

# Reducing Your AI Risk Exposure

Five ways to lower your exposure  
without giving up what works

**Risk lives in a handful of specific decisions, not in the technology itself.** You don't have to ban AI to be careful, and you don't have to commit to it to get value. Most exposure comes from things nobody decided on purpose: a feature a vendor switched on, a free account someone opened to hit a deadline, a draft that went out because everyone assumed someone else had read it. Five checks. No IT department required.

## Start here

If AI touches **decisions about people** — who your organization serves, who gets hired, who gets placed, who gets scheduled — that outranks everything below. Clients, employees and volunteers all count. The person affected by a mistake isn't in the room to catch it. Everywhere else on this page you can take your time. Not here.

### 1 Have someone read it before it goes out

**ASK** Does anything AI helped write reach a client, funder, or the public without a person who would catch a mistake reading it first?

**WATCH FOR** "Someone skims it" and "depends who's busy" both mean no.

### 2 Get it off personal accounts

**ASK** Is any of this happening on someone's personal login?

**WATCH FOR** A personal account leaves no record of who put what in, nothing to switch off when someone quits, and it takes the history with them. **78% of knowledge workers using AI at work bring their own tools.**

### 3 Put in less than you think you need

**ASK** What kind of information actually has to go in?

**WATCH FOR** Client records, giving history and board financials are not the same as general boilerplate. Usually the whole file went in because that was faster.

### 4 Find out whose model is learning from you

**ASK** Do your inputs train the tool — and does anything it writes feed a decision without being checked?

**WATCH FOR** Free tiers commonly train on what you type. Your strategy and your language become someone else's training data.

### 5 Know how to pull it all back

**ASK** If someone asked you to delete everything your team has put into an AI tool, could you?

**WATCH FOR** "I don't know" is the most common answer. That is the finding.

Written for the people who make the decisions, not the people who run the network. Firewalls, logins and monitoring matter too — those belong with your IT partner. These five are yours.

#### SOURCES

Anthropic, *Zero Trust for AI Agents*, 2026 — the five principles this page adapts ([claude.com/blog/zero-trust-for-ai-agents](https://claude.com/blog/zero-trust-for-ai-agents)). · Microsoft & LinkedIn, *2024 Work Trend Index Annual Report: AI at Work Is Here. Now Comes the Hard Part*, May 2024 — 75% of knowledge workers use AI at work; 78% of them bring their own tools; 60% of leaders say their organization lacks a plan and vision ([microsoft.com/worklab/work-trend-index](https://microsoft.com/worklab/work-trend-index)). · Insights4Equity, *Is Your Tech Stack Working For You? A People-Centered Assessment Guide for Nonprofits* — companion guide ([insights4equity.com](https://insights4equity.com)).

Ready to go deeper?  
Reach out to start a conversation.

[www.insights4equity.com](https://www.insights4equity.com) · [info@i4eq.com](mailto:info@i4eq.com)

Scan to book  
a 30-minute  
conversation

