Enterprise Artificial Intelligence Policy

Document Ref #
200-POL-007

Document Control		
	Version #	1.0
	Signed	Kristin H. Darby
	Approval Date	9/26/2025
	Last Reviewed by Policy Review Committee	9/09/2025

A. EXECUTIVE SUMMARY

The main purpose of this document is to define the Enterprise Artificial Intelligence Policy of the State of Tennessee along with the organization and framework required to communicate, implement, and support this policy. Information and data, like any other asset owned by the State of Tennessee, has significant value to the stakeholders of the State. This policy establishes and upholds the minimum requirements necessary to protect the State's information and data, as well as the work performed by every department and agency by enabling and ensuring the valid, reliable, transparent, and ethical use of Artificial Intelligence. Throughout the remainder of this document Artificial Intelligence will be referred to as AI. Accompanying AI governance protocols will assist to communicate and ensure the accountable, safe, and secure use of AI technologies, as set forth by the National Institute of Standards and Technology (NIST) Artificial Intelligence Risk Management Framework (AI RMF 1.0). This policy aligns with the Governor's Executive Order No. 2, requiring each employee to avoid actions which might result in or create the appearance of making a government decision outside of official channels, or affecting adversely the confidence of the public in the integrity of the government.

B. INTRODUCTION

The State of Tennessee recognizes that as AI technologies continue to evolve, it is imperative for the State to establish an enterprise policy for safe and effective usage. This enterprise policy is designed to promote the acceptable use of AI solutions by minimizing the potential for intentional or unintentional misuse, information security breaches, and unethical use of AI in State Government operations. Harnessing the benefits of AI requires alignment with the Enterprise Information Security Policy for the State of Tennessee and the NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0).

This policy applies to the use of all available and those yet to be developed AI solutions by an employee of the State of Tennessee, including, but not limited to:

- those that are open source;
- those developed by a State Department;
- those developed by a third party;
- other similar applications that mimic human behavior to generate responses, work product, or perform operational tasks.

This policy is designed to promote the acceptable and responsible use of AI solutions, while creating a framework that minimizes the potential for intentional or unintentional information security breaches, misuse of sensitive information and data, unethical decision-making, and outcomes, and potential biases. With the ever-evolving AI landscape, this enterprise policy will be updated regularly to reflect changes in the existing environment.

C. SCOPE

This enterprise policy has been created to establish a minimum requirement essential to protect the State against unauthorized or unintentional access, modification, destruction, or disclosure set forth by the Information Systems Council (ISC) of the State of Tennessee. This policy is intended for all State of Tennessee employees and contractors doing business on behalf of the State of Tennessee. This enterprise policy is intended to bring awareness to and reduce the risks of using AI solutions, recognizing the potential business benefits of and capabilities for select use cases when used appropriately, transparently, legally, and ethically.

As Strategic Technology Solutions (STS) is the consolidated Information Technology Division of Tennessee State Government, this policy is also intended to be applied to all consolidated and non-consolidated departments and agencies of Tennessee State Government as a framework for developing individualized specific policies. By establishing an appropriate enterprise policy, associated governance protocols, and utilizing a documented development process that includes all stakeholders, the State envisions maximum compliance with these minimum requirements.

All full and part-time employees of the State of Tennessee, all third parties, outsourced employees, or vendors who work on State premises or remotely connect their computing platforms to the State of Tennessee's computing platforms, and any cloud provider storing, processing, or transmitting State information and data should adhere to the requirements set forth in this document, including:

All AI solutions, regardless of type, must be reviewed and approved to verify purposeful use and ensure compliance with this Enterprise AI Policy and all associated governance protocols. No accounts shall be created within AI solutions using State credentials not officially approved by the STS AI Review Committee or listed on the State's Standard Products List.

As AI solutions evolve, responses to queries may be inaccurate, incomplete, misleading, biased, fabricated, or may even contain hallucinations. AI created information may contain material subject to a third party's intellectual property ownership and all departments and agencies should verify any response generated from an AI solution, and confirm whether it is accurate, appropriate, not biased, not a violation of any other individual or entity's intellectual property or privacy, and consistent with State policies.

D. AUTHORITY

This Enterprise AI Policy and any associated governance framework or operating procedures, have been authorized by the Information Systems Council, the Commissioner of the Department of Finance and Administration, and Chief Information Officer of STS:

The Information Systems Council (Tenn. Code Ann. §§ 4-3-5501-5525)

The Commissioner of the Department of Finance and Administration (Tenn. Code Ann. § 4-3-1003).

