# AI Usage Policy

# (for Small & Mid-Sized Businesses)

*Prepared BY: SafeAi for business*

horizontal line

# AI Usage Policy for Small and Mid-Sized Businesses

**Purpose:**  
This policy establishes rules and expectations for the safe, ethical, and compliant use of Artificial Intelligence (AI) tools within our organization. It aims to protect data, ensure responsible use, and align with international frameworks (ISO/IEC 42001, NIST AI RMF, EU AI Act, GDPR).

**Scope:**

This policy applies to all employees, contractors, and third-party vendors who use, procure, or manage AI systems and tools on behalf of the organization.

## Policy Statements:

* AI must only be used for approved business purposes, never for personal gain or unauthorized activities.
* Data used in AI tools must be accurate, relevant, and handled in compliance with GDPR and local privacy laws.
* High-risk AI applications (e.g., decision-making on hiring, finance, or safety) require senior management approval.
* Human-in-the-loop oversight is mandatory for AI decisions that significantly affect individuals or business operations.
* Sensitive or confidential data must not be uploaded into public AI tools without anonymization and prior approval.
* Third-party AI vendors must undergo due diligence for security, compliance, and reliability.
* Employees must complete training on ethical and secure AI use before using AI-powered systems.
* AI outputs must be verified for accuracy before use in official reports, communications, or customer-facing activities.
* All AI use must comply with intellectual property laws, copyright protections, and licensing agreements.
* Incidents, misuse, or potential AI-related risks must be reported immediately to the Quality or Compliance team.

## Roles and Responsibilities:

Management: Approves high-risk AI use, ensures compliance, and provides resources for oversight.

Employees: Follow policy, complete training, and report risks or misuse.

IT/Quality Team: Monitor AI use, conduct audits, and manage vendor assessments.

Vendors: Demonstrate compliance with this policy and relevant frameworks.

**Enforcement:**

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract. Vendors in violation may face contract termination.

**References:**

* ISO/IEC 42001: AI Management Systems.
* NIST AI Risk Management Framework.
* ISO/IEC 27001: Information Security.
* EU AI Act (2024)
* GDPR.

Disclaimer: This policy is provided as operational best practice, not legal advice.