

Seven lines for one agent. Each one a decision someone signs.

Write the set for one agent that is already live. Its owner in the room.

AGENT NAME		PURPOSE	OWNER — a named, accountable person
LINE		EXAMPLE · INVOICE AGENT	YOUR AGENT
1	Identity Its own identity. Not a person's account. Not a shared service account.	Its own agent identity, owned by the head of accounts receivable	
2	Credential life How long the token lasts and who can revoke it mid-task. Hours rather than months. Never a token that does not expire.	8-hour token. Finance or security can revoke it	
3	Reads Every source it reads, named. Mark content written outside the organisation.	Shared mailbox (outside content) · invoice ledger	
4	Tools and actions An allow list of named tools. Read or write for each. Anything not on the list is not permitted.	Ledger: read · Reminders: send · Payee records: none	
5	Limits Maximum value · maximum volume · maximum rate.	20 reminders an hour. Known customers only	
6	Approval Actions that need a person first. Start with anything irreversible, anything that leaves the organisation, and anything that moves money.	Any message outside the standard reminder	
7	Stop Who can stop it · how fast · what happens to work in progress · when the stop was last tested.	Accounts receivable lead, within 5 minutes. Queue held. Tested last month	
.	Logging Every action logged under the agent's own identity.	Logged under the agent's identity	

WORST-CASE TEST The worst thing it could do before a person intervenes, in one sentence. If you cannot write it, the set is not finished.

Invoice agent: twenty wrong reminders in an hour. Small. Visible. Easy to put right.

FIX FIRST Runs as a person · a token that never expires · a deny list instead of an allow list.	MONDAY Pick one agent already live, not one in design. Write the seven lines with its owner in the room.	WHAT IT IS NOT A working set, not an OWASP template. A permission set nobody signed is still a default.
---	--	---

OWNER	SECURITY	DATE	NEXT REVIEW
-------	----------	------	-------------

Reference: OWASP Top 10 for Agentic Applications 2026 — ASI02 Tool misuse and exploitation; ASI03 Identity and privilege abuse; the principle of least agency. genai.owasp.org