E. EXCEPTIONS

All proposed AI solutions must be reviewed, evaluated and processed by the State of Tennessee AI Review Committee having gone through the State's Standard Products List exception process. Only AI solutions should be installed or used on State devices that have been approved through this process.

F. REVIEW

Review of this document takes place within the STS Policy Review Committee sessions and will occur on a quarterly basis or as determined by the State's AI Advisory Council, the STS AI Workgroup, and any related groups within State Government.

This policy and any associated governance supporting documentation are published on the STS intranet site and published annually located at:
Policies and Procedures (teamtn.gov)

G. ARTFICIAL INTELLIGENCE (AI) USE CASES

The rise of AI may unlock new productivity levels and other benefits for State Government. This policy recognizes that as AI usage evolves, it is expected that use cases will be expanded to encompass additional business processes and programs that exist within State Government.

H. INFORMATION SECURITY

As AI offers advanced capabilities to inform critical missions, it is imperative to protect and secure the privacy, civil rights, and civil liberties of citizens. As AI evolves, the State will continue to transform its existing capacity to improve and enrich the public's experience, while keeping pace with security protocols that guarantee effective oversight of AI. All departments and agencies of the State are required to seek to minimize all negative impacts of AI systems, by effectively monitoring all design, development, and deployment and by ensuring all procurements and partnerships are effectively evaluated to assess potential impact, via the STS AI Review Committee, in alignment with security protocols.

State departments and agencies are allowed to manage State information or data consumed by vendor's Natural Language Processing (NLP), Large Language Model (LLM) or Large Action Model (LAM) that is on the Standards Products List, having been approved by the STS AI Review Committee or has gone through the State's Standard Product List Exception Process. As AI technologies advance the State's Standard Product List Exception Process is subject to change.

I. MANAGEMENT OF INFORMATION SECURITY

Objective: To provide management direction and support for the effective use of AI, in accordance with all department and agency business requirements and relevant State and federal statutes and regulations.

1. Information Security Governance

The STS AI Workgroup, under advisement of the STS Chief Information Officer (or an approved delegate), will initiate, control, and communicate an enterprise information security architecture that includes, but is not limited to, this Enterprise AI Policy and associated governance protocols. It is expected that each of the parameters below will be maintained to align with State Security protocols:

- Transparency on the use of AI tools, depending on the type of use case.
- Verification of the correctness of the generated output with attention to correctly attributing the source.

- Maintain respect for personal information and data, as well as confidential information by not entering any on platforms that are not managed on State-controlled servers.
- Remain responsible for the correct use of AI and the published output.
- Ensure that state data is not used to train non state generative AI models.

2. Alignment with AI

Departments and agencies are required to develop a plan to communicate the requirements of this policy and any associated governance framework and protocols, ensuring that all State employees and vendors as defined in the Scope should adhere to all applicable AI policies and governance. AI should be used with safety, security, and privacy in mind, minimizing potential harm and ensuring that systems are reliable, resilient, and controlled by humans.

To ensure that the use of tools and solutions with embedded AI functionality align with the objectives of departments and agencies across State Government, it is imperative that users remain aware that information generated by AI may be inaccurate, incomplete, misleading, biased, or hallucinated. **Departments and agencies are required to train all users on the responsible use of AI technologies including AI features in any approved AI solution.**

J. OPERATION SECURITY AND PRIVACY

1. Operational Procedures and Responsibilities

Objective: To document the protection of critical State information assets, including hardware, software, and data from unauthorized use, misuse, or destruction to ensure correct and proper operations. Employees should be mindful to safeguard the use of State data, limiting unintended exposure to:

- confidential or privileged information or communications;
- personally identifiable information (PII);
- protected health information (PHI);
- justice and public safety information;
- any information that has the potential to erode public trust;
- any Federal information and data.

To ensure this policy recognizes the diversity of business processes and programs that exist within State Government the table below was developed. As AI usage evolves, it is expected that the Data Classification Designation terms will be expanded.

Data Classification Designation	
Category	Description
Public Record	Data which the department and agency may release to the public without concern for confidentiality or privilege. Please consult agency legal counsel regarding public records.
Confidential Record	Data which department and agencies must protect from unauthorized access, disclosure, or public release based on State or Federal regulatory requirements. Please consult agency legal counsel for confidentiality distinction.
Restricted Access Record	Data to which department and agency must apply elevated or prescribed protections from unauthorized access, disclosure, or public release based on State or Federal regulatory requirements. Please consult agency legal counsel regarding restricted access records.

