

Before staff rely on an AI knowledge base

Document fixes first, then a six-step test, built from dated evidence (Stanford, 30 May 2024; Moffatt v. Air Canada, 14 Feb 2024; OpenAI and Microsoft documentation, 2026). Our method, not an industry standard.

1 One current version per topic

Archive old price lists, expired policies and superseded templates outside the folders the knowledge base reads.
Air Canada's chatbot contradicted Air Canada's own policy page (2024 BCCRT 149, 14 Feb 2024).

2 An owner and a date on each document

When an answer is wrong, someone must know which file to correct and when it was last checked.

3 A written scope, and clean sharing

Decide which questions it may answer and which it must refuse. Remove 'everyone' links on sensitive folders before connecting anything.

Microsoft Copilot blueprint, updated 18 Aug 2026: first pillar 'Remediate oversharing'.

4 Collect 30 to 50 real questions

Use questions staff or customers asked in the past three months, in their own words.

5 Add 5 to 10 questions the files cannot answer

The right response is 'I don't know', not a guess.

Stanford 2024: legal tools built on curated sources hallucinated on 17–33% of 202 questions.

6 Check every source on a sample

For at least ten answers, open the cited passage and confirm it says what the answer claims.

Stanford counts answers that 'falsely assert a source supports a statement' as hallucinations.

7 Plant an outdated document

Put an old version beside a current one and see which the knowledge base quotes.

8 Run a two-person permission test

Ask the same question as two people with different access. The one without access must not get the file's contents.

9 Repeat after every change

Run the same set again whenever documents, models or settings change, and keep the results.

Limits to know

- ChatGPT Business projects hold up to 40 files; a custom GPT up to 10 knowledge files for its lifetime (OpenAI help, October 2026).
- Outside ChatGPT Enterprise, ChatGPT reads only a file's digital text, not its embedded images.
- Customer-facing answers are statements by your company: hold them for review where the stakes are high.

Not legal advice. Sources and full notes: yardwork.dev/en/blog/ai-knowledge-base. Provider limits change; re-check the dates above before relying on them.