AI Safety Checklist

for Small Businesses

16 practical steps to reduce AI risk in your business

Your employees are already using AI tools. The question is whether they're doing it safely. This checklist covers the 16 most impactful steps small businesses can take to protect customer data, prevent AI fraud, train employees, and stay ahead of regulatory requirements.

Work through each section with your team. Check off what you've done. Prioritize what you haven't. Use it as the foundation for your AI policy.

TOOLS & VENDOR VETTING | DATA PROTECTION | EMPLOYEE TRAINING & POLICY | FRAUD & COMPLIANCE

HOW TO USE THIS CHECKLIST

Print this checklist and work through it with your operations or HR lead.
For each item: ☐ Done · ☐ In progress · ☐ Not started — prioritize the ☐ items.
Share the completed checklist with your team as evidence of your AI governance process.

Not legal advice. This checklist is for informational purposes only. Consult a licensed attorney for guidance specific to your business and jurisdiction.

TOOLS & VENDOR VETTING

1 **Build an approved AI tools list**
Document every AI tool your team uses. Evaluate each for data retention, privacy policy, and security…

2 **Review free-tier data policies**
Free accounts on ChatGPT, Otter.ai, and similar tools often retain inputs by default. Verify settings…

3 **Check for SOC 2 certification**
Any AI tool handling customer or employee data should hold SOC 2 Type II certification or equivalent.…

4 **Review vendor change-of-control clauses**
AI companies are acquired frequently. Confirm your contract addresses what happens to your data if the…

DATA PROTECTION

5 **Classify your sensitive data**
Define what data is off-limits for AI tools: customer PII, financial records, health info, legal…

6 **Audit what employees are sharing**
Ask your team what they're entering into AI tools. Many businesses discover sensitive data is being…

7 **Opt out of model training where available**
ChatGPT Team/Enterprise and many other tools offer opt-outs from model training. Enable these settings…

8 **Establish a data retention review cycle**
Review AI vendor data retention policies annually, and whenever a vendor updates its terms of service or…

EMPLOYEE TRAINING & POLICY

9 **Deploy a written AI use policy**
A policy doesn't need to be long. It needs to answer: approved tools, prohibited data, content review…

10 **Train employees before they use AI tools**
Don't wait for an incident. Train new hires on your AI policy during onboarding and all staff at least…

11 **Establish a human review step for AI output**
Any AI-generated content used in customer communications, legal documents, or public materials must be…

12 **Create an AI incident reporting process**
Employees need a clear, low-friction way to report AI-related incidents — accidental data sharing,…

FRAUD & COMPLIANCE

13 **Implement a callback policy for payment changes**
Any request to change vendor banking information must be verified by calling the vendor at a number you…

14 **Train staff to recognize AI voice and video fraud**
AI voice cloning and deepfake video are being used to impersonate vendors and executives. Establish…

15 **Review FTC AI advertising compliance**
AI-generated testimonials, reviews, and advertising claims are subject to FTC disclosure requirements.…

16 **Document your AI use for regulatory readiness**
Maintain a record of your AI tool inventory, use cases, and review processes. This documentation is your…