Mirazon

GUIDE

How to Create an AI Use Policy (Without Killing Innovation)

How SMBs Can Create Smart AI Guardrails with Confidence

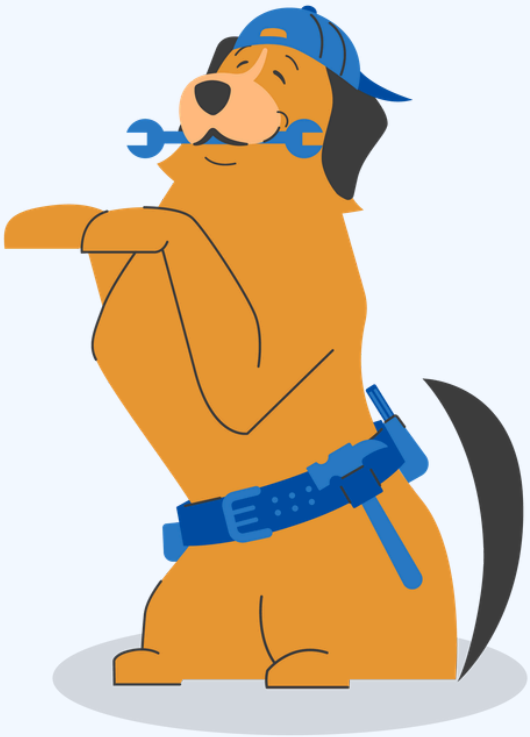
www.mirazon.com
(502) 240-0404
info@mirazon.com

The AI Reality for SMBs (Hint: You've Been Living It for Years...)

AI didn't arrive with a rollout meeting or a formal approval process. It quietly showed up in inboxes, browser tabs, and everyday workflows. One employee uses it to draft emails. Another leans on it for research. Someone else uses it to help analyze a large data set. And the list goes on and on.

None of this is unusual, and that's exactly the point. For small and midsize businesses (SMBs), AI adoption isn't happening *strategically* first; it's happening *organically*. This leaves many SMB leaders asking an uncomfortable question: ***Are we actually okay with how AI is being used in our business right now?***

An AI Use Policy isn't about slowing teams down or saying "no" to new tools. It's about giving people **clarity**, **consistency**, and **confidence** so AI becomes a strength, not a gamble. This guide is here to help SMBs put practical guardrails in place without losing momentum or creativity along the way.



Why an AI Use Policy Matters for SMBs

AI isn't coming. It's already here. Your employees are using tools like ChatGPT, Copilot, and AI-powered SaaS features every day to write emails, analyze data, and move faster. That's a good thing… until it isn't. Without clear guardrails, AI use can quietly introduce security risks, compliance issues, data leakage, and even brand damage. An AI Use Policy helps SMBs strike the balance between encouraging innovation and protecting the business so teams can use AI confidently, responsibly, and productively instead of guessing what's allowed.

An effective policy isn't about fear or restriction; it's about clarity. When employees know where the lines are, they're far more likely to use AI in ways that actually support business goals. And for leadership, it creates a shared understanding of risk, accountability, and expectations around rapidly evolving technology.

Key Benefits of Having an AI Use Policy

Reduces Risk of Sensitive Data Exposure

Sets Clear Expectations for Employees and Contractors

Supports Compliance and Governance Requirements

Encourages Responsible, Value-Driven AI Adoption

Protects Brand Reputation and Intellectual Property

DID YOU KNOW?

Only 23% of organizations have a formal AI governance or security policy in place, even as AI use becomes widespread across daily business operations.

Source

Start With Clear Intent: What AI *Should* Be Used For

Before writing policy language, SMBs need to align on intent.

The goal isn't to list every AI tool on the planet. It's to define how AI should support the business. That means identifying approved use cases that improve efficiency, creativity, and decision-making while staying aligned with company values and risk tolerance. When intent is clear, policies feel empowering instead of restrictive.

This is also the time to define where AI adds the most value today. Is it content creation? Data analysis? Internal documentation? Customer communications? Anchoring the policy in real-world workflows helps employees understand *why* the policy exists, not just *what* it says. A strong AI policy starts by saying "yes" to the right things before it says "no" to anything.

"When intent is clear, policies feel empowering instead of restrictive."

Examples of Approved AI Use Cases

- **Drafting Internal Documents or First-Pass Marketing Material**
- **Brainstorming Ideas or Summarizing Non-Confidential Data**
- **Improving Productivity in Analysis or Reporting Workflows**
- **Enhancing Customer Support with Approved AI Platforms**

Define the Guardrails: Data, Security, and Privacy

This is where most SMBs get nervous, and rightly so.

AI tools often learn from the data they're given, which means sensitive information can travel further than intended. A strong AI Use Policy clearly defines what cannot be shared, uploaded, or processed through AI tools, such as sensitive customer data, financial information, intellectual property, and anything covered by regulatory requirements.

