

DevOps & Security Audit Points (AI Edition)

Audit Points

- ☐ Where are AI keys stored and rotated?
- ☐ Do your logs contain any raw AI prompts or outputs? Are they redacted?
- ☐ Has a threat model for AI misuse or prompt injection been completed?
- ☐ What observability tools track AI performance, misuse, and errors?
- ☐ Are fallback workflows in place if the AI service is down or compromised?