{{company}} AI Policy

Executive Summary | One-Pager

What We're Doing

We're implementing a formal AI policy that governs how {{company}} employees and contractors use AI tools (ChatGPT, Claude, Gemini, Copilot, etc.).

The rule in one sentence: If you wouldn't email it to a stranger on the internet, don't paste it into an AI tool.

Why Now?

AI tools are everywhere. Most of our team uses them. Without guardrails, we risk:

• **Data breach:** Accidental exposure of customer PII, payment data, or trade secrets (company-ending risk)
• **Regulatory exposure:** Customer data sent to third-party AI services violates GDPR, HIPAA, PCI-DSS, etc. (legal liability)
• **IP theft:** Our product roadmap, pricing, and algorithms could be exposed (competitive disadvantage)
• **Compliance gaps:** Board, auditors, and customers are asking "what's your AI governance?" (business risk)

The upside: Clear rules = confidence that employees can use AI tools safely, boosting productivity without the fear.

Risk Mitigation

■ **Before policy:** Sarah, a customer success manager, pastes top 10 customer names and spend into ChatGPT to get ideas for upsells. Data retention unclear. Competitor could see it.

■ **After policy:** Sarah knows Tier 2 requires anonymized data. She asks security for help sanitizing the list. Security reviews, approves. Sarah uses Claude API with the anonymized data. No risk.

Implementation Plan

Week 1: Announce policy, get team buy-in, run manager training

Week 2: Train all teams on the 4-tier framework

Week 3: Enforcement begins; ChatGPT Free is off-limits

Week 4: Measure compliance, iterate on policy

Ongoing: Monthly reviews, quarterly training for new hires, exception requests for new tools.

Success Metrics

Compliance: 80%+ of teams using approved tools
Violations: <5 total over 30 days
Exceptions: <10 requests (shows the rule is working)
Data breaches: 0 customer data leaks attributable to AI tool usage

The Policy (TL;DR)

Tier 1 (Approved): General writing, brainstorming, coding help. No approval needed. Use {{approvedAiTool}}, ChatGPT Pro, Claude.ai

Tier 2 (Approved-with-controls): Anonymized internal data. Manager approval. Use {{approvedAiTool}} only

Tier 3 (Needs-review): High-risk decisions (strategy, security, M&A;). Security + legal sign-off, 5 days. Use {{approvedAiTool}} only

Tier 4 (Banned): Customer PII, payment data, passwords, trade secrets. Never, no exceptions

Enforcement

First violation: Retrain + audit of uploaded data.

Second violation: Escalation to leadership + discipline.

Egregious (customer data): Termination.

We monitor using DLP tools, access logs, and manager reports. Employees can report violations anonymously.

Next Steps

Monday: Review + approve this policy

Tuesday: Announce to all-hands

Weeks 2–4: Follow the rollout playbook