

The MCP Security Checklist

Controls that reduce risk in a Model Context Protocol deployment. Based on OWASP, NSA, and vendor-neutral security practices. Use during design review, before production, or after adding a new MCP server. — MCP Security Hub, July 2026

1. Server Inventory & Trust

- ☐ Maintain a list of every MCP server your agents connect to.
- ☐ Verify the publisher or maintainer of each server.
- ☐ Review the source code or a trusted audit report before connecting third-party servers.
- ☐ Avoid installing MCP servers from unverified community repositories.

2. Authentication

- ☐ Every MCP connection uses authenticated sessions, not static tokens in config files.
- ☐ Tokens are stored in a secrets manager or OS keychain, not plaintext.
- ☐ OAuth scopes are limited to the minimum required actions.
- ☐ Per-client consent is enforced on the server side, not just in the client UI.

3. Authorization & Scope

- ☐ Each MCP tool has a documented permission scope.
- ☐ Agents cannot call high-risk tools without explicit approval.
- ☐ Tool permissions are reviewed when the server updates.
- ☐ A gateway or policy layer enforces deny-by-default for new tools.

4. Input & Output Validation

- ☐ Tool arguments are validated before execution.
- ☐ Tool responses are inspected for embedded instructions or prompt-injection payloads.
- ☐ Large or unexpected responses are rate-limited or truncated.

5. Monitoring & Logging

- ☐ Every tool call is logged with caller identity, arguments, and result metadata.
- ☐ Logs are shipped to a SIEM or centralized log platform.
- ☐ Anomalies trigger alerts: new servers, unusual argument patterns, high failure rates.

6. Runtime Isolation

- ☐ MCP servers run in a sandboxed process or container.
- ☐ Network egress from MCP servers is restricted.
- ☐ Local filesystem access is denied unless explicitly required.

7. Incident Response

- ☐ There is a runbook for revoking an MCP server.
- ☐ Compromised tokens can be rotated in under 15 minutes.
- ☐ Tool call logs are retained long enough to support forensics.