# Enterprise Generative AI Policy

**Document Ref #**

**XXX-POL-XXX**

## EXECUTIVE SUMMARY

The main purpose of this document is to define the Enterprise Generative Artificial Intelligence (Gen AI) policy of the State of Tennessee along with the organization and framework required to communicate, implement, and support this policy. Information, 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 the work performed by every department and agency by enabling and ensuring the valid, reliable, transparent, and ethical use of Gen AI. Throughout the remainder of this document Generative AI will be referred to as Gen AI. This policy further provides a governance framework required to communicate and ensure the accountable, safe, and secure use of Gen 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 specifically making a government decision outside of official channels, affecting adversely the confidence of the public in the integrity of the government.

## INTRODUCTION

The State of Tennessee recognizes that as Gen 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 Gen AI solutions, by minimizing the potential for intentional or unintentional misuse, information security breaches and unethical use AI in State Government operations, in addition to creating a governance framework. Harnessing the benefits of Gen 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 Gen AI solutions by an employee of the State of Tennessee, including, but not limited to:

- those that are open source
- developed by a State Department
- 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 Gen AI solutions, while creating a framework that minimizes the potential for intentional or unintentional information security breaches, misuse of sensitive data, unethical decision-making and outcomes, and potential unethical biases. With the ever-evolving AI landscape, this enterprise policy will be updated regularly to reflect changes in the existing environment.

## SCOPE

This enterprise policy has been created to establish and uphold the minimum requirements that are necessary to protect the State against unavailability, unauthorized or unintentional access, modification, destruction, or disclosure as 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 Gen 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 framework and utilizing a documented development processes 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 data should adhere to the requirements set forth in this document, including:

All Gen AI solutions, regardless of type, must be reviewed and approved to verify purposeful use and ensure compliance with this Enterprise Generative AI policy and other associated governance framework. ISC Policy 3.00: Generative Artificial Intelligence. No accounts will be

created within AI solutions using State credentials not officially approved through the State authorized vendor procurement process.
As Gen AI solutions evolve, responses to queries may result in inaccurate, incomplete, misleading, biased, fabricated, or may even contain hallucinations. Gen 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 a Gen 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.

## AUTHORITY

This Enterprise Generative AI policy and associated governance framework have been authorized by the Commissioner of the Department of Finance and Administration and State Chief Information Officer (STS), as a component of Information Security Council (ISC) policies.

## EXCEPTIONS

Only Gen AI solutions that have been licensed and approved by the State's Standard Exception process, in alignment with security protocols should be installed on devices covered by the software's license agreement.

## 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 States 's AI Advisory Council, the STS Gen AI Workgroup, and any successive groups within State Government.

The States 's AI Advisory Council, the STS Gen AI Workgroup, and any successive groups within State Government are established to provide expertise in the development of this policy and associated governance protocols that include, technology emblements, security, data governance, data privacy, legal, ethical, and other expertise relevant to the successful oversight of Gen AI.
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)

## Definitions

As this policy requires the responsible, ethical, and safe use of AI technologies by all stakeholders, it was deemed essential to define key terms related to AI:

**Artificial Intelligence (AI)** - any system that performs tasks under varying and unpredictable circumstances without significant human oversight or can learn from experience and improve such performance when exposed to data sets, AI is also made up of a set of techniques, including, but not limited to, machine learning, that is designed to approximate cognitive tasks.

**Generative AI (Gen AI)** - any system that learns patterns and relationships from massive amounts of data, which enables them to generate new content that may be similar, but not identical, to the underlying training data. The systems generally require a user to submit prompts that guide the generation of new content. (Adapted slightly from U.S. Government Accountability Office Science and Tech Spotlight: Generative AI)

**Large Action Model (LAM)** - An artificial intelligence model that can understand and execute complex tasks by translating human intentions into action. While LLMs are adept at generating text based on input prompts, LAMs focus on understanding actions and orchestrating sequences of actions to accomplish specific goals.

**Large Language Model (LLM)** – A type of AI program that can recognize and generate text, among other tasks. LLMs are trained on huge sets of data — hence the name "large." LLMs are built on machine learning: specifically, a type of neural network called a transformer model.

**Reinforcement Learning from Human Feedback (RLHF)** - A type of algorithm, used to fine-tune human preferences.

**AI Hallucinations** - a phenomenon where an AI system perceives patterns or objects that are nonexistent or imperceptible to human observers, creating outputs that are nonsensical or altogether inaccurate.

**Algorithmic Discrimination** – The use of automated systems to inflict unjustified different treatment or impact disfavoring people based on their race, gender, age, religion, disability, or sexual orientation.

As AI usage evolves, it is expected that definitions of key terms will be expanded.

## Gen AI Use Cases

The rise of Gen AI may unlock new productivity levels and other benefits for State Government. This policy recognizes the diversity of business process and programs that exist within State Government by providing parameters that align with all department and agency goals and priorities.

