

AI Policy Crash Test

Aona-sponsored workshop worksheet · 2026-10-01T06:11:11.926Z

Workshop: Not entered · Review: Not set

Environment: Not entered

User-entered observations only. No infrastructure inspection, security score, independent validation or coverage certification. Tests, uploads and scans are not performed by this utility.

Use synthetic data only under separately approved test scope.

1. Same AI tool. Different account.

An employee drafts a public announcement in an approved business account, then switches to a personal account in the same browser.

Synthetic input: "Summarise the public launch agenda for ExampleCo."

Can the control distinguish the approved business account from a personal account?

Expected control / scope: Not defined

Status: Untested / unknown

Collect: Record the allowed/blocked route, account class and policy version without storing identifiers.

Observation: Not recorded

Owner: Unassigned · Review: Not set

Can you attribute each decision to the right user, device and tenant?

Expected control / scope: Not defined

Status: Untested / unknown

Collect: Reference a sanitized event and timestamp. An app name alone does not establish account or tenant attribution.

Observation: Not recorded

Owner: Unassigned · Review: Not set

2. The extension is logged out.

A new browser session opens before the extension signs in. A second check uses a private window, where extension access may differ.

Synthetic input: "Explain this fictional office lunch menu."

What happens before extension sign-in and in a private window?

Expected control / scope: Not defined

Status: Untested / unknown

Collect: Record both routes separately: prevention, explicit exception or unknown. Do not assume protection follows installation.

Observation: Not recorded

Owner: Unassigned · Review: Not set

Can IT tell that this browser is outside the expected protection state?

Expected control / scope: Not defined

Status: Untested / unknown

Collect: Reference a posture alert, inventory entry or documented exception. Observe it; do not infer it from the icon.

Observation: Not recorded

Owner: Unassigned · Review: Not set

3. A browser pass is not a desktop pass.

An employee repeats an approved synthetic request in a desktop AI app. A mobile route is assessed separately, including unmanaged-device limits.

Synthetic input: "Rewrite this fictional meeting agenda."

Are browser, desktop and mobile routes individually covered or documented as excluded?

Expected control / scope: Not defined

Status: Untested / unknown

Collect: Record the OS, app version, device management and each route. A single browser result cannot answer this check.

Observation: Not recorded

Owner: Unassigned · Review: Not set

Does the event identify the actual device and input path?

Expected control / scope: Not defined

Status: Untested / unknown

Collect: Compare sanitized evidence for each authorized route. Record missing paths as untested or unsupported.

Observation: Not recorded

Owner: Unassigned · Review: Not set

4. A sensitive file reaches the boundary.

A fictional employee prepares a synthetic file with clearly labeled fake personal and confidential fields. They discuss paste and file-upload behavior separately.

Fixture: "SYNTHETIC ONLY · Person: Alex Example · ID: TEST-000 · Contract: fictional £123."

Does the expected allow, redact or block outcome hold for paste and file upload?

Expected control / scope: Not defined

Status: Untested / unknown

Collect: Use only separately authorized synthetic checks. Record file type, route and redacted/blocked result; no real data or uploads in this utility.

Observation: Not recorded

Owner: Unassigned · Review: Not set

Does risky-only logging match the policy and preserve useful evidence?

Expected control / scope: Not defined

Status: Untested / unknown

Collect: Compare a harmless synthetic request with a flagged one. Record retained metadata, content policy and retrieval limits without pasting logs here.

Observation: Not recorded

Owner: Unassigned · Review: Not set

5. A plausible answer is still unverified.

An AI-generated supplier summary includes a fictional unsupported certification claim. The draft is about to be sent to a customer.

Synthetic output: "Example Vendor is certified to Fictional Standard 9000."

Can the employee spot and withhold the unsupported claim before external use?

Expected control / scope: Not defined

Status: Untested / unknown

Collect: Record the source check and reviewer decision. Prompt protection does not establish factual accuracy.

Observation: Not recorded

Owner: Unassigned · Review: Not set

Is there a named human review step for consequential output?

Expected control / scope: Not defined

Status: Untested / unknown

Collect: Reference the approved review process and responsible role. An AI-generated confidence statement is not evidence.

Observation: Not recorded

Owner: Unassigned · Review: Not set

6. An employee leaves. A vendor changes.

A test user is offboarded and an AI vendor changes its account terms. IT also needs an authorized, clean agent uninstall on a test device.

Tabletop fixture: TEST-USER leaves; Example Vendor changes its retention terms.

Are account access, policy ownership and vendor approval rechecked after the change?

Expected control / scope: Not defined

Status: Untested / unknown

Collect: Record revocation verification and an approval owner/date. A closed ticket alone does not prove access ended.

Observation: Not recorded

Owner: Unassigned · Review: Not set

Can IT remove the agent cleanly and verify the new coverage state?

Expected control / scope: Not defined

Status: Untested / unknown

Collect: Use a separately authorized test device only. Reference uninstall result, residual permissions and updated inventory; no uninstall occurs here.

Observation: Not recorded

Owner: Unassigned · Review: Not set

Optional Aona demo

30-minute product demo to discuss relevant controls and scoped coverage. Not a security audit.

https://aona.ai/book-demo?intent=ai_policy_crash_test

No worksheet answers are transmitted.