MCP SERVER | NO CODE | CLOUD HOSTED

Emergency Response Planning MCP

Build safer facilities with data-driven emergency protocols.

Emergency Response Planning MCP gives your AI client the ability to handle complex facility safety tasks. It identifies physical risks, maps out management zones, and calculates safe exit paths. You can also use it to check if your current staff and equipment levels meet regulatory requirements for specific emergency scenarios.

A+ Quality Score 100/100

safety | emergency | evacuation | risk-assessment | compliance

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · SEPTEMBER 2026
vinkius.com/en/ai-agent-connect/emergency-response-planning

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.

Emergency Response Planning MCP

4 tools available
Cloud-hosted on Vinkius

You can use this MCP to turn your AI agent into a safety coordinator. Instead of manually reviewing floor plans and equipment lists, you can ask your agent to run specific checks against your facility data. It handles the heavy lifting of identifying hazards and determining if your current resources are actually enough to handle a crisis.

When a risk is identified, the MCP helps you organize your response by dividing the facility into manageable zones based on those risks. It also builds movement paths to get people out of the building safely. If you are preparing for an audit or a drill, you can use the tool to verify that your personnel and gear meet the necessary standards for specific events like fires or gas leaks. It moves safety planning from static documents to active, actionable intelligence within your AI client.

Core Capabilities

01 — Hazard Identification

Your agent uses this to find and evaluate risks within a building.

02 — Zone Mapping

Your agent uses this to divide facilities into risk-based management areas.

03 — Path Calculation

Your agent uses this to create safe movement routes for personnel.

04 — Resource Auditing

Your agent uses this to check if equipment and staff levels meet standards.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/en/ai-agent-connect/emergency-response-planning** — connect your AI agent in three steps.

01 Connect the MCP to your AI client through Vinkius.

02 Provide your facility ID or data to your agent.

03 Ask your agent to run a specific tool like hazard analysis or evacuation planning.

04 Review the generated routes, zones, or resource reports.

Get your safety data into your AI client and start running checks immediately.

Built For

This MCP is built for professionals managing physical sites and safety protocols.

Facility Managers

They hand off hazard analysis and resource checking to the AI.

Safety Officers

They use the AI to generate evacuation routes and zone maps.

Compliance Auditors

They use the tool to verify if equipment levels meet specific standards.

What Changes When You Connect

01	Automates the identification of facility-specific risks.
02	Creates precise evacuation paths based on real-time scenarios.
03	Verifies resource availability against regulatory requirements.
04	Organizes facility management through risk-based zoning.

Real-World Applications

Emergency Drill Prep

Use the MCP to generate specific evacuation routes for different scenarios before a drill begins.

Compliance Verification

Check if your current PPE and staff counts meet the standards for a gas leak or fire.

Risk Assessment

Identify high-severity hazards in a specific facility zone to prioritize safety upgrades.

Facility Zoning

Divide a large complex into management areas based on the type of risks present in each area.

4 Tools Available

#	TOOL	DESCRIPTION
01	`calculate_evacuation_plan`	This tool generates safe movement paths for people to follow during an emergency.
02	`evaluate_resource_sufficiency`	This tool checks if your facility has the right amount of equipment and staff to handle a specific event.
03	`generate_response_zones`	This tool maps out how to divide a facility into management areas based on identified risks.
04	`analyze_facility_hazards`	This tool identifies and evaluates the specific risks present inside a facility.

See It in Action

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

U Analyze the hazards for facility ID 'FAC-123' and tell me what the risks are.

The analysis for facility FAC-123 identified a high-severity chemical leak hazard with an impact radius of 50 meters, affecting zones Z-01 and Z-02.

U Generate an evacuation plan for facility 'FAC-123' under scenario 'FIRE-09'.

The evacuation plan for scenario FIRE-09 is ready. The safe route starts in zone Z-04, moves through waypoints W-12 and W-15, and ends at assembly point A-01.

U Is facility 'FAC-456' compliant with US-Standard for a gas leak scenario?

No, there is a deficit. For scenario GAS-02, the required amount of PPE is 15 units, but only 10 units are currently available.

Frequently Asked Questions

01 **What AI clients can I use with this MCP?**

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

02 **How does the MCP help with compliance?**

The tool evaluates if your current personnel and equipment meet the necessary standards for specific emergency scenarios.

03 **Can I generate evacuation routes for specific scenarios?**

Yes, the tool calculates safe movement paths for personnel based on the specific emergency scenario you provide.

04 **Does this MCP host the data?**

Vinkius hosts and manages the MCP, so you just connect your client and start using the tools.

05 **Can I map out different areas of my facility?**

Yes, you can use the tool to divide your facility into risk-based management zones.

06 **How can I check if my facility is prepared for a specific hazard?**

You can use `analyze_facility_hazards` to evaluate the risks and then `evaluate_resource_sufficiency` to see if your current inventory meets the required regulatory standards.

07 **Can this tool generate evacuation routes?**

Yes, the `calculate_evacuation_plan` tool generates safe movement paths that avoid high-risk zones based on the current emergency scenario.

08 **How are response zones determined?**

Response zones are mapped using `generate_response_zones`, which partitions the facility based on the intersection of hazard impact radii and facility boundaries.

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 `"emergency-response-planning": { "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

Emergency Response Planning 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

DOCUMENT INFORMATION

Generated	September 2026
MCP Server	Emergency Response Planning MCP
Server ID	`01a0937f-4796-732a-b4e9-4bdb7cab252f`
Platform	Vinkius Cloud for AI Agents
Endpoint	`https://edge.vinkius.com/{token}/mcp`

LICENSE & USAGE