SANCTUMSHIELD · AGENTIC GOVERNANCE FOR THE OTHER 99%

Responsibility Register

Who holds each AI governance responsibility today, by name.

Most organizations have the responsibilities without the titles. A regulator or an underwriter asks for the name, not the title. One name per row, a backup, and a date you last checked that it was still true.

Educational template, not legal advice.

Last updated: November 9, 2026

Responsibility	What it covers	Holder (one name)	Title today	Backup	Last reviewed
Trust engineering	Validates that AI systems conform to regulation and to contract				
Agentic workflow assurance	Keeps the end-to-end chain of automated decisions behind each critical service documented and reviewed				
AI testing and red-team coordination	Schedules and records jailbreak, prompt-injection and content-safety testing				
AI governance advice	Owns the AI Acceptable Use Policy and the				

Responsibility	What it covers	Holder (one name)	Title today	Backup	Last reviewed
	register's review cadence				
AI security operations	Operates and reviews the guardrails and the gateways				
AI forensics	Reconstructs what an agent did, from logs, after an incident				
Incident signatory (per agent)	Signs the incident report when an AI agent causes the incident				
Runtime control owner	Owns the per-action record that shows the action an agent executed is the one that was authorized				
Stop authority (per agent)	Can stop or pause the agent mid-task, and records the date that stop was last exercised				
Change approver (per agent)	Approves the changes an agent proposes, its scheduled tasks and any running past its quota				
Spend owner (per agent)	Owns what the agent spends and its cap				
MCP gateway owner	Owns each gateway or connector and the list of				

Responsibility	What it covers	Holder (one name)	Title today	Backup	Last reviewed
	systems behind it				
Document-grounded answers reviewer	Checks the cited document, version and page before an AI answer is used in a consequential decision				
Personal-account AI rule owner	Owns the staff rule on personal AI accounts and personal devices with company data				

How to use it. One accountable name per row, never a team. Where one person holds several rows, write the name several times; the point is that the question "who?" has an answer. Review the page when a holder changes role and at least quarterly. The AI Acceptable Use Policy generated by SanctumShield lists the same holders in its deployed-agent section, so the two records agree.

Governance is an ongoing program, never a one-time audit. Date this page when you fill it in, and again when you review it.

Terms: Responsibility register, Agent-incident signatory, Proven Stop. The Academy covers who holds what in module M6 (Stakeholder Map & RACI); see the Legal / Compliance track.

Free, and there is nothing to sign up for. The Board AI Register and the free Shadow AI Check are at sanctumshield.com/templates and sanctumshield.com/check.

© PIGENAI LLC · SanctumShield · sanctumshield.com · Last updated November 9, 2026 · This is an educational template, not legal advice.