2. **Role-Based Access**

   Systems should be built and managed in line with EISP including (but not limited to):

   - least privileges;
   - need to know;
   - separation of duties.

3. **Documented Operating Procedures**

   All departments and agencies of the State of Tennessee and vendors acting on behalf of the State should identify, document, and maintain standard security operating procedures and configurations for their respective operating environments and ensuring efforts using AI technologies are responsible, safe, secure, and ethical.

K. BUSINESS CONTINUITY MANAGEMENT

Objective: To ensure the availability of critical systems and infrastructure and the continued ability to provide services in the event of a crisis or disaster.

As public stewards, all State departments and agencies should use AI responsibly ensuring human input and oversight in the performance, impact, and consequences of its use in

department and agency work. As AI usage evolves, it is expected that perspectives on business continuity will be expanded.

Business Continuity and Disaster Recovery requirements need to be evaluated and in line with current STS/Security Team's internal processes including "Business Impact Analysis."

L. RISKS OF AI USAGE

While AI solutions represent significant opportunities for innovation and the potential to help solve a wide variety of business and technical challenges, the use of these solutions without human oversight introduces several risks. All departments and agencies are discouraged from entering, managing, or consuming State information and data within AI solutions. All departments and agencies are further encouraged to verify any responses generated from applications with embedded NLP, LLM, or LAM solutions. To manage risk of AI usage all department and agency inputs and outputs must be reviewed by a human to verify accuracy. Such risks may include, but are not limited to, the following:

Accuracy

AI models are designed to generalize responses based on the data on which they are trained. Therefore, if those data sets are erroneous or incomplete, the models may not always produce accurate responses for specific queries.

Bias

AI systems can inherit biases that are present in the data they are trained on. If the training information and data contains biased or discriminatory information, AI algorithms can perpetuate and amplify these biases, leading to potential Algorithmic Discrimination.

Legal liability & intellectual property

AI solutions may use information that is protected under intellectual property or other ownership rights, such as copyright. Such usage may lead to plagiarism, intellectual property law infringement, and violation of licensing requirements, and can result in legal ramifications such as lawsuits, fines, and even criminal penalties.

Ethical, potential for toxic or harmful outputs

AI solutions can generate photorealistic images, videos, and audio. Such AI generated content may be difficult, or sometimes impossible, to distinguish from authentic content, which poses ethical implications. These generations may spread misinformation, manipulate public opinion, or defame individuals.

Data Exposure/Leakage

AI is often built upon storing and processing user prompts for the AI to respond to. These prompts are stored for later learning and as a result could be breached and exposed depending upon the security around the AI model and infrastructure.

Departments and agencies should not use AI solutions as primary decision-makers when performing State operations impacting citizens or employees, instead human input and oversight must be maintained.

M. COMPLIANCE

Compliance with Legal and Contractual Requirements

Objective: To avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security and of any security requirements. It is recommended that all State departments and agencies develop clear strategies for using AI to ensure continued compliance with all legal and contractual requirements.

N. INFORMATION SECURITY REVIEWS

Objective: This policy confirms that information security is implemented and operated in accordance with organizational policies and procedures. With the ever-evolving AI landscape, this policy and any associated governance protocols will be updated regularly to reflect changes in the existing environment.

All new AI solutions should be reviewed to ensure that cybersecurity provisions are implemented throughout the entire IT Solution Development Life Cycle.

O. GOVERNANCE FRAMEWORK PROTOCOLS

Upon approval of this policy, the State's AI Advisory Council, the STS AI Workgroup, and any related groups within State Government will coordinate and socialize governance protocols and an approved implementation strategy with all State of Tennessee Departments and agencies.

Automation and Supporting Solutions

The State's Intranet platform will be used for publishing policies, processes, standards, and procedures.

P. POLICY CHANGE CONTROL

REFERENCES

F&A STS Standard Product List Standard Products List (SPL)

F&A STS Standard Product Exception Request Process SPL Exception Request

Governor Lee's Executive Order No. 2 exec-orders-lee2.pdf (tnsosfiles.com)

Governor Lee's Executive Order No. 3 exec-orders-lee3.pdf (tnsosfiles.com)

National Institute of Standards and Technology (NIST) – Artificial Intelligence Risk Management Framework (AI RMF 1.0)

STS Intranet Site – Published Policies and Procedures

F&A Enterprise Information Security Policy

Tenn. Code Ann. § 4-3-1003—Authority of the Commissioner of the Department of Finance and Administration
Tenn. Code Ann. §§ 4-3-5501-5525—Establishment and responsibilities of the Information Systems Council

GLOSSARY

See STS Glossary