AI Agent Security Proof Packet

TechSaaS | Security and Compliance Evidence Pipeline Setup | June 8, 2026

Use this one-page packet before an AI agent is approved for a customer-facing workflow, procurement answer, or security review. The goal is one artifact that shows what the agent can do, what it cannot do, where evidence lands, and who owns rollback.

Five Fields To Fill Before Approval

1. Allowed Tools

Exact tools, commands, scopes, queues, APIs, and environments the agent may touch.

2. Blocked Actions

Production writes, customer messaging, billing changes, privilege edits, and denied paths.

3. Secret Boundary

Scoped tokens, storage location, rotation owner, and data that must never enter prompts or logs.

4. Audit Receipt

Dated log, run receipt, approval note, denied-action event, and reviewer confirmation.

5. Rollback Owner

The person who can reverse the action, notify support or sales, and update the buyer-safe answer after an incident.

Evidence Lane

Buyer Question	Required Proof	Owner	Review Date
What tools can the agent use?	Tool-token matrix and environment scope	Platform lead	Next release gate
Can it touch customer data?	Data boundary, redaction rule, blocked-path receipt	Security owner	Security review date
How do you prove what happened?	Audit log, approval note, run receipt, rollback note	Ops owner	After material workflow change

Comment Keyword Handoff

LinkedIn keyword: PROOF. When someone comments PROOF, reply with this packet and route the lead as source linkedin, campaign linkedin-agent-security-proof-format-20260608, content proof_packet_text, guide slug agent-security-proof-packet.

Implementation path

Security and Compliance Evidence Pipeline Setup
https://techsaas.cloud/services/security-compliance-evidence-pipeline