MCP Pre-Flight Checklist

Run through this before you connect an agent to any remote MCP server. Five minutes. Print it, keep it where you work.

Server: _____ **Date:** _____

Command used to start it: **Checked by:**

_____ _____

- [ ] **1. Who publishes this server?**

  Name, repo link, changelog. No public source means untrusted until proven otherwise.

- [ ] **2. Is the source code readable?**

  If yes, skim it. If no, note it here and connect with narrow permissions only.

- [ ] **3. Baseline saved before first use?**

  Run: node mcp-tool-diff.js --snapshot baseline.json -- . Read the tool list it prints.

- [ ] **4. Any surprising tools?**

  Email, shell, or network tools on a file server mean stop. A surprise is the checklist working.

- [ ] **5. Smallest scope set?**

  One directory, one database, least privilege. Scope is the cheapest security you will ever buy.

- [ ] **6. Network reach checked?**

  Which hosts can it call? Can that list change without you knowing?

- [ ] **7. Secrets handled safely?**

  Keys via environment variables, minimal permissions, never shared across servers.

- [ ] **8. Change rule agreed in advance?**

  When the diff reports a change, the server stays disconnected until the change is read. Decide now, calmly.

- [ ] **9. Baseline stored with the project?**

  Keep the snapshot file with the project, not in a temp folder. A baseline never read is not a baseline.

- [ ] **10. Re-check scheduled?**

  Weekly, and after every server update. An audit is a snapshot, not a monitor.

Verdict: ■ Approved ■ Not approved ■ Approved with narrow scope only

Notes: _____

_____