Artificial Intelligence Governance Policy			
AI-GV-P1			
Effective Date: 01/31/2025	**Date Approved:** 01/15/2025	**Version:** 1	**Page #:** 1 of 6

BACKGROUND

Artificial Intelligence (AI) Governance Policy is a set of technologies, systems, and algorithms using machine learning techniques in response to user inputs to create new content such as code, images, text, simulations, videos, 3-D objects, etc., and/or deliver predictions, recommendations, or decisions influencing real or virtual environments. Some examples below are:

- Textual (ChatGPT, Bard, etc.)
- Visual (Canva, DALL-E, etc.)
- Spoken (Polly/LEX, ElevenLabsM4t, etc.)
- Musical (Amadeus Code, etc.)

AI poses risks such as data inaccuracies, embedded bias, unauthorized use or presentation of sensitive data or intellectual property, and security and/or privacy exposures.

GOVERNANCE

This document is governed by the IT Governance policy which provides the following guidance:

a. Roles and Responsibilities
b. Policy Control Application
c. Policy Compliance Requirements
d. Policy Exceptions and Exemptions
e. Policy Reviews and Updates

SCOPE

This policy provides the planning, implementation, procurement, security, privacy, and governance requirements for AI, and authorizes the implementation of AI while establishing an operational framework to assist in protecting the confidentiality, integrity, and availability of data delivered through AI solutions.

This policy covers all State information and information systems to include those used, managed, or operated by a contractor, an agency, or other organization on behalf of the State. This policy applies to all State employees, contractors, and all other users of State information and information systems that support the operations and assets of the State.

APPLICABILITY

This policy is based on National Institute of Standards and Technology (NIST) Artificial Intelligence (AI) Risk Management Framework Version 1.0 (RMF v1.0) and noted sources below. This policy covers all State information and information systems including those used, managed, or operated by a contractor, employee, agency, or other organization on behalf of the State. This policy applies to all State employees, contractors, and all other users of State information and information systems supporting the operations and assets of the State.

IT activities shall require adherence to this policy and include but are not limited to the following:

- **Development:** Creating, integrating, or acquiring AI systems and models.
    - Coding (software development, enhancement, modification, etc.)
- **Deployment:** Integrating AI systems into operational workflows.

- **Use:** Utilizing AI systems to assist in decision making.
    - Writing policies, legislation, regulations, emails, texts, memorandums, etc.
    - Proofreading any written communication or media.
- **Attestation:** Agencies implementing Generative AI will be required to provide periodic attestation to OIT stating they are continuing to meet the regulations and guidelines stated within the NIST AI RMF v1.0.

Sources:

- NIST AI RMF v1.0
- U.S. AI Safety Institute Workshop data (NIST action)
- U.S. Government Accountability Office (U.S. GAO) AI Accountability Framework
- U.S. Department of State (CT:DATA-2; 04-24-2023) (Office of Origin: M/SS/CFA)
- U.S. White House, Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

AI-1 POLICY AND PURPOSE

Responsible AI implementation and use requires a deliberate and detailed approach. NIST AI Risk Management Framework (AI RMF) is designed to effectively manage Generative AI technology and capitalize on its presumptive business value to the State of Alabama. The four core functions of the AI RMF 1.0 are as follows:

AI-1.1 GOVERN

The Govern function aligns the technical aspects of AI Risk Management to policies and operations to drive a purpose-driven culture focused on risk understanding and management to anticipate, identify, and manage AI systems risk.

The State shall:

a. Establish an AI Governance Board or equivalent for oversight and strategic direction. This board shall consist of OIT leadership and staff along with agency Chief Information Officers (CIOs) as determined by the Secretary of OIT.
b. Define risk tolerance levels for different types of AI systems.
c. Develop AI-specific security standards and procedures.

AI-1.2 MAP

The Map function establishes the context to frame risks related to an AI system. The AI lifecycle consists of many interdependent activities involving a diverse set of AI factors which often do not have relevant context of the larger picture and can create complex uncertainty in associated risk management practices.

Information gathered during the Map function enables negative risk prevention and can triage initial decisions about appropriateness or need for an AI solution. Results of this function are the basis for the Measure and Manage functions and are intended to enhance the State’s ability to identify risks and broader contributing factors.

The State shall:

a. Inventory all AI systems currently used or under development by Executive Branch Agencies.
b. Classify AI systems based on their potential impact and risk level.
c. Identify relevant laws, regulations, and ethical frameworks.

AI-1.3 MEASURE

The Measure function employs quantitative, qualitative, or mixed-method tools, techniques, and methodologies to analyze, assess, benchmark, and monitor AI risk and related impacts. It uses knowledge relevant to AI risks identified in the Map function and informs the Manage function. AI systems should be tested before their deployment and re-tested regularly while in operation. AI risk measurements include documenting aspects of systems' functionality and trustworthiness.

The State shall:

a. Conduct regular risk assessments to evaluate vulnerabilities and threats.
b. Monitor AI systems for anomalous behavior and potential security incidents.
c. Implement metrics to track compliance with security controls and ethical principles.

AI-1.4 MANAGE

The Manage function entails allocating risk resources to mapped and measured risks on a regular basis and as defined by the State, as well as the Govern function. Risk treatment comprises plans to respond to, recover from, and communicate about incidents or events.

The State shall:

a. Implement appropriate security controls for each AI system based on its risk level.
b. Train personnel on AI security best practices and ethical considerations.
c. Develop incident response plans for addressing security vulnerabilities and breaches.

Specific Security Controls

a. Data Security: Implement data encryption, access control, and data loss prevention measures for training data, models, and outputs.
b. System Security: Secure AI systems and infrastructure against unauthorized access, malware, and cyberattacks. Secure State information systems and data against unauthorized access and use by AI or AI systems.
c. Algorithmic Bias: Identify and mitigate potential biases in AI algorithms, especially when dealing with sensitive data.
d. Explainability and Transparency: Ensure AI decisions are explainable and interpretable to stakeholders.
e. Human Oversight: Establish clear decision-making processes where human intervention is required for critical tasks.

Training and Awareness

a. Provide mandatory training for all personnel involved in AI development, deployment, and use.
b. Foster a culture of awareness about AI security risks and ethical considerations.

Compliance and Enforcement

a. Establish mechanisms for monitoring compliance with this policy across OIT and Executive Branch Agencies.
b. Define consequences for non-compliance, including disciplinary actions and potential corrective measures.

Review and Revision

i. Review this policy regularly to ensure its effectiveness and alignment with evolving AI technologies and best practices.
j. Encourage stakeholder feedback and input for continuous improvement.

POLICY OWNER

Secretary of Office of Information Technology (OIT)

MATERIAL SUPERSEDED

This is the first State of Alabama Artificial Intelligence Governance Policy. All State agencies and vendors of the State are required to comply with the current implemented version of this policy.

REVISION HISTORY

Revision Date	Summary of Change
12/31/2024	Policy Creation

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK

APPROVED BY

Signature	Daniel Urquhart
Approved by	Daniel Urquhart
Title	Secretary of Office of Information Technology (OIT)
Date Approved	01/15/2025

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK