interoperability.

DOCUMENT INFORMATION

Generated	September 2026
MCP Server	Insurance Document Retention Plan MCP
Server ID	01a0e1c3-e1a6-7290-89c8-f19a280ec681
Platform	Vinkius Cloud for AI Agents
Endpoint	https://edge.vinkius.com/{token}/mcp

LICENSE & USAGE

This document is generated automatically by the Vinkius PDF Engine. Content reflects the MCP server configuration at the time of generation and may change as updates are deployed. For the most current information, visit vinkius.com/en/ai-agent-connect/insurance-document-retention-plan.