AI SECURITY WORKING RESOURCE

MCP Tool Inventory and Blast Radius Worksheet

Trace each MCP tool to its permissions, credential, target and stop procedure.

Purpose

Complete this workbook before an MCP client receives access to internal systems, SaaS accounts, file stores, databases, messaging, repositories, deployment, or payment tools.

System / program	
Review owner	
Environment	[ ] Prototype [ ] Pilot [ ] Production
Review date / next review	

How to use this worksheet

- [ ] Use one row per system, tool, credential, source, action, or test. Add rows in Word when needed.
- [ ] Use factual system state. Do not place passwords, private keys, access tokens, or unnecessary personal data in the file.
- [ ] Assign an owner and verification step to every blocker. Re-review after architecture, permission, or model changes.
- [ ] This worksheet supports engineering review. It does not replace product-specific testing or a formal security assessment.

Handling note: keep credentials, customer identifiers, and restricted system details out of shareable copies.

WORKSHEET 01

MCP server and client inventory

Record each server-client relationship separately. A server that is safe for one client or environment may create a different exposure elsewhere.

Server / transport	Client and owner	Environment	Systems and data reached	Network / trust notes

Review prompts

[ ] Identify local, remote, stdio, HTTP, and gateway-mediated connections.

[ ] Record who can change server configuration, startup commands, tool definitions, or upstream endpoints.

[ ] Flag local filesystem, shell, browser, database, repository, messaging, deployment, and payment access.

WORKSHEET 02

Tool permission matrix

Use one row per tool. Tool descriptions can change model behavior, but server-side authorization must remain independent of those descriptions.

Tool and server	Action / target	Class	Default authorization	Destructive or external effect

Review prompts

[ ] Classify actions as read, write, delete, send, execute, approve, deploy, spend, or permission change.

[ ] Document default-deny rules, parameter allowlists, tenant checks, and resource-level authorization.

[ ] Treat send, delete, merge, deploy, payment, permission, and customer-visible actions as high impact.

WORKSHEET 03

OAuth scopes, tokens, and identity binding

Map the credential used by each tool to the human or service identity it represents, including scope, lifetime, storage, rotation, and revocation.

Credential / OAuth grant	Tools using it	Scopes and user binding	Lifetime / rotation	Revocation owner

Review prompts

[ ] Flag shared credentials and scopes broader than the tool's declared purpose.

[ ] Confirm revocation removes effective tool access, including caches, sessions, and downstream tokens.

[ ] Record whether approval is tied to the same human identity that owns the action.

WORKSHEET 04

Approval, logging, and rate controls

A useful action record connects the human principal to the exact MCP tool call and its result. Generic application logs are rarely enough.

Control check	Status and notes
Required approvals bind to the final arguments and target before execution.	[ ] Yes [ ] No [ ] N/A
The approval screen shows the exact resource, recipient, repository, environment, amount, or account.	[ ] Yes [ ] No [ ] N/A
Records include the request reference, tool, safe argument fields, approval, policy result, outcome and time.	[ ] Yes [ ] No [ ] N/A
Denied and policy-blocked calls are retained for review.	[ ] Yes [ ] No [ ] N/A
Rate limits constrain repeated calls, fan-out, and retry behavior.	[ ] Yes [ ] No [ ] N/A
Logs are protected from tool users and retained long enough for response and customer commitments.	[ ] Yes [ ] No [ ] N/A

Missing records, approval gaps, and remediation owner

WORKSHEET 05

Blast radius and emergency shutdown

Test the worst credible tool sequence, then verify that a named owner can stop it without depending on the agent, client, or compromised server.

Abuse path / sequence	Maximum impact	Containment control	Shutdown step	Test result / owner

Decision

Release posture	[ ] Ready [ ] Limited pilot [ ] Blocked [ ] Formal assessment needed
Conditions to proceed	
Decision owner / date	
Next verification	