**Repetitive Tasks**

Gen AI can be particularly useful for automating repetitive and mundane tasks, that can consume significant amounts of time and effort. Effective and responsible use of Gen AI systems can streamline these tasks, allowing resource allocation towards more strategic and value-added activities.

**Data Analysis and Insights**

Gen AI-powered analytics tools can help our employees analyze large volumes of data, identify patterns, trends, and insights, and make data-driven decisions. Allow employees access to Gen AI systems for data analysis tasks to enhance their decision-making capabilities and improve operational efficiency.

**Customer Service and Support**

Gen AI-driven chatbots (which we are currently working with) and virtual assistants can assist employees in providing customer service and support by answering common inquiries, resolving issues, and providing relevant information to customers. Allow employees to leverage Gen AI-powered customer service systems to enhance the customer experience and increase efficiency.

**Content Creation and Curation**

Gen AI-powered systems can assist employees in content creation and curation tasks, such as generating written content, editing videos, or curating relevant articles and resources. Allow employees to use Gen AI systems to streamline content creation, processes, and improve content quality.

**Risk Management and Compliance**

Gen AI algorithms can analyze data to identify potential risks, fraud patterns, or compliance issues within the organization. Allow employees to use Gen AI-driven risk management and compliance tools to detect anomalies, mitigate risks, and ensure regulatory compliance.

**Training and Development**

Gen AI-powered learning platforms can provide personalized training and development opportunities for employees based on their skills and which department and agency they are working for, knowledge gaps, and learning preferences. Allow employees to

access Gen AI-driven learning systems to enhance their skills, knowledge, and professional development.

Allowing State employees to use Gen AI in high-impact applications depends on several factors, including the department and agency readiness, the complexity of the application, awareness of potential risks involved and alignment with Information Security protocols.

As Gen AI usage evolves, it is expected that use cases will be expanded to encompass any additional business process or programs that exist within State Government.

## INFORMATION SECURITY

As Gen 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 Gen 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 Gen AI. All departments and agencies of the State are required to perform IT Operations, in a manner that would not compromise the security or integrity of any network systems. All State departments and agencies must routinely assess technical capabilities, data and integration capabilities, scalability, user interface, and security considerations.

State departments and agencies shall seek to minimize anticipated and emergent negative impacts of AI systems, by ensuring all procurement and partnerships are effectively evaluated to assess potential impact, by the F&A STS Standard Exception Process, in alignment with security protocols.

State departments and agencies should not use tools or allow State data to be consumed by a vendor Large Language Model (LLM) or Large Action Model (LAM) that is not on the Standards Products List or has not been approved through the F&A STS Standard Exception Process.

Gen AI should be used with respect for user privacy, ensuring data protection, and complying with relevant privacy regulations and standards. Privacy values such as anonymity, confidentiality, and control generally should guide choices for Gen AI system design, development, and deployment. Privacy-enhancing Gen AI should safeguard human autonomy and identity where appropriate.

## MANAGEMENT OF INFORMATION SECURITY

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

### Information Security Governance

The STS Gen AI Workgroup, under advisement of the STS Chief Technology Officer, will initiate, control, and communicate an enterprise information security architecture that includes, but is not limited to, this Enterprise Generative AI policy and governance framework and associated organizational communication a security technology framework. It is expected that each of the below parameters 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 data and confidential information by not entering these on platforms that are not managed on State-controlled servers.
- Remain responsible to the responsibility for the correct use of Gen AI and the published output.

### Alignment with Generative AI

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

To ensure that the use of tools and solutions with embedded Gen 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.

# OPERATION SECURITY

## 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.

- Confidential or privileged information or communications.
- Personal Identifiable Information (PII).
- Protected health information (PHI).
- Justice and public safety information.
- Any information that has the potential to erode public trust.

To ensure this policy recognizes the diversity of business processes and programs that exist within State Government the below table was developed. As Gen AI usage evolves, it is expected that the below 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. Examples of Confidential Records may include but are not limited to:<br>• Emergency response plans<br>• Enterprise and Departmental policies<br>• Press releases and marketing materials<br>• Vendor Requests for Information (RFI), Purchase (RPF) or Qualification (RFQ)<br>• Regulatory and legal filings |
| Confidential Record | Data which department and agencies must protect from unauthorized access, disclosure or public release based on State or Federal regulatory requirements. Examples of Confidential Records may include but are not limited to:<br>• Departmental policies, procedures, and training materials<br>• Employee web/intranet portals<br>• Pre-release department, agency, or program articles |

| | |
|---|---|
| | • Drafts of research vendor Requests for Information (RFI), Purchase (RPF) or Qualification (RFQ)<br>• System and Network Security related documents<br>• Privileged, Legal, Audit and Human Resources documents.<br>• Personally Identifiable Information regarding:<br>• Benefit applicants or members<br>• Workforce members<br>• Vendors or Providers<br>• Financial information<br>• Protected Health Information<br>• Social Security Administration Information |
| Restricted Access Record | Data to which department agency must apply elevated or prescribed protections from unauthorized access, disclosure or public release based on State or Federal regulatory requirements. Examples of Restricted Access Records may include but are not limited to:<br>• Federal Tax Information (FTI)<br>• Government issued identifiers (e.g., Social Security Number, Passport number, State identification or driver's license)<br>• Prosecutable Tennessee Bureau of Investigation (TBI)/Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS)<br>• Payment Card Industry (PCI)<br>• Center for Medicare & Medicaid Services (CMS) – Social Security Administration (SSA) |

