MCP GATEWAY SECURITY FOR LAW FIRMS

The gateway controls checklist for law firms

COCHA TECHNOLOGY

- [ ] Use delegated authentication for every MCP server that touches client documents.
- [ ] Prohibit shared service accounts and static API keys for document system servers.
- [ ] Keep an allowlist of approved MCP servers and block the rest.
- [ ] Block write tools by default and require approval for any exception.
- [ ] Gate permission changing tools, including sharing, labeling, moving and deleting, behind approval.
- [ ] Record the human user in the audit log, not only the gateway.
- [ ] Validate token audience on every request and prohibit token passthrough.
- [ ] Start clients with read scopes and step up only when a named process needs more.
- [ ] Prefer short lived tokens and revoke on offboarding.
- [ ] Sandbox local MCP servers or ban them on firm devices.
- [ ] Apply Power Platform data policies to Copilot Studio MCP connectors.
- [ ] Test ethical wall behavior after every connector change and every document move.
- [ ] Keep an inventory of agents, owners and the systems each can reach.
- [ ] Review tool lists whenever a vendor updates a connector, since tools can change.
- [ ] Name who can disable a connector, token or agent in an emergency, and test that revocation ends access.

Start with the free AI Readiness Snapshot **cochatechnology.com**
https://www.cochatechnology.com/ai-readiness-snapshot/

Full guide: https://www.cochatechnology.com/mcp-gateway-security-law-firms/