MCP SERVER | NO CODE | CLOUD HOSTED

Accessible Contingency Contact Plan MCP

Organize your response protocols when critical access is lost.

Accessible Contingency Contact Plan MCP manages response protocols and contact summaries for operations that depend on constant access. When service interruptions occur, your AI client uses this MCP to pull contact cards, draft stakeholder notifications, evaluate fallback plans, and follow standardized documentation procedures to keep your escalation paths organized.

A+ Quality Score 100/100

contingency | escalation | protocol | emergency-response | business-continuity

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · SEPTEMBER 2026
vinkius.com/en/ai-agent-connect/accessible-contingency-contact-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.

Accessible Contingency Contact Plan MCP

4 tools available
Cloud-hosted on Vinkius

You shouldn't have to hunt for contact details or guess the next step when a critical system goes down. This MCP handles the heavy lifting of contingency management by providing your AI client with the specific tools needed to navigate service interruptions. Instead of scrambling through spreadsheets during an outage, you can ask your agent to pull up a contact card for a specific responder or check which fallback actions are already pre-approved for a failed activity. It bridges the gap between a sudden loss of access and an organized, documented response. You can use it to draft specific messages for stakeholders based on the exact type of interruption you're facing, ensuring communication stays consistent. Once the issue is resolved, the MCP provides the standard steps to document the event and update your contact plans so you're ready for the next time.

Core Capabilities

01 — Rapid Contact Retrieval

Your agent pulls essential contact summaries instantly during an outage.

02 — Automated Stakeholder Messaging

The AI drafts scenario-specific notifications for different groups of people.

03 — Fallback Plan Execution

Your client identifies which alternative actions must be triggered immediately.

04 — Standardized Post-Incident Documentation

The AI follows set procedures to document events and update plans after resolution.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/en/ai-agent-connect/accessible-contingency-contact-plan** — connect your AI agent in three steps.

01 Connect your AI client to the Vinkius hosted MCP.

02 Describe the interruption or scenario to your agent.

03 The agent uses the MCP tools to pull contacts or fallback plans.

04 Your agent drafts or executes the necessary response actions.

05 Follow the guided procedure to document the event once resolved.

Get your contingency protocols running in your preferred AI client in minutes.

Built For

This MCP is built for professionals managing logistics or business continuity where downtime requires immediate, organized action.

Logistics Managers

They use the MCP to manage interruptions in supply chain or transport access.

Emergency Response Coordinators

They rely on the tool to pull contact cards and draft stakeholder alerts.

Business Continuity Officers

They use the fallback evaluation and documentation tools to maintain operational standards.

What Changes When You Connect

01 Reduces response time by providing instant access to contact data.

02 Standardizes communication through scenario-specific message drafting.

03 Eliminates guesswork by identifying pre-approved fallback actions.

04 Ensures consistent documentation through guided update procedures.

Real-World Applications

Hardware Failure Response

When a primary terminal fails, the AI identifies the manual data entry fallback plan.

Supply Chain Interruption

The MCP drafts notifications to stakeholders when a logistics route becomes inaccessible.

Post-Incident Review

After a service interruption is fixed, the AI follows the update procedure to refresh the contact plan.

Emergency Escalation

The AI pulls contact cards for Tier 1 responders to initiate immediate escalation.

Patterns to Avoid

Manual contact searching

AVOID

You spend twenty minutes digging through old spreadsheets to find a phone number while a system is down.

✓ INSTEAD

Ask your agent to use `generate_contact_card` to get a single-view summary of the responder you need immediately.

Guessing fallback steps

AVOID

A logistics manager tries to decide on a new route without checking if that specific fallback was actually approved.

✓ INSTEAD

Use `evaluate_fallback_plan` to identify the pre-approved alternative actions required for that specific interruption.

Generic crisis messaging

✗ AVOID

You send a one-size-fits-all email to every stakeholder regardless of how the interruption actually affects them.

✓ INSTEAD

Use `draft_notification_messages` to create tailored communications based on the exact type of scenario you are facing.

The Right Fit

Connect this MCP if your operations rely on strict business continuity protocols or logistics where downtime requires immediate, documented action. Do not connect it if your team handles low-impact interruptions that don't require pre-approved fallback plans or formal stakeholder alerts.

4 Essential Tools for Contingency Management

These tools give your agent the ability to pull contact data, evaluate fallback plans, and manage stakeholder communications during an outage.

#	TOOL	DESCRIPTION
01	`draft_notification_messages`	This tool creates specific messages for stakeholders based on the type of interruption occurring. It ensures your communications are tailored to the exact scenario.
02	`evaluate_fallback_plan`	This tool identifies the pre-approved alternative actions and commitments required when an access-dependent activity is interrupted.
03	`generate_contact_card`	This tool produces a single-view summary of essential contact info for a specific person or entity during a contingency event.
04	`get_update_procedure`	This tool provides the standard steps for documenting an event and updating your contact plan after an interruption is resolved.

See It in Action

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

U I need the contact card for contact ID 'C-101' in scenario 'S-500'.

Contact Name: John Doe, Primary Channel: SMS, Details: +1-555-0199, Role: Tier 1 Responder, Priority: High.

U Draft a notification for technical support regarding scenario 'S-500'.

Notification for Technical Support: An interruption has occurred in scenario S-500. Please review the current escalation status and prepare for activation.

U What is the fallback plan for activity 'A-202' due to a hardware failure?

Fallback Action: Switch to manual data entry via the secondary terminal. Commitment: Ensure all logs are synchronized within 2 hours. Trigger: Loss of primary hardware access.

Frequently Asked Questions

01 **What does this MCP do?**

It provides tools to manage contingency scenarios, such as generating contact cards, drafting notifications, and evaluating fallback plans when access is lost.

02 **Which AI clients can I use with this MCP?**

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

03 **How does it help with stakeholder communication?**

It uses the draft_notification_messages tool to create messages that are specific to the type of interruption you are experiencing.

04 **Can I use this for business continuity planning?**

Yes, it is designed for logistics and emergency response, helping you identify pre-approved fallback actions and standardize post-incident documentation.

05 **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.

06 **How do I get contact details during an interruption?**

You can use the `generate_contact_card` tool to retrieve a structured summary of essential contact information for a specific person or entity.

07 **Can I draft messages for my team?**

Yes, the `draft_notification_messages` tool generates tailored, professional messages for different recipient types like technical support or approvers.

08 **What happens if a primary access method fails?**

You can use `evaluate_fallback_plan` to identify the specific alternative actions and commitments that must be activated.

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 `"accessible-contingency-contact-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

Accessible Contingency Contact 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 Accessible Contingency Contact 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	Accessible Contingency Contact Plan MCP
Server ID	`01a0d37c-24d9-71cd-8877-d6de386cff57`
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/accessible-contingency-contact-plan.