Artificial Intelligence (AI) Policy

Date of Change	Summary of Change	Change Made By	Approved By
07/31/25	Initial version	Caleb Long	

Contents

Purpose

This document establishes guidelines for the responsible use of Artificial Intelligence (AI) tools and systems used within the organization.

Scope

This policy and supporting procedures encompass all information systems that are owned, operated, maintained, and controlled by <Company Name> and all other information systems, both internally and externally, that interact with these systems, and applies to all employees, consultants, contractors, agents, and authorized users accessing business IT systems and applications whose conduct, in the performance of work for <Company Name>, is under the direct control of <Company Name>, regardless of compensation for services/work by <Company Name>.

Roles and Responsibilities

Implementing and adhering to organizational policies and standards is a collaborative effort, requiring a true commitment from all personnel, including management, internal employees, and users of information systems, along with vendors, contractors, and other relevant third parties. Additionally, by being aware of one’s roles and responsibilities as it pertains to <Company Name> information systems, all relevant parties are helping promote the confidentiality, integrity, and availability principles for information security in today’s world of growing cybersecurity challenges.

- **Management Commitment:** Responsibilities include providing overall direction, guidance, leadership, and support for the entire information systems environment, while also assisting other applicable personnel in their day-to-day operations. The Security Program Manager is to report to other members of senior management on a regular basis regarding all aspects of the organization’s information systems posture.
- **Internal Employees and Users:** Responsibilities include adhering to the organization’s information security policies, procedures, practices, and not undertaking any measure to alter such standards on any <Company Name> information systems. Additionally, end users are to report instances of non-compliance to senior authorities, specifically those by other users. End users – while undertaking day-to-day operations – may also notice issues that could impede the safety and security of <Company Name> information systems, and are to also report such instances immediately to senior authorities.
- **Vendors, Contractors, and Third-Party Entities:** Responsibilities for such individuals and organizations are much like those stated for end users: adhering to the organization’s information security policies, procedures, practices, and not undertaking any measures to alter such standards on any such system components.

Policies

AI Policy

<Company Name> shall implement sufficient governance, processes, and technical controls to ensure that risks related to the use of Generative AI tools and agents are understood and managed.

- The organization must name a senior management official to serve as the AI Officer
- Management must maintain accountability for all decisions supported by AI
- Use of AI tools must be monitored to ensure compliance with the organization's policies and procedures
- Output of AI tools must be subject to human oversight to ensure accuracy
- Processes that leverage AI for automation must include the ability for humans to override AI actions as necessary
- Derivative works created from AI output by <Company Name> personnel in the course of their work for the organization become the intellectual property of <Company Name>
- Use of AI tools must be disclosed to management
- Only approved AI tools may be used within the organization

Acceptable Use-Cases for AI

The following are examples of acceptable uses of AI at <Company Name> This list is not exhaustive.

- Code Review
- Drafting or suggesting code fragments
- Meeting summaries
- Marketing content creation
- Drafting communications
- Drafting documentation
- Drafting presentation materials
- Querying documentation
- Research and analysis of information
- Data analysis and reporting

Unacceptable Use-Cases for AI

The following are examples of unacceptable uses of AI at <Company Name>. This list is not exhaustive.

- Making final decisions regarding business, personnel, technical, or security matters
- Generating financial reports
- Generating legal guidance

- Performance review evaluations
- Handling customer data without written authorization from the customer
- Processing Protected Health Information

AI Specific Vendor Risk Review Criteria

- AI tools must be documented and reviewed under <Company Name>’s vendor risk management program prior to use within the organization
- Vendors must not use <Company Name> data to train their models

Policy Compliance

If you are found to have breached this policy, you may be subject to <Company Name>’s disciplinary procedures. If you have broken the law, you may be subject to prosecution. If you do not understand the implications of this policy or how it applies to you, contact the AI officer.

The Director of Human Resources in collaboration with the member's department management will determine the level of corrective action, if warranted, based on the nature and severity of the violation