SOP: MCP Agent Mapping & Tooling Strategy

*Generated: 03/09/2025 14:16*

# SOP: MCP Agent Mapping & Tooling Strategy

## 1.0 Purpose

.

## 2.0 The Two-Tiered Tooling Strategy

Our agentic model is divided into a high-level "Conductor" and low-level "Specialists." Their toolsets MUST remain distinct to ensure a clear separation of concerns.

* \*\*Conductor AI (`workflow\_orchestrator`):\*\* This agent operates at a high level of abstraction. It MUST only be equipped with MCPs that interact with project-level, cloud-based APIs.
* \*\*Specialist AIs (`dev\_implement`, `test\_generate`, etc.):\*\* These agents operate at the implementation level. They MUST only be equipped with MCPs that interact with the local development environment.

## 3.0 Agent-to-MCP Tool Mappings

The Orchestrator AI is responsible for enforcing these permissions.

|  |  |  |
| --- | --- | --- |
| **Agent (Sub-Agent)** | **Role in Workflow** | **Required MCP Tools** |
| \*\*`workflow\_orchestrator`\*\* | Conductor / Orchestrator | `Official GitHub MCP`, `Jira MCP`, `Slack MCP` |
| \*\*`dev\_implement`\*\* | Core Developer | `Official Git MCP`, `Filesystem MCP` |
| \*\*`test\_generate`\*\* | QA Engineer | `Filesystem MCP`, `Docker MCP` (for tests) |
| \*\*`security\_audit`\*\* | Security Auditor | `Filesystem MCP`, `GitHub MCP` (read-only history) |
| \*\*`asset\_find`\*\* | Research Assistant | `Web Search MCP`, `GitMCP` (for doc retrieval) |

## 4.0 Security Gateway Mandate

* It is responsible for managing all OAuth 2.1 with PKCE authentication flows for remote MCP servers.
* It MUST enforce explicit, granular user consent for every action that modifies state.
* It is responsible for sanitizing all data passed between agents and tools.

## 5.0 "Trust but Verify" Vetting Protocol

The MCP ecosystem contains a mix of official and community-driven servers of varying quality. A data exposure incident has been documented with a community server.

* \*\*Mandate:\*\* Before any new community-driven MCP server is integrated, it MUST undergo a formal security audit.
* \*\*Procedure:\*\* The audit will be performed by the `security\_audit` agent using the \*\*"SOP: Automated MCP Auditing Protocol"\*\* as its knowledge base. A "Low Risk" score is required for approval.
* \*\*Preference:\*\* Official servers from tool vendors (e.g., Atlassian, GitHub) are strongly preferred.

## 6.0 The Composite MCP Roadmap

. These are high-level tools that encapsulate complex, multi-step workflows into a single, reliable command.

* \*\*Example Candidate:\*\* `create\_pr\_from\_staged\_changes`
* \*\*Internal Workflow:\*\*

1. Call the `Official Git MCP` to `git\_add`.
2. Call the `Official Git MCP` to `git\_commit`.
3. Call the `Official Git MCP` to `git\_push`.
4. Call the `Official GitHub MCP` to `create\_pull\_request`.