GP Solutions

Your AI Coding Security Checklist

Use this checklist to assess how well your development environment controls AI coding agents.

	SECURITY CONTROL	CHECK
☐	**Approved AI tools**	Is every AI tool, IDE extension, and MCP server in use on the approved list?
☐	**Sensitive-data restrictions**	Are .env files, secret stores, production logs, and customer records excluded from agent context by default?
☐	**Least privilege**	Does each agent have its own identity, read-only access by default, and expiring credentials?
☐	**Sandboxed environments**	Do agents run in temporary, isolated environments with outbound network access blocked by default?
☐	**Repository and tool trust**	Do sensitive tool calls require confirmation, with permissions enforced outside the model?
☐	**Dependency verification**	Is every new package checked against an allowlist or approved by a person before installation?
☐	**SAST, SCA, secret scanning**	Do these scans run on every pull request with AI-generated changes and block merging on findings?
☐	**Human review**	Does a qualified engineer review every change to authentication, authorization, cryptography, payments, or access controls?
☐	**CI/CD protection**	Do workflow file changes require a named reviewer, and are deployment credentials out of the agent's reach?
☐	**Audit log**	Can you trace any AI-assisted change back to who started it, which tools ran, and who approved it?
☐	**Human accountability**	Is a named person responsible for each high-risk approval, with autonomous merging prohibited in sensitive areas?

In case of any questions regarding secure AI-assisted coding, reach out to our team.

Talk to an Expert →