BASIC AI ACCEPTABLE USE POLICY

Sample Starting Point for Small and Mid-Sized Businesses

Purpose

The purpose of this policy is to establish guidelines for the responsible, secure and appropriate use of artificial intelligence (AI) tools within the organization. This policy is intended to reduce operational, security, legal and compliance risks while enabling employees to use approved AI technologies productively and responsibly.

Scope

This policy applies to all employees, contractors, temporary staff and third-party users with access to company systems or data. This policy applies to all AI technologies used for business purposes, including generative AI platforms, AI assistants and copilots, AI-enabled productivity tools, AI-powered analytics or automation tools and AI features embedded within approved business software.

Approved AI Tools*

Employees may only use AI tools that have been approved by the company. Approved AI tools may include Microsoft Copilot, Google Workspace AI tools, approved CRM or PSA embedded AI tools, approved cybersecurity AI platforms and other company-authorized AI applications. The use of unauthorized public AI platforms for business purposes may be restricted or prohibited.

Prohibited Use

Employees may not use AI tools to upload, share or process confidential company information without authorization; input customer protected information, regulated data or sensitive business data into unapproved AI systems; generate discriminatory, harassing or inappropriate content; make fully autonomous business decisions without human oversight; circumvent security, compliance or privacy requirements; create misleading, fraudulent or deceptive content; violate copyright, intellectual property or licensing obligations; or upload source code, credentials or security-sensitive information into unapproved AI platforms.

Human Oversight Requirements

AI-generated content, recommendations or outputs must be reviewed by a human before external publication, customer delivery, financial decisions, legal or contractual use, HR or hiring decisions, security or compliance actions and executive or operational decision-making. Employees are responsible for validating the accuracy and appropriateness of AI-generated outputs.

Data Security and Privacy

Employees must follow all company security and data protection policies when using AI tools, avoid entering confidential or regulated data into unapproved AI systems, use company-approved AI tools whenever possible and report suspected data exposure or misuse immediately.

AI Transparency and Disclosure

When appropriate, employees should disclose when content or materials were substantially generated or assisted by AI, particularly in customer-facing communications, marketing materials, reports or recommendations and public-facing work.

Ownership and Intellectual Property

All work product created using company-approved AI systems for business purposes remains the property of the organization, subject to applicable vendor licensing terms. Employees may not use AI tools in ways that violate copyright or intellectual property laws.

Monitoring and Compliance

The company reserves the right to monitor use of company-approved AI systems, audit AI-related activities conducted on company systems, restrict or revoke access to AI tools and update approved AI tool lists and governance requirements. Failure to comply with this policy may result in disciplinary action.

Policy Governance

The organization will periodically review and update this policy to address regulatory changes, security developments, vendor changes, emerging AI risks and business operational requirements.

Employee Acknowledgment

All employees are expected to review, understand and comply with this policy as part of their ongoing responsibilities.

Recommended Next Steps

As organizations mature, they can expand this policy to include AI vendor review procedures, AI risk classification tiers, industry-specific compliance requirements, AI procurement standards, shadow AI detection processes, AI governance committees, Responsible AI frameworks and AI audit and retention requirements.

Disclaimer

**This sample policy is intended as a general informational starting point and should be reviewed by legal, compliance and security professionals before formal adoption.*