AHA! INSIGHTS TECHNOLOGY, LLC

AI Governance Policy

LAST REVISION DATE August 19th, 2024

1. Purpose

The purpose of this AI Governance Policy is to define guidelines for the ethical, secure, and responsible use of Artificial Intelligence (AI) within our organization. This policy ensures that all AI-related activities align with our values, respect user privacy, and comply with legal and regulatory requirements.

2. Scope

This policy applies to all AI systems, models, and processes used, developed, or maintained by the organization. It covers the collection, storage, processing, and use of data by AI systems, including any third-party AI services including OpenAI and AWS.

3. Definitions

- **Artificial Intelligence (AI):** The simulation of human intelligence by machines to perform tasks such as learning, reasoning, and problem-solving.
- **Sub-processors:** Third-party entities that process data on behalf of our organization, specifically related to AI systems.
- **Data Flow:** The movement and handling of data from collection through processing, analysis, and storage, including interactions with external systems.

4. Governance Principles

a. Ethical AI Use

We are committed to developing and deploying AI systems in a manner that is ethical, transparent, and fair. Our AI models:

-
- **Prompt Engineering and Input Control:** We control the inputs sent to AI systems, ensuring that neutral language is used to minimize the risk of biased outputs.
- **User Feedback:** We provide mechanisms for users to report any responses they consider biased or inappropriate, and we use this feedback to improve our interactions with AI systems.

- **Human Oversight Where Appropriate:** Human oversight is maintained in critical decision-making processes or where AI outcomes have significant consequences, to ensure that AI remains aligned with ethical standards.

b. Data Privacy and Protection

We take the protection of personal and sensitive data seriously. To ensure compliance with privacy regulations:

- **Data Minimization:** Only the minimum necessary data is collected for AI purposes, and personal data is anonymized or de-identified where feasible.
- **Data Security:** All data used for AI training and processing is encrypted at rest and in transit. Access is restricted to authorized personnel.
- **Third-party Services:** Any third-party AI services or sub-processors (e.g., OpenAI, AWS) must comply with our data protection and security standards. Sub-processors will be reviewed periodically for continued compliance.

c. Compliance with Legal and Regulatory Standards

Our AI systems comply with relevant laws and regulations, such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and other applicable data protection laws. This includes obtaining user consent for data processing where required and providing data access and deletion rights to users.

d. Bias Mitigation

We actively test our AI models for potential biases including regular audits of AI outputs.

e. Model and Data Security

We take steps to protect our AI models and data:

- **Security of Models:** AI models are protected from adversarial attacks and data poisoning through input validation and security reviews.
- **Access Control:** Only authorized personnel have access to AI models, training datasets, and output results.
- **Incident Response:** Our security team monitors for anomalies and will respond quickly to any security incidents, including those involving AI.

f. Transparency and Explainability

We commit to providing stakeholders with information about how AI models operate, how data is processed, and how decisions are made. Users will have access to explanations for decisions that affect them and will be informed when AI is used.

5. Monitoring and Continuous Improvement

- **Model Performance Monitoring:** AI models are continuously monitored for accuracy, fairness, and unintended outcomes. Feedback from users is incorporated into the development cycle for model improvement.
- **Regular Audits:** Periodic audits will be conducted to ensure compliance with this policy and to evaluate the effectiveness of AI systems in meeting our ethical and performance standards.

6. Roles and Responsibilities

- **AI Governance Committee:** Oversees AI strategy, ethical guidelines, and compliance with this policy. Reviews and approves new AI initiatives.
- **Technology Team:** Our technology team is responsible for developing, deploying, and maintaining AI systems. They oversee compliance with this policy, manage security practices, and ensure that AI interactions align with our governance principles.

7. Incident Response

In the event of a security breach or unintended outcome involving AI systems, the organization will:

- Immediately notify relevant stakeholders.
- Investigate and mitigate the incident to minimize impact.
- Take corrective measures to prevent future incidents.

8. Policy Enforcement and Compliance

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment, as well as legal consequences. Regular reviews of AI use cases will ensure alignment with this policy and regulatory requirements.

9. Policy Review

This policy will be reviewed annually or whenever significant changes to AI technology, legal requirements, or business practices occur.