

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

File Retention Schedule MCP

Automate document lifecycles and stay compliant with automated rules.

File Retention Schedule MCP manages the entire lifecycle of your digital documents. It connects your AI client to organizational and regulatory retention rules to determine exactly when files need to be kept, archived, reviewed, or destroyed. Instead of manual tracking, your agent handles the math and the logic for every file in your system.

A+

Quality Score 100/100

retention

lifecycle

compliance

document-management

automation



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.

File Retention Schedule MCP

4 tools available

Cloud-hosted on Vinkius

Managing document lifecycles manually is a liability. This MCP connects your AI client to the specific retention rules your organization follows, turning your agent into a compliance officer. You can use it to calculate precise timelines for any file based on its metadata, ensuring you never delete something too early or keep something too long. It handles the heavy lifting of identifying which documents are ready for archiving or permanent destruction, making it easy to manage massive datasets without missing a single deadline. Whether you are dealing with tax records, HR files, or legal documents, the MCP validates that any manual overrides still follow your established policies. It keeps your data lifecycle predictable and your audit trails clean.

Core Capabilities

01 — Timeline Generation

Your agent calculates specific keep, archive, and deletion dates for individual files.

02 — Batch Identification

The agent finds groups of files that need to move to the next lifecycle stage.

03 — Policy Enforcement

The agent checks manual retention overrides against your official organizational rules.

04 — Rule Retrieval

Your agent looks up the standard retention settings for any document category.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/file-retention-schedule — connect your AI agent in three steps.

- 01
- Connect your MCP-compatible client to Vinkius.
- 02
- Provide your agent with document metadata or category types.
- 03
- The agent uses the MCP tools to calculate dates or fetch rules.
- 04
- Your agent executes the identified lifecycle actions like archiving or deletion.

Connect the MCP to your client and let your agent handle the lifecycle logic.

Built For

This MCP is built for professionals managing large volumes of regulated data who need to automate document lifecycles.

Compliance Officers

They use the agent to ensure all document destruction and archiving meets regulatory standards.

Data Managers

They hand off the task of identifying files ready for deletion to the AI.

Legal Operations

They use the tool to manage the retention and review timelines for sensitive legal records.

What Changes When You Connect

- 01
- Automates the calculation of archive and deletion dates.
- 02
- Prevents non-compliance by validating manual retention overrides.
- 03
- Identifies batches of files ready for specific lifecycle actions.

- 04 Standardizes document handling through category-specific rules.
-

Real-World Applications

Regulatory Compliance

Ensure tax and financial records are kept for the exact duration required by law before being purged.

Data Privacy

Automate the permanent destruction of sensitive user data once its retention period expires.

Storage Optimization

Identify large batches of old documents that can be moved to cheaper archive storage.

Audit Preparation

Use the agent to quickly pull lists of files that have undergone specific lifecycle stages.

Patterns to Avoid

Manual timeline guessing

❌ AVOID

You try to manually calculate when a tax document should be deleted based on a spreadsheet. This leads to errors and missed deadlines.

✓ INSTEAD

Let your agent handle the math. Use `calculate_retention_milestones` to build an exact lifecycle timeline based on file metadata and your specific rules.

Ignoring policy constraints

❌ AVOID

A user requests to delete a file early to save space, but that file is actually under a legal hold.

✓ INSTEAD

Always run manual changes through the system. Use `validate_retention_override` to ensure any requested changes still follow your official organizational policies.

Searching for files one by one

❌ AVOID

You spend hours looking through folders to find which documents are old enough to be archived.

✓ INSTEAD

Automate the discovery process. Use `filter_files_by_action` to pull a complete list of every file that has reached a specific lifecycle stage.

The Right Fit

Connect this MCP if you manage large volumes of regulated data like HR, tax, or legal records. Do not connect it if your data has no formal retention requirements. The decision rests on whether you need to automate the enforcement of specific document lifecycles.

File Retention Schedule MCP Tools

These tools give your agent the ability to calculate lifecycles, enforce organizational policies, and identify files ready for action.

#	TOOL	DESCRIPTION
01	calculate_retention_milestones	This tool builds a complete lifecycle timeline for a specific file. It uses file metadata and your retention rules to set exact dates for every stage.
02	filter_files_by_action	This tool pulls a list of files that have reached a specific lifecycle stage. Use it to find everything ready for deletion or archiving.
03	get_category_rules	This tool retrieves the default retention settings for a specific document classification. It tells your agent what the standard rules are for a given category.
04	validate_retention_override	This tool checks if a user-requested retention change follows your organizational policy. It prevents accidental non-compliance when manual changes are requested.

See It in Action

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

U What is the lifecycle timeline for file ID 'doc_123' which is a 'Tax' document created on 2020-01-01?



For file doc_123 (Tax), the keep date is 2030-01-01, the archive date is 2025-01-01, the review date is 2029-01-01, and the delete-on date is 2030-01-01.

U Are there any files ready to be deleted as of today?



There are 12 files currently eligible for permanent destruction based on their retention schedules.

U What are the default retention rules for the 'HR' category?



The default retention for HR documents is 5 years, with archiving occurring after 3 years and a review triggered 1 year before deletion.

Frequently Asked Questions

01 How does this MCP help with document compliance?

It connects your AI client to specific retention rules, allowing the agent to calculate exact dates for archiving and deletion while validating that any manual changes still follow policy.

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 What happens if I want to keep a file longer than the rule allows?

You can request a retention override, and the MCP will use the validation tool to check if that request complies with your organization's rules.

04 Can the AI identify all files that need to be deleted today?

Yes, the agent can use the filtering tool to identify all files that have reached their scheduled destruction date.

05 Does this MCP host my files?

No, this MCP provides the logic and rules for your agent to manage your existing files. Vinkius hosts the MCP itself to ensure it is always ready to run.

06 How does a legal hold affect file retention?

When a legal hold is active, the ``calculate_retention_milestones`` tool ensures the deletion date is pushed to the infinite future, preventing any files from being flagged for destruction.

07 Can I override the default retention period for a category?

You can attempt an override, but you should first use ``validate_retention_override`` to ensure the proposed duration complies with mandatory regulatory requirements for that category.

08 How can I find all files that need to be archived?

You can use the ``filter_files_by_action`` tool with the 'archive' action type and a specific reference date to retrieve a list of all files ready for long-term storage.

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>"file-retention-schedule": { "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

File Retention Schedule 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 File Retention Schedule. 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	October 2026
MCP Server	File Retention Schedule MCP
Server ID	01a0eddd-e055-7380-b275-729cc43a3639
Platform	Vinkius Cloud for AI Agents
Endpoint	<code>https://edge.vinkius.com/{token}/mcp</code>

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/file-retention-schedule.