

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

Interview-Based Story Plan MCP

Organize your investigative and qualitative reporting workflows.

Interview-Based Story Plan MCP provides a structured framework for managing the lifecycle of an interview-driven story. It helps you handle everything from initial outreach to final participant reviews while enforcing strict consent and attribution boundaries to keep your reporting ethical and organized.

A+ Quality Score 100/100

storytelling

interview

ethics

workflow

planning



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.

Interview-Based Story Plan MCP

5 tools available

Cloud-hosted on Vinkius

You can use this MCP to move from a raw interview idea to a finished narrative without losing track of the ethical details. It acts as a specialized planning engine for journalists and qualitative researchers who need to manage complex human interactions. Instead of juggling messy notes and scattered emails, you use your AI client to build a cohesive roadmap. You can plan how you'll reach out to sources, prepare specific questions for sessions, and keep a clear, immutable record of what each person has consented to. It keeps your story development on track by defining the necessary narrative steps and managing how participants review your final work. This ensures you stay compliant with attribution requirements and maintain the integrity of your reporting throughout the entire process.

Core Capabilities

01 — Outreach Planning

Your agent uses this to build communication timelines for securing interviewees.

02 — Interview Preparation

Your AI client generates structured agendas to guide your live sessions.

03 — Consent Management

The MCP logs permission records to ensure you follow participant instructions.

04 — Workflow Mapping

Your agent defines the specific steps needed to move from interview to finished story.

05 — Feedback Control

The tool manages how participants review and provide feedback on your final work.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/interview-based-story-plan — connect your AI agent in three steps.

- 01 Connect your AI client to the Vinkius hosted MCP.
- 02 Ask your agent to generate an outreach sequence for your subjects.
- 03 Use the tool to create a session agenda for your upcoming interviews.
- 04 Log participant permissions immediately after your sessions.
- 05 Follow the narrative steps to build your final story.

Connect your preferred client to Vinkius and start planning your story immediately.

Built For

This MCP is built for professionals handling sensitive human-interest stories or qualitative data.

Journalists

They hand off outreach planning and consent logging to the AI.

Qualitative Researchers

They use the tool to organize interview agendas and narrative workflows.

Documentary Producers

They rely on the MCP to manage participant permissions and review cycles.

What Changes When You Connect

- 01 Enforces ethical boundaries through formal permission logging.
- 02 Reduces manual planning for interview outreach and scheduling.

-
- 03 Maintains a clear audit trail for participant consent.
-
- 04 Standardizes the transition from raw interview to final narrative.
-

Real-World Applications

Investigative Reporting

Plan complex outreach to multiple sources while keeping strict records of what they allow you to publish.

Feature Storytelling

Create structured agendas for deep-dive interviews and manage how subjects review the final draft.

Academic Research

Organize qualitative interview sessions and manage the subsequent narrative development steps.

Consent Tracking

Keep an immutable record of participant permissions to ensure ethical compliance.

Patterns to Avoid

Ignoring formal consent logs

❌ AVOID

You rely on your memory or a messy notebook to remember what a source agreed to during a sensitive interview.

✓ INSTEAD

Use ``log_permission_record`` to create a permanent, immutable record of every permission granted by a participant.

Unstructured interview sessions

❌ AVOID

You jump into a deep-dive interview without a plan, leading to missed questions and wasted time.

✓ INSTEAD

Run ``create_session_agenda`` to build a structured guide that keeps your live sessions focused and productive.

Disorganized story progression

❌ AVOID

You lose track of the specific stages needed to turn raw notes into a finished piece of journalism.

✓ INSTEAD

Use `develop\_narrative\_steps` to generate a clear, step-by-step workflow from the first interview to the final draft.

The Right Fit

Journalists, researchers, and documentary producers should connect this MCP if they manage human-interest stories requiring strict ethical compliance. If your work involves purely automated data scraping or non-human subjects, this tool isn't for you. The deciding factor is whether you need to track specific participant permissions and review cycles.



Interview-Based Story Plan MCP Tools

These tools handle the heavy lifting of managing source communications, interview structures, and ethical consent records.

#	TOOL	DESCRIPTION
01	create_session_agenda	This tool builds a structured guide to keep your interviews focused and productive.
02	define_review_options	Use this to set how participants can check and approve your final story output.
03	develop_narrative_steps	This tool generates a step-by-step workflow to take you from the first interview to a completed story.
04	generate_outreach_sequence	This tool creates a timeline of communications to help you secure interviews with your sources.
05	log_permission_record	Use this to create a permanent record of the specific permissions and consent given by a participant.

See It in Action

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

U I need to interview three experts about climate change over the next two weeks. Can you help me plan the outreach?



I have generated an outreach sequence for your three experts, scheduled to complete within your two-week window, including initial contact and follow-up steps.

U Help me prepare for an interview about urban planning. The topics are zoning, public transit, and green spaces. The source has requested full attribution.



I have created a session agenda covering zoning, public transit, and green spaces, with a prioritized section at the beginning to confirm consent and recording preferences.

U I need to log that Jane Doe has given permission for her full name to be used, but only for internal reports.



The permission record for Jane Doe has been logged, specifying full attribution with usage limited to internal reports.

Frequently Asked Questions

01 What does this MCP do?

It provides a framework for managing the entire lifecycle of an interview-based story, focusing on planning, ethics, and narrative development.

02 How does it help with ethics?

The MCP includes tools to log permission records, ensuring you have a clear account of what each participant has consented to.

03 Which AI clients can I use with this?

You can use this MCP with any compatible client, including Claude, Cursor, Windsurf, and VS Code.

04 Do I need to host the MCP myself?

No, Vinkius hosts and manages the MCP for you. You just connect your client and start using the tools.

05 Can I use this for simple interviews?

Yes, it works for any interview-based workflow, from quick outreach to complex, multi-step narrative projects.

06 How does this tool handle participant consent?

The tool uses ``log_permission_record`` to create an immutable record of all permissions, ensuring that all subsequent narrative steps respect the established consent and attribution rules.

07 Can I use this to plan my interview schedule?

Yes, you can use ``generate_outreach_sequence`` to create a chronological timeline of communications to secure your interviewees based on your specific project timeline.

08 What happens if I need to change the story structure?

You can use ``develop_narrative_steps`` to generate a new workflow that aligns with your updated story purpose and attribution requirements.

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>"interview-based-story-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

Interview-Based Story 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 Interview-Based Story 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	Interview-Based Story Plan MCP
Server ID	01a0d6eb-7b43-71f4-8d40-6f1880880767
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/interview-based-story-plan.