But here's where a lot of organizations get tripped up: not all AI tools are created equal.

There's a big difference between public, open AI tools and private, licensed platforms built for business use. What you *never* allow in a public GPT might be perfectly acceptable in a secure, approved environment. Your policy should make that distinction clear, so employees aren't left guessing or overcorrecting.

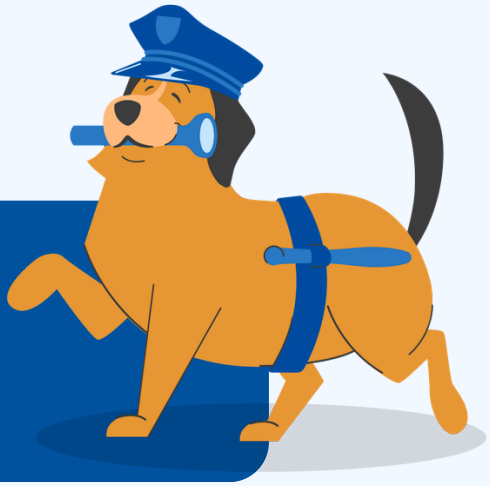
By clearly spelling out those boundaries, SMBs protect both their people and their business. Employees shouldn't have to wonder if something is okay to share with AI. Your policy should make that decision easy. This is also the place to align AI usage with your existing security policies, acceptable use policies, and compliance frameworks, so nothing lives in a silo.

Common Data Guardrails to Include in Your AI Use Policy

- No use of confidential, regulated, or customer data in public AI tools
- Clear definitions of "sensitive" vs. "non-sensitive" data
- Guidance on approved AI platforms and when to use them
- Distinction between public, open tools and private, licensed tools, i.e., approved AI environments
- Enforcement of existing security and privacy policies

Ultimately, these guardrails aren't about slowing innovation. They're about making AI safe to use with confidence. When the rules around data, security, and privacy are clear, employees can focus on using AI to work smarter instead of worrying about crossing a line.

With the boundaries set, the next step is to ensure everyone understands how AI *should* show up in their day-to-day work.



"When the rules around data, security, and privacy are clear, employees can focus on using AI to work smarter, instead of worrying about crossing a line."

Set Expectations for Employees and Leadership

An AI Use Policy only works if everyone understands their role in it. That means setting expectations not just for employees, but for leadership, managers, and IT teams as well.

Who approves new AI tools? Who reviews usage? What happens if the policy is violated? Clear accountability keeps policies from becoming shelfware.

This section should also emphasize responsible judgment. AI outputs aren't automatically correct, and employees should understand they're still accountable for the work they produce with AI assistance. When expectations are communicated clearly and respectfully, teams are far more likely to follow them.

Expectations Your Policy Should Clarify

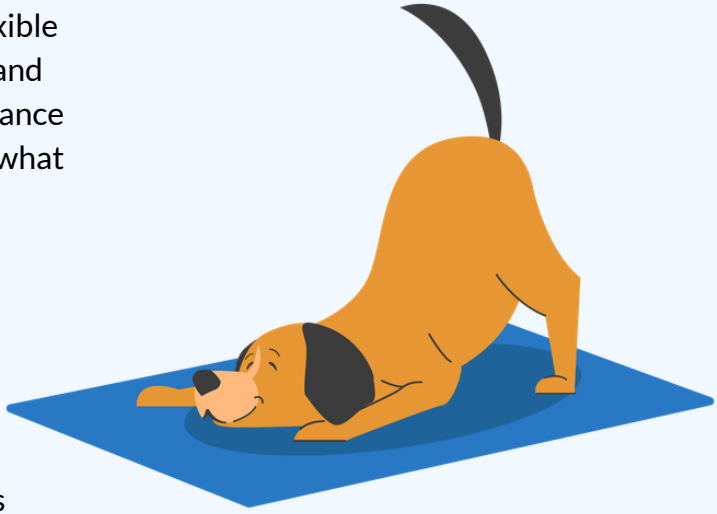
- Employees are responsible for reviewing and validating AI output
- AI does not replace human judgment or oversight
- An approval process for adopting new AI tools
- Consequences for misuse or policy violations

Keep It Actionable, Not Overwhelming

The biggest mistake SMBs make with AI policies? Overcomplicating them.

A policy that's too long, too legal, or too technical won't be read or followed. The best AI Use Policies are concise, written in plain language, and grounded in real scenarios employees encounter every day. Think guidance, not a legal dissertation.

AI will continue to evolve, and your policy should be flexible enough to evolve with it. Build in regular review cycles and make updates part of your normal IT or security governance rhythm. The goal is progress, not perfection. Start with what you know today and adapt as the technology changes.



