KIMREY CONSULTING

AI Governance Starter Kit for Small Business

A practical starting point for using AI responsibly — without creating unnecessary bureaucracy.

PREPARED BY KIMREY CONSULTING

kimreycg.com

Why AI Governance Matters

Every time an employee pastes a client email into ChatGPT, drafts a proposal with Copilot, or asks Gemini to summarize a contract, your business is already making a decision about AI risk — whether or not anyone has written it down.

AI governance is not a legal mandate or a compliance formality for most small businesses. It is simply the practice of deciding, *on purpose*, how your team uses these tools — instead of leaving those decisions to chance, habit, or whichever employee is most comfortable experimenting.

The organizations that get this right rarely start with a lengthy policy manual. They start by answering four practical questions: which tools are allowed, what information can go into them, when a human needs to check the output, and what gets written down. That is the entire starting point — and it is achievable in a single afternoon.

The Point

You don’t need a 40-page policy to govern AI responsibly. You need four decisions, made on purpose, written down, and reviewed periodically.

The Four Essentials

These four elements — grounded in the structure of the NIST AI Risk Management Framework — form a lightweight governance baseline that any small business can put in place without new software, new staff, or new bureaucracy.

1

Approved Tools
Decide which AI tools your team may use for business purposes, and communicate the list clearly. Unapproved, informal “shadow AI” use is where most avoidable risk hides.

2

Data Rules
Set clear boundaries on what information can and cannot be entered into an AI tool — client records, health information, financials, employee data, and trade secrets, at minimum.

3

Human Review
Require a qualified person to review AI-generated output before it informs a decision, reaches a client, or is published. AI drafts; people decide.

4

Documentation
Keep a simple written record of what tools are approved, what rules apply, and when they were last reviewed. Documentation is what turns good habits into an actual program.

One-Page Implementation Framework

A simple reference for translating the Four Essentials into ownership and routine. This is the entire framework — there is no additional layer beneath it.

Essential	What to Decide	Who Should Own It	Review Frequency
Approved Tools	Which AI platforms and plans staff may use for work	Owner or operations lead	Quarterly, or when a new tool is requested
Data Rules	What information may never be entered into an AI tool	Owner, or privacy/compliance lead if applicable	Semi-annually, or after handling a new data type
Human Review	Which AI outputs require review before use, and by whom	Department or team leads	Quarterly
Documentation	Where the policy lives and how it is communicated	Owner or office manager	Annually, at minimum

Why This Maps to NIST

The National Institute of Standards and Technology's AI Risk Management Framework (AI RMF 1.0) organizes AI risk management into four functions: Govern, Map, Measure, and Manage. The framework above is a small-business-scale translation of that same logic — govern (ownership), map (what to decide), measure (documentation), and manage (review cadence).

READY TO ADAPT

Sample One-Page AI Use Policy

Editable model language your business can adopt as-is or adjust to fit your industry and risk profile. Replace bracketed placeholders with your organization's specifics.

Approved Tools	[Company Name] employees may use the following AI tools for work purposes: [lis approved tools, e.g., ChatGPT Team/Business, Microsoft Copilot, Google Gemini Use of any other AI tool for company business requires prior approval fror [owner/role].
Prohibited Data	Employees must not enter the following into any AI tool unless it has bee specifically approved for that purpose: client-identifying information, patient c health records, Social Security numbers or financial account details, employe personnel data, trade secrets, and unpublished financials or contracts.
Human Review	AI-generated content must be reviewed by a qualified team member before it i sent to a client, used in a business decision, or published externally. AI output is draft, not a final product.
Accuracy Checks	Employees are responsible for verifying the factual accuracy of AI-generate content — including statistics, citations, names, dates, and figures — before it i used or shared.
Client Confidentiality	AI tools that have not been approved for confidential use must never be used t process client-identifiable, protected health, or contractually confidentia information.
Documentation	[Company Name] will maintain a written record of approved tools, data rules, an review responsibilities, updated whenever tools or practices change.
Policy Review	This policy will be reviewed at least [annually / semi-annually] by [owner/role] an updated as AI tools, regulations, or business needs evolve.

FROM READING TO DOING

30-Day Action Plan

A realistic pace for a small business to move from no policy to a working one — without pulling anyone off their regular job for more than an hour a week.

Week 1	**Inventory Current AI Use** Ask each team or department which AI tools they are already using, formally or informally. Flag any high-risk uses involving client, health, or financial data.
Week 2	**Approve Tools and Data Rules** Finalize your approved-tools list and draft data-handling rules using the sample policy language on the previous page.
Week 3	**Assign Human Review Responsibilities** Decide which AI outputs require review before use, and assign that responsibility by role. Build it into existing workflows rather than creating new ones.
Week 4	**Publish and Train the Team** Share the finalized policy with all staff, hold a short briefing (15–20 minutes is enough), and put a review date on the calendar.

QUICK SELF-ASSESSMENT

Final Checklist

Use this to confirm your governance basics are in place. If you can check every box, you are ahead of most small businesses using AI today.

- ☐ An approved AI tools list is documented and shared with the team
- ☐ Written data rules define what may and may not be entered into AI tools
- ☐ A qualified person reviews AI output before it is used externally
- ☐ Responsibility for accuracy checks is clearly assigned
- ☐ Client confidentiality rules specifically address AI tool use
- ☐ The policy exists in writing, not just as a verbal understanding
- ☐ A review date is scheduled on the calendar
- ☐ All employees have been briefed on the policy

Disclaimer

This guide is provided for general educational purposes by Kimrey Consulting. It does not constitute legal, compliance, or cybersecurity advice and should not be relied upon as a substitute for guidance from a qualified attorney, compliance professional, or security specialist. AI governance obligations vary by industry, jurisdiction, and business circumstances; businesses in regulated industries — including healthcare and financial services — should consult appropriate legal or compliance counsel before finalizing a policy.

NEXT STEPS

Build a Governance Framework That Fits Your Business

This starter kit is a foundation, not a finished program. Every business handles different data, works in different regulatory environments, and takes on different risk. Kimrey Consulting helps small businesses, healthcare administrators, and professional service firms translate frameworks like this one into a practical, right-sized AI governance approach.

Visit **kimreycg.com** or contact Kimrey Consulting to get started.

Sources & Further Reading

• National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1 — nist.gov/itl/ai-risk-management-framework

• U.S. Small Business Administration, AI Resources for Small Business — sba.gov/business-guide/manage-your-business/ai-small-business

• Businesses in regulated industries should also confirm applicability of relevant federal and state guidance specific to their sector.