MCP SERVER | NO CODE | CLOUD HOSTED

Documentary Source Plan MCP

Keep your production ethical, verified, and organized.

Documentary Source Plan MCP manages the complex logistics of documentary filmmaking. It helps you map out how to use specific footage, organize outreach to interviewees, and maintain a clear record of editorial decisions and participant communications. Your AI client uses these tools to ensure your narrative stays grounded in verified facts and ethical standards.

A+ Quality Score 100/100

documentary | workflow | verification | outreach | editorial

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · SEPTEMBER 2026
vinkius.com/en/ai-agent-connect/documentary-source-plan

SCAN TO VIEW

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.

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.

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.

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	Ed25519	24h TTL	V8 Isolate
Encryption at rest	PKI vault signatures	Ephemeral session keys	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.

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.

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.

06 — Honeytoken Trap System

Phantom credentials are injected into isolated environments. If a honeytoken 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.

Agent Activity

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

FinOps

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

Tool Health

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

Firewall & DLP

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

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.

Documentary Source Plan MCP

5 tools available
Cloud-hosted on Vinkius

Documentary filmmaking requires more than just good footage; it requires a rigorous system for managing sources and verifying claims. This MCP acts as your production's logical backbone. Instead of digging through messy spreadsheets, you can use your AI client to map out exactly how specific materials fit into your narrative while respecting legal and ethical boundaries.

You can manage the entire lifecycle of a source, from the first outreach attempt to the final editorial decision. It helps you track how you communicate with participants so you never lose the thread of a conversation. When you need to verify a claim, the MCP helps you generate the right investigative questions to cross-reference against your archival materials. It keeps your editorial decisions documented, ensuring that every creative choice is backed by a clear rationale. This is about building a reliable, verifiable record of your entire production process.

Core Capabilities

01 — Source Mapping

Your agent uses this to align footage usage with narrative needs and legal permissions.

02 — Outreach Logistics

Your AI client generates checklists to manage interviewee contact and scheduling.

03 — Fact Verification

Your agent generates investigative questions to test the validity of source claims.

04 — Decision Tracking

Your AI client maintains a log of the rationale behind your editorial choices.

05 — Communication Management

Your agent organizes the timing and method of all participant interactions.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/en/ai-agent-connect/documentary-source-plan** — connect your AI agent in three steps.

01 Connect your AI client to the Vinkius hosted MCP.

02 Provide your production data or context to your AI agent.

03 Ask your agent to generate plans, logs, or questions using the available tools.

04 Review the outputs to guide your filming, interviewing, or editing.

Connect your preferred AI client to Vinkius to start managing your production data immediately.

Built For

This MCP is built for documentary filmmakers and investigative producers who need to manage high-stakes source data.

Documentary Director

Hands off editorial decision-making and narrative mapping to the AI.

Producer

Uses the tool to manage outreach logistics and participant communication plans.

Fact Checker

Relies on the tool to generate verification questions and cross-reference claims.

What Changes When You Connect

01 Maintains a clear audit trail of editorial decisions.

02 Prevents legal issues by mapping source usage to specific permissions.

03 Reduces logistical errors in interviewee outreach.

04 Strengthens narrative integrity through structured fact verification.

Real-World Applications

Managing Permissions

Use the source use plan to ensure you don't exceed the legal limits of your footage licenses.

Interviewee Coordination

Generate outreach actions to keep track of when you last spoke to a subject.

Verifying Claims

Use verification questions to challenge a source's statement against your archival footage.

Editorial Auditing

Review the decision log to ensure your creative choices remain consistent with your production goals.

Patterns to Avoid

Ignoring legal usage limits

AVOID

You decide to use a specific piece of archival footage in a scene without checking if your license covers it.

✓ INSTEAD

Always run a check through get_source_use_plan to confirm your footage permissions align with your narrative plan.

Unstructured outreach attempts

AVOID

You send random emails to interviewees and lose track of who responded or when you last spoke.

✓ INSTEAD

Use generate_outreach_actions to build a structured checklist of contact steps for every subject.

Vague editorial reasoning

AVOID

You change the direction of a scene but can't remember why you cut a specific interview segment.

✓ INSTEAD

Record the logic behind every creative pivot using get_editorial_decision_log to maintain a clear audit trail.

The Right Fit

Documentary directors and investigative producers should connect this MCP if they manage high-stakes source data or complex legal permissions. Small, casual vloggers won't find value here. The deciding factor is whether your production requires a verifiable record of editorial decisions and source usage.

Documentary Source Plan MCP Tools

These tools manage the lifecycle of your production data, from participant outreach to final editorial verification.

#	TOOL	DESCRIPTION
01	`get_editorial_decision_log`	This tool documents the reasoning behind your narrative and creative choices. It keeps a running record of why you made specific storytelling decisions.
02	`get_participant_communication_plan`	Use this to organize how and when you talk to subjects. It manages the logistics of your communication with interviewees.
03	`generate_outreach_actions`	This tool creates a checklist of logistical steps for contacting potential interviewees. It turns outreach goals into actionable tasks.
04	`get_source_use_plan`	This tool determines how you can legally and narratively use specific materials in your film. It helps you stay within the bounds of your source permissions.
05	`get_verification_questions`	This tool generates investigative questions to help you validate claims. It helps you cross-check what sources say against your available evidence.

See It in Action

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

U I have footage of a protest but only have Tier 2 permission. How should I use it?

Based on your Tier 2 permission, the footage should be used only within the specific geographic regions and time durations defined in your source-consent documentation.

U Help me plan my outreach for three primary subjects.

Your outreach priority is set to High for the three primary subjects. You should begin with initial inquiries, followed by technical checks and formal scheduling.

U Is the claim that the event happened in 1992 verified?

The current credibility score is low; you need to cross-reference this claim with official archival documents or secondary witness accounts to satisfy verification.

Frequently Asked Questions

01 **How does this MCP help with legal compliance?**

It uses the source use plan tool to help you determine how specific materials can be used based on the permissions you have documented.

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 through Vinkius.

03 **What does the editorial decision log do?**

It allows you to document and review the specific rationale behind your narrative and creative choices during production.

04 **Does Vinkius host the data?**

Vinkius hosts the MCP and manages the connection, allowing you to use the tools directly within your AI client.

05 **How do I verify a source's claim?**

You can use the get_verification_questions tool to generate a list of investigative questions designed to validate specific claims.

06 **How does this help with ethical production?**

The server includes tools like `get_participant_communication_plan` to manage consent and `get_source_use_plan` to ensure materials are used within their granted permissions.

07 **Can I use this to verify facts?**

Yes, the `get_verification_questions` tool generates investigative questions to validate claims against your available source materials.

08 **How do I track my creative choices?**

You can use `get_editorial_decision_log` to record the rationale behind narrative decisions and ensure they stay within your defined editorial boundary.

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 `"documentary-source-plan": { "url": "…" }`
Windsurf	MCP Settings → `mcp_settings.json` → 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

Documentary Source 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 Documentary Source 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	Documentary Source Plan MCP
Server ID	`01a0d87f-6db9-7365-8cbb-8dbd2f3ce4aa`
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/documentary-source-plan.