

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

Digital Records Review Calendar MCP

Turn static governance policies into active audit schedules.

Digital Records Review Calendar MCP connects your AI client to your digital record governance system. It moves your compliance efforts from passive documents to active scheduling by allowing your agent to identify managed assets, calculate upcoming audit windows, check legal destruction mandates, and plan owner alerts.

A+ Quality Score 100/100

records

audit

compliance

scheduling

governance



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.

Digital Records Review Calendar MCP

4 tools available

Cloud-hosted on Vinkius

You can stop manually tracking compliance deadlines. This MCP gives your AI client direct access to your digital record governance data, turning rigid policies into a living schedule. Instead of digging through spreadsheets to see what needs reviewing, you can ask your agent to pull up the current status of any record group.

Your agent can use this connection to map out exactly when audits need to happen based on your specific retention rules. It handles the heavy lifting of calculating review windows and checking the legal requirements for when data should be destroyed. When it's time to notify stakeholders, your agent can pull the necessary notification details to keep everyone on track. It effectively bridges the gap between having a policy on paper and actually executing it in your daily workflow.

Core Capabilities

01 — Asset Identification

Your agent identifies all managed record groups within the governance system.

02 — Audit Window Mapping

The agent calculates specific dates for upcoming review events.

03 — Retention Rule Retrieval

Your agent pulls legal destruction mandates for specific data sets.

04 — Notification Planning

The agent gathers details for upcoming owner alerts and reminders.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/digital-records-review-calendar — connect your AI agent in three steps.

- 01

Connect your preferred MCP-compatible client to Vinkius.
- 02

The agent accesses your digital record governance system through the MCP.
- 03

You ask your agent questions about record groups or review dates.
- 04

The agent executes the necessary tools to pull real-time compliance data.
- 05

Your agent provides the specific schedule or rule details you requested.

Connecting this MCP to your AI client enables direct interaction with your governance data.

Built For

This MCP is built for professionals managing high-stakes data lifecycles and regulatory compliance.

Compliance Officers

They hand off the task of monitoring audit windows and retention deadlines to their agent.

Records Managers

They use the agent to track record groups and schedule necessary reviews.

Legal Operations Specialists

They rely on the agent to verify destruction mandates and legal hold requirements.

What Changes When You Connect

- 01

Converts static policy documents into actionable schedules.
- 02

Automates the calculation of audit windows and review dates.

-
- 03 Centralizes retention and destruction rules for easy querying.
 - 04 Reduces manual oversight of compliance notification timelines.
-

Real-World Applications

Audit Readiness

An agent calculates all upcoming review events to ensure the team is prepared for scheduled audits.

Data Destruction Management

A user checks specific retention rules to determine when a record group is legally eligible for destruction.

Compliance Monitoring

The agent monitors managed record groups to ensure no audit windows are missed.

Stakeholder Alerting

The agent pulls reminder notification details to help plan alerts for record owners.

Patterns to Avoid

Manual Spreadsheet Tracking

❌ AVOID

You spend your morning manually updating a spreadsheet to track which record groups are due for a review next month.

✓ INSTEAD

Let your agent handle the math. Use ``calculate_review_schedule`` to pull all upcoming review events for a specific date range automatically.

Guessing Destruction Dates

❌ AVOID

A team member assumes a file set is ready to be deleted because it looks old enough.

✓ INSTEAD

Always verify the legal requirements first. Use ``get_group_retention_details`` to pull the exact retention and destruction rules for that specific group.

Missing Stakeholder Alerts

❌ AVOID

You realize too late that a record owner was never notified about an upcoming audit window.

✓ INSTEAD

Stay ahead of the deadline. Use ``get_reminder_notifications`` to pull the necessary details for upcoming owner alerts.

The Right Fit

Connect this MCP if your organization manages high-stakes data lifecycles that require strict adherence to legal retention mandates. Do not connect it if your data governance is informal or lacks documented destruction rules. The decision rests on whether you need to turn static policy documents into an active, automated schedule.

Digital Records Review Calendar 4 Tools

These tools give your agent direct access to record groups, retention rules, and upcoming audit schedules.

#	TOOL	DESCRIPTION
01	get_group_retention_details	This tool retrieves the specific retention and destruction rules for a selected record group.
02	get_reminder_notifications	Use this to pull the details for upcoming reminder notifications.
03	list_record_groups	This tool provides a full list of all managed record groups in your system.
04	calculate_review_schedule	This tool calculates all upcoming review events that fall within a specific date range.

See It in Action

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

U What record groups are currently managed in the system?



The system currently manages the following record groups: Financial Audits 2023, Employee Onboarding, and Legal Contracts.

U When is the next review for the Financial Audits 2023 group?



The next review for Financial Audits 2023 is scheduled for October 15th, 2024.

U What are the retention rules for the Employee Onboarding group?



The Employee Onboarding group must be kept for 7 years, after which the destruction action is Digital Shredding.

Frequently Asked Questions

01 What does this MCP actually do?

It connects your AI client to your digital record governance system so your agent can manage audit schedules and retention rules.

02 Can I use this with Claude or Cursor?

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

03 How does it handle data destruction?

The agent uses the retention tool to retrieve specific legal destruction mandates for your record groups.

04 Does it help with scheduling audits?

Yes, it includes a tool to calculate upcoming review events within any date range you specify.

05 Do I need to host this myself?

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

06 How can I see all my managed record groups?

You can use the ``list_record_groups`` tool to retrieve a list of all managed groups, including their owners and next review dates.

07 How do I find out when a specific review is due?

Use the ``calculate_review_schedule`` tool with a specific date range to find all upcoming review events.

08 Can I check the retention rules for a specific group?

Yes, the ``get_group_retention_details`` tool provides the specific legal and operational mandates for any given group ID.

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>"digital-records-review-calendar": { "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

Digital Records Review Calendar 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 Digital Records Review Calendar. 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	Digital Records Review Calendar MCP
Server ID	01a0db08-aaaa-72dc-a930-36ced2896a07
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/digital-records-review-calendar.