TAG1
tag1.com

A PRACTICAL AI SECURITY CHECKLIST

Use this anytime you are giving AI agents access to a new system, tool, or workflow.

1 BEFORE YOU CONNECT ANYTHING	**Ask: What is the worst thing this AI could do with this access?** Would you be liable for it?	☐
	Map every platform, system, and data source the agent will be able to touch.	☐
	Define the human–AI boundary explicitly. What can the agent do autonomously? What requires your approval?	☐
2 WHEN SETTING ACCESS PERMISSIONS	Start with read-only. Add write access only when the task requires it.	☐
	Write access should produce drafts, not published output. **The agent creates. You make it happen.**	☐
	Never let one agent hold all three S's simultaneously, including **sniffing access** to private data, susceptibility to **social engineering**, and unrestricted **send** capability.	☐
	Scope access to the specific task. One email thread, not the full inbox. Revoke access when the task is complete.	☐

THE GOLDEN RULE — The agent creates. You make it happen.

3 WHEN WORKING WITH FILES AND IMAGES	Strip metadata from files before sharing them with an agent. Images carry GPS coordinates and other data you may not intend to expose.	☐
	When possible, convert images before sharing them with an agent. Steganographic data can survive casual inspection.	☐
4 WHEN USING MCP OR API INTEGRATIONS	**Separate read and write actions at the integration level.** Read: permitted. Write: human approval required. Delete: always human-gated.	☐
	Require human sign-off at every irreversible step, including sending, deleting, purchasing, deploying, publishing.	☐
5 ONGOING	Maintain an audit log of every action your agent takes. Autonomous action requires a record.	☐
	Remember that a well-constructed phishing attempt, in your voice, with your credentials, is something an agent can produce. Social engineering applies to agents too.	☐
	If an agent behaves unexpectedly, treat it as a signal to refine the environment. Clearer boundaries almost always produce better behavior.	☐

Bring practical, proven AI adoption strategies to your organization — let's start a conversation!

support@tag1.com
+1 (727) 350-6344
tag1.com