Enterprise AI Acceptable Use Policy & Data Classification Framework

***AIThinkerLab** | Trust First Governance for Secure, Scalable AI Adoption*

Prepared by: AIThinkerLab
Purpose: Trust-First Governance for Secure, Scalable AI Adoption

This document provides a trust-first framework for responsible enterprise AI adoption. It balances innovation, security, and intellectual property protection while enabling employees to use AI tools transparently and safely.

1. Executive Summary

Artificial Intelligence is now embedded in everyday enterprise work. Employees across functions are already using AI tools to improve productivity, decision-making, and speed of execution. However, without clear guidance and approved pathways, this reality creates a growing **Shadow AI risk**—where AI is used outside organizational visibility, security controls, and governance frameworks.

This policy provides a **practical, enterprise-ready approach** to managing AI adoption responsibly. It is designed to balance **innovation and speed** with **security, intellectual property protection, and organizational trust**. Rather than relying on restrictive bans or intrusive monitoring, the framework emphasizes **enablement, transparency, and shared accountability**.

2. Guiding Principles

a. Enable innovation rather than restrict it
b. Build trust instead of surveillance
c. Protect data, IP, and customer confidence
d. Maintain human accountability for AI outcomes

3. Data Classification Model

a. Red Data: PII, source code, trade secrets — no public AI usage
b. Yellow Data: Internal documents — approved enterprise AI only
c. Green Data: Public content — public AI allowed with human review

4. Acceptable AI Use Guidelines

a. Use approved enterprise AI tools whenever available
b. Never input confidential or proprietary data into public AI tools
c. Validate all AI generated outputs before use or publication

5. Intellectual Property & Ownership Protection

All AI assisted work created using approved systems remains the property of the organization. Employees must not use personal AI accounts to develop proprietary products, algorithms, or features. AI outputs must be reviewed to avoid copyright contamination or trademark risk.

6. Shadow AI Disclosure & Amnesty

The organization encourages voluntary disclosure of AI tools currently used for work. Good faith disclosure will not result in disciplinary action. The purpose is to improve visibility, security, and enablement — not punishment

7. Monitoring & Governance

Monitoring exists to guide policy and improve tooling, not to surveil individuals. System level insights may be used to identify trends, improve training, and strengthen enterprise AI governance.

8. Training & Awareness

The organization commits to ongoing AI literacy training covering safe usage, prompt hygiene, data classification, and evolving risks associated with generative AI

9. Policy Review & Evolution

This policy will be reviewed periodically to align with technological change, regulatory developments, and organizational needs. Updates will be communicated clearly.

Disclaimer: This document is provided as a general framework and should be reviewed by legal and compliance teams before formal adoption.