

Employee AI security evaluation checklist

Version: 19 September 2026.

Synthetic tests only. This is an evaluation worksheet, not a completed test or coverage certification.

Before the test

- ☐ Use an approved non-customer environment and a dedicated test group.
- ☐ Record the AI product and interface, OS, browser, installed Aona version and policy version.
- ☐ Record backend hosting and prompt-processing placement separately.
- ☐ Agree the action to test: block, redact or another explicitly supported policy response.
- ☐ Use the supplied fictional examples, never customer prompts, secrets or documents.
- ☐ Define pass, fail and not-tested before running the test. An empty result means not tested.

Prompt checks

- ☐ 1. Submit a clean synthetic prompt as a negative control.
- ☐ 2. Test typed and pasted sensitive prompts separately.
- ☐ 3. For block: confirm the request is not submitted and the employee has no continue override.
- ☐ 4. For redact: compare original and submitted content, the employee notice and the retained useful task.
- ☐ 5. Confirm the event identifier and policy outcome for that same attempt.
- ☐ 6. Repeat on each app and client in scope. A result on ChatGPT does not establish Claude or desktop coverage.

Evaluation checklist continued

Document checks

- ☐ 1. Build the sample DOCX from file-test-recipe.md. Keep an unchanged original.
- ☐ 2. Test attachment button, drag-and-drop and multiple-file paths separately where supported.
- ☐ 3. Compare the original, returned document and submitted content.
- ☐ 4. Check names, email addresses, account fields, paragraphs and table layout.
- ☐ 5. Test XLSX formulas, hidden sheets/comments and PDF text/scanned pages separately. Do not assume support from the extension alone.
- ☐ 6. Record rejection, failure and recovery behavior for unsupported or malformed content.

Sentinel checks

- ☐ 1. Record the connector artifact/version, API contract and test workspace.
- ☐ 2. Trace one synthetic EventOriginalUid from the source API to AonaEvents_CL and Aona().
- ☐ 3. Compare EventTime, Disposition and the query result. TargetAppName is Aona in the current mapping.
- ☐ 4. Check overlapping-poll deduplication, missing periods, pagination and event completeness.
- ☐ 5. A local fixture or parser check is not a live Sentinel-ingestion result.

Decision record

Use test-record.json. Capture evidence location, observed result, exclusions, reviewer and next action. Record not-tested explicitly. Remove customer identifiers and credentials from every artifact before sharing it.

Read current coverage: <https://aona.ai/resources/ai-security-coverage/>

Read deployment options: <https://aona.ai/resources/ai-security-deployment/>

Discuss your security evaluation: <https://aona.ai/book-demo/>