Artificial Intelligence Acceptable Use Policy

Template

This policy template should be modified to ensure it conforms to the control posture and reflects the risk tolerance of the specific business environment.

POLICY NAME	Artificial Intelligence Acceptable Use Policy
DESCRIPTION	Ensure artificial intelligence (AI) systems and tools are used only for authorized business purposes and in accordance with applicable law.
OWNER	Chief information officer (CIO)
EFFECTIVE DATE	Immediately
REVIEW FREQUENCY	At least annually

INTRODUCTION

Purpose for Policy

The purpose of this policy is to set out principles to help ensure the ethical and responsible deployment of AI at Company LLC and ensure that all employees adhere to the AI acceptable use policies and procedures and that appropriate disciplinary or mitigation actions are taken against those who violate this policy.

Scope of Policy

This policy applies to:

a) All employees, contractors, consultants, temporary staff, interns, visitors, and other workers at Company LLC, including all personnel affiliated with third parties
b) All Company LLC locations where IT resources are located or used
c) All Company LLC IT resources
d) Any information not specifically identified as the property of other parties that is transmitted or stored on Company LLC IT resources (including email, text and chat messages, and files)
e) All devices connected to a Company LLC network or used to access Company LLC IT resources
f) All systems, tools, or services including those enabled with generative AI such as ChatGPT (collectively, "AI Systems")

Exceptions

Any exceptions to this policy require submission and approval of appropriate documentation in accordance with the established policy exception process "xxxxx." Exceptions deemed high risk will be escalated to and reviewed by the "xxxxx Risk Forum" and recorded in the risk register.

GUIDELINES AND REQUIREMENTS

1. **Securing AI Systems**
    - AI systems that generate content that could be harmful if misused must be protected against unauthorized access and tampering.
    - AI systems must be fully tested to be secure and in line with privacy standards at all stages of the AI system life cycle.
    - Company data must not be shared with generative AI tools like ChatGPT unless part of an approved process.
    - A feedback approach must be established to help ensure the trustworthiness of AI outputs (e.g., contents, decisions, etc.) and system performance.

2. **AI Ethics**
    - Processes must be developed, reviewed, and approved prior to AI system or tool implementation to ensure all AI system use does not create or reinforce damaging biases.
    - Mechanisms must be in place to ensure algorithmic-based decisions for AI-enabled systems and tools are transparent and can be explained by an authorized human.
    - The appropriate multidisciplinary stakeholders must be identified and engaged in all AI system and tool strategy, requirements, testing, implementation, and maintenance to help ensure legal compliance, technical feasibility, and alignment with business and societal values.

3. **AI Acceptable and Unacceptable Use**
    - Use of AI-enabled systems and tools must be limited to well-defined, legitimate purposes and comply with ethical and privacy company policies and relevant external regulations and laws.
    - AI-enabled systems must not be used to violate laws, compromise systems or users, internal or external to the company.
    - Inappropriate use of AI-enabled systems and tools must be monitored, and policy violations must be reported to the appropriate level of management (e.g., chief information security officer [CISO]).
    - Company information technology policies apply to AI-enabled systems and tools. This policy does not supersede or negate information technology policy or other company policies (e.g., information security, privacy, code of conduct, etc.).

4. **Data Handling and Training**
    - Data can only be used for training and testing AI systems if there is explicit permission from the data owner and if the use aligns with applicable personal data regulations.
    - Sensitive and confidential data used for training and testing AI systems must be deidentified and anonymized to ensure privacy.
    - Mechanisms must be established to ensure data quality and the accuracy and reliability of the generated output.

5. **AI Transparency and Attribution**
    - AI-generated content that is shared or published is mandated to have the appropriate disclosures and/or other indicators (e.g., watermarks, inherent limitations of AI models, copyright, etc.).
    - A steering committee led by the CISO or another technically qualified designate will provide the required human oversight and establish mechanisms to review, approve, and validate AI-generated projects and resultant content or AI outputs for compliance with policy and applicable external regulations and laws.

6. **Violations and Reporting**
    - Reporting and investigation mechanisms must be established to ensure suspected violations of this policy are evaluated and appropriate action is taken.

ROLES AND RESPONSIBILITIES

1. The Company LLC board, audit and risk committee, and IT committee are ultimately accountable for the management of risk related to AI-enabled systems and tools and are supported by the senior leadership team (SLT) and chief operating officer (COO), who oversee AI-enabled system and tool deployment strategy, funding, and resourcing.

2. The chief information officer (CIO) has the authority to:
   a. Establish AI-enabled systems and tools policies, standards, and guidelines.
   b. Assign management responsibilities for AI-enabled systems and tools.

3. The chief information security officer (CISO) is accountable for:
   a. Management of overall Company LLC AI-enabled system and tool risk
   b. Providing AI-enabled systems and tools advice and user awareness
   c. Designing and implementing the Company LLC AI-enabled systems and tools strategy in consultation or partnership with the enterprise AI specialist/leader
   d. Managing AI-enabled systems and tools specific to information security incidents

4. Company LLC senior management is accountable for managing risk related to AI-enabled systems and tools within their area of responsibility.

5. Information resource owners are responsible for:
   a. Assessing, reporting, and escalating AI-enabled system and tool risk associated with their IT resources
   b. Assessing and managing AI-enabled system and tool risk associated with their third-party service providers
   c. Overseeing all access to their AI-enabled system and tool IT resources
   d. Management assurance over their AI-enabled system and tool controls

CONSEQUENCES OF POLICY VIOLATIONS

Breaches of this policy and/or the Code of Conduct shall be considered grounds for disciplinary action up to and including dismissal.

QUESTIONS/CONTACT INFORMATION

For questions about the Artificial Intelligence Acceptable Use Policy or any material addressed herein, please email the CIO Policy group (or Information Security or CISO group) at xxxxxxx@CompanyLLC.com.

DOCUMENT INFORMATION

Document Location	Z:\Policies & Procedures\Policies\IT Policies

VERSION HISTORY

Version	Date	Author	Additional Information
V1.0	xx/xx/xx		

DOCUMENT REVIEW

Version	Date	Reviewed By	Additional Information
V1.0			Approved