Mindset180

AI Usage Policies

A Practical Guide for Risk-Aware Organizations

With Sample Policy Frameworks for Regulated Industries and SMBs

Before we begin...

What this guide is:
A starting point

What it is not:
Legal advice or a complete policy

Who it's for:
Leaders, managers, and professionals navigating
real-world AI use

Why AI Policies Matter Now

Most organizations did not make a formal decision to adopt AI.

It arrived quietly:
- Built into everyday tools
- Used by individuals to save time
- Introduced without shared rules

At the same time:
- Expectations are rising
- Decisions are happening faster
- Accountability is getting blurry

An AI policy is not about slowing people down.
 It is about making responsibility clear.

Good policies:
- Create safe boundaries
- Support learning and experimentation
- Protect people, data, and reputation

Bad or rushed policies:
- Sit on a shelf
- Create false confidence
- Push AI use underground

Mindset180 Insight

Most organizations discover AI risk after it already exists.
Policies are often written in response to fear, not understanding.
That's when they do the least good.

A Reality Check Before You Start

It's important to be clear about one thing:

A policy does not create safety by itself.

Safety comes from:
- Clear ownership
- Informed users
- Risk awareness
- Ongoing review

Policies without training and governance often create silence instead of safety.

This guide is designed to help you see what an effective AI policy must address before you try to finalize one.

If you finish this document thinking,

"We have more questions than answers."

That's a healthy outcome.

Mindset180 Insight

A policy can say what's allowed.
It cannot explain judgment, context, or tradeoffs.
Those must be learned.

What All Good AI Policies Have in Common

Across industries and organization sizes, strong AI policies share a few traits:

- People remain accountable
- Controls scale with risk
- AI supports decisions; it does not replace them
- Data protection comes first
- Learning is expected, not optional

With that foundation, the next sections include two sample policy frameworks:

1. A structured example for regulated environments
2. A lighter-weight example for SMBs and early adopters

Both are intentionally incomplete.

PART I

Sample AI Usage Policy - Regulated of High-Risk Environments

Audience: Healthcare, financial services, insurance, government-adjacent, or highly regulated organizations

Purpose: Show structure and intent, not provide a finished policy

Mindset180 Insight

In regulated environments, risk usually comes from good intentions paired with unclear boundaries. Most failures are process failures, not technology failures.

HeathTech, Inc.

AI Usage Policy

This policy defines how AI tools may be used responsibly within the organization.
Its goals are to:
- Enable appropriate AI use
- Protect sensitive and regulated data
- Clarify ownership and accountability
- Reduce legal and operational risk

Scope

This policy applies to:
- Employees, contractors, and vendors
- All AI tools used for work purposes
- Company-approved and personally sourced tools

If AI is used to support work, this policy applies.

Guiding Principles

AI use within the organization follows these principles:
- **Human Accountability**
  - People remain responsible for decisions and outcomes.
- **Risk-Based Controls**
  - Higher-risk use requires stronger oversight.
- **Transparency**
  - AI-assisted outputs must be explainable and reviewable.
- **Data Protection**
  - Sensitive and regulated data must be protected at all times.

Mindset180 Insight

"Human-in-the-loop" only works if someone is trained, empowered, and expected to say no.
If no one can explain the output, accountability has already been lost.

AI Usage Policy

Acceptable Use

AI tools may be used for:
- Drafting non-sensitive documents
- Summarizing internal materials without regulated data
- Research using public information
- Idea generation and analysis

All outputs must be reviewed by a human before use or distribution.

Prohibited and Restricted Use

AI tools must not be used for:
- Processing PII, PHI, PCI, or confidential client data
- Making autonomous decisions affecting people, finances, or compliance
- Training models using organizational data without approval

Mindset180 Insight

Many AI tools retain context to improve results. That strength becomes a liability when users assume inputs disappear.

Data Handling and Privacy

Users must:
- Avoid entering sensitive data
- Anonymize information when possible
- Follow existing data classification rules

When unsure, stop and escalate.

AI Usage Policy

Roles and Responsibilities

- Executive Sponsor: Owns AI governance
- AI Owner: Oversees approved use cases and policy alignment
- Managers: Ensure team understanding and compliance
- Users: Validate outputs and raise concerns

Escalation and Review

Concerns must be escalated when:
- Outputs appear incorrect or biased
- Data exposure is suspected
- Use cases exceed policy boundaries

PART II

Sample AI Usage Policy - SMB and Early Adoption Environments

Audience: Small to mid-sized organizations
Purpose: Enable learning without creating chaos

Mindset180 Insight

Smaller organizations are not "too small" for AI risk.
They are simply less protected from mistakes.

Innovai, LLC

AI Usage Policy

This policy supports responsible AI use while protecting customers, employees, and the business.

Acceptable Use

AI tools may be used for:
- Writing and summarization
- Internal analysis using non-sensitive data
- Learning and skill development

All outputs must be reviewed before use.

Not Allowed

AI tools must not be used for:
- Sensitive customer or employee data
- Automated decisions with real-world impact
- Presenting AI output as verified fact

Responsibility and Escalation

AI assists work.
 It does not own outcomes.

When unsure:
1. Pause
2. Ask
3. Document

Mindset180 Insight

Early adoption should focus on understanding, not speed.
Automation without understanding scales mistakes faster than value.

What This Guide Does Not Provide

This guide does not include:

- Risk classification models
- Tool approval workflows
- Training programs
- Enforcement mechanisms

These cannot be created responsibly without understanding your organization.

Mindset180 Insight

Policies answer what is allowed.
They do not answer who is ready.
That gap is where most AI failures begin.

A Better Question to Ask

Instead of asking:
"Do we have an AI policy?"

Ask:
"Do we understand how AI is being used, and who is accountable when it goes wrong?"

For many organizations, the honest answer is not yet.

How Mindset180 Helps

Mindset180 works with organizations that want to:
- Enable AI safely
- Avoid policy theater
- Build literacy alongside governance
- Create guardrails people actually follow

Our work includes:
- AI readiness assessments
- Policy and governance co-creation
- Leadership and user education
- Ongoing advisory support

If this guide raised questions, that's a sign you're thinking about AI the right way.

Final Thought

**AI does not need blind trust or blanket fear.
It needs clarity, capability, and accountability.**

Mindset180

For enquiries reach out to: contact@mindset180.com