Tips for Keeping Your AI Policy Effective

- Use plain language and real-world examples
- Keep it short enough to actually be read
- Review and update annually (or sooner if needed)
- Train employees on the "why," and not just the rules

Common Mistakes SMBs Make with AI Policies

Many SMBs don't struggle with AI policies because they don't care. They struggle because the approach misses the mark. AI gets handed off to IT, a policy gets written in a vacuum, and suddenly there's a long list of "do nots" that doesn't reflect how people actually work. When that happens, the policy feels out of touch from day one, and employees either ignore it or quietly work around it.

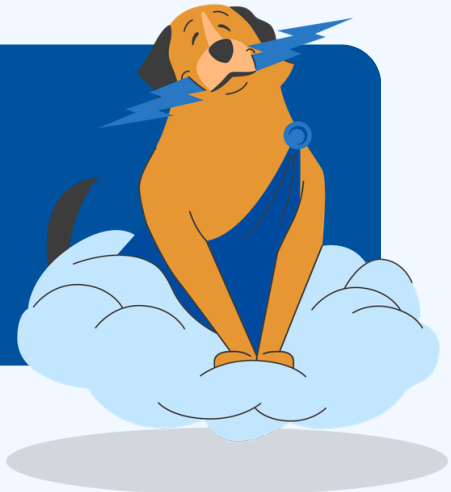
We also see SMBs unintentionally create hesitation instead of clarity. If a policy is too restrictive or bans tools people already depend on, AI use doesn't stop—it just goes unspoken. Add in the instinct to "deal with it later," and many organizations wait until a close call or data scare forces action. The strongest AI policies come from being proactive, practical, and honest about how AI is already being used across the business.

Common Pitfalls

- Treating AI as strictly an IT problem
- Writing policies that prohibit instead of providing guidance
- Making the policy too vague to be useful in real situations
- Ignoring tools employees already rely on
- Rolling out the policy once and never revisiting it
- Failing to train employees on what the policy actually means in practice
- Waiting for a data incident before taking action
- Overlooking how AI intersects with existing processes and tools

The most effective AI policies strike a balance: protecting the business while enabling smarter work.

"The strongest AI policies come from being proactive, practical, and honest about how AI is already being used across the business."



DID YOU KNOW?

68% of organizations experienced data leakage tied directly to employee AI usage, often through sharing sensitive information with generative AI tools.

Source

How We Help SMBs Get AI Policies Right

Creating an AI Use Policy doesn't have to be overwhelming or done in isolation. At Mirazon, we help SMBs turn uncertainty about AI into confident, practical action. We work with your leadership, IT, and security teams to build policies that reflect how your business actually operates while reducing risk and unlocking value from AI responsibly.

Whether you're just starting to explore AI or already knee-deep in adoption, we help you create clear guardrails, align policies with security best practices, and prepare your organization for what's next. **Because AI should be a competitive advantage, not a ticking time bomb.**

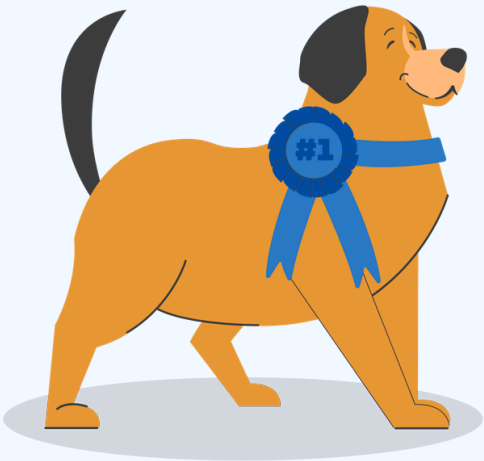
How Mirazon Supports AI Governance for SMBs

- AI Policy Development Tailored to Your Business
- Identifying Where and How AI is Already Being Used
- Alignment with Security, Compliance, and Risk Strategy
- Creating Policies that are Practical and Enforceable
- Employee Education and AI Readiness Planning
- Ongoing Guidance as AI Tools and Regulations Evolve

AI is moving fast, but that doesn't mean SMBs have to move blindly.

With the right guidance, you can put smart policies in place that protect your business *and* help your people do their best work.

Mirazon helps you take a thoughtful, right-sized approach to AI so you can move forward with confidence, not hesitation.



Ready to Put Smart Guardrails Around AI?

AI is *already* changing how work gets done inside SMBs, often faster than policies can keep up. Whether it's drafting emails, analyzing data, or speeding up everyday tasks, your teams are using AI today. The difference is whether they're doing it with clear guidance and confidence or figuring it out as they go.

Mirazon helps SMBs **take control** of that reality. We work with you to put practical, people-friendly guardrails in place that protect your business while empowering your teams to **use AI the right way**. No panic. No overcomplication. Just smart, intentional progress.

Let's talk about building an AI use policy that supports how your business works *right now* and where it's headed next.

Contact Us

Mirazon®

www.mirazon.com
(502) 240-0404
info@mirazon.com