## 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 Gen AI technologies are responsible, safe, secure, and ethical.

All departments and agencies of the State are encouraged to establish and communicate a robust strategy to implement this policy and associated governance framework, essential to maintaining public trust in the performance of operations. It is further recommended that State departments and agencies routinely assess technical capabilities, data integrity and integration capabilities, scalability, user interface, and security considerations.

## 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 Gen AI responsibly ensuring accountability for the performance, impact, and consequences of its use in department and agency work. Similarly, Gen AI usage can be explained, meaning "how" the decision was made using logical interpretability for "why" a decision was made, and its meaning or context to business continuity and operations. As Gen AI usage evolves, it is expected that perspectives on business continuity will be expanded.

## RISKS OF AI USAGE

While Gen 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 data within Gen AI solutions. All departments and agencies are further encouraged to verify any responses generated from applications with embedded Large Language Model (LLM) or Large Action Model (LAM) solutions. To manage risk of Gen AI usage all department and agency inputs and outputs are encouraged to be reviewed by a human to verify accuracy. Such risks may include, but are not limited to, the following:

**Accuracy**

Generative 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**

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

**Legal liability & intellectual property**

Gen 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**

Gen 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.

To mitigate the above risks, departments and agencies are discouraged from using Gen AI solutions as primary decision-makers when performing State operations impacting citizens, or employees.

## 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.

## INFORMATION SECURITY REVIEWS

Compliance with Legal and Contractual Requirements
**Objective:** To ensure that information security is implemented and operated in accordance the 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.

## PREREQUISITES, AUTHORITY, AND STANDARDS

**Prerequisite** is the set of Information Resources Policies adopted by the ISC.
**Authority** to develop policies, processes, standards, and procedures is derived from two sources:

1. The Information Systems Council (TCA 4-3-5501-5525)
2. The Commissioner of the Department of Finance and Administration (TCA 4-1003)

## GOVERNANCE PROTOCOLS

Upon approval of this policy, the States ’s Gen AI Advisory Council, the STS Gen AI Workgroup, and any successive groups within State Government will coordinate and socialize governance protocols and an approved implementation strategy with all State of Tennessee Departments and agencies after publication of this enterprise policy.

**When to Use this Enterprise Policy**

While Gen AI presents an incredible opportunity to increase efficiency and efficacy in the work of State Government, there are many irresponsible applications that can negatively impact the business and welfare of the State.

To safeguard the business and citizens of the State, departments and agencies must proactively prioritize security, bringing awareness to the risks posed by Gen AI, and establish clear governance and policies for responsible Gen AI use. As public stewards, all State departments and agencies should encourage the responsible use of Gen AI by:

1. Intentionally promoting the use of Gen AI by verifying output, maintaining privacy, addressing biases, and protecting intellectual property rights.
2. Ensuring compliance with ethical and legal requirements of each department and agency.
3. Ensure the appropriate level of cybersecurity of these systems, especially those connected to the internet.
4. Analyzing the limitations of technology tools and provide feedback and recommendations, as needed.
5. Using this policy as a basis for discussion, and a benchmark for further action that includes all employees and vendors as defined in the Scope.
6. Applying and adhering to this enterprise policy whenever possible and if needed, develop complimentary recommendations and/or requirements that align with department and agency operational standards.
7. Referring to this document quarterly, as guidance will change as technology, laws and industry best practices evolve.

**Automation and Supporting Solutions**

The following solutions will be used in the development and revision of policies, processes, standards, and procedures:

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

## POLICY CHANGE CONTROL

This policy adheres to the Policy Change Control as defined in 100-POL-001 Policies, Processes, Standards & Procedures Life Cycle.

## REFERENCES

F&A STS Standard Product List Exception Request – Service Portal (service-now.com)

F&A STS Standard Product List

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

Governor'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

TCA 4-3-1003—Authority of the Commissioner of the Department of Finance and Administration
TCA 4-3-5501-5525—Establishment and responsibilities of the Information Systems Council

## GLOSSARY

*Terms not already defined in STS Centralized Glossary.

**Artificial Intelligence (AI)** - any system that performs tasks under varying and unpredictable circumstances without significant human oversight or can learn from experience and improve such performance when exposed to data sets. AI is also made up of a set of techniques, including, but not limited to, machine learning, that is designed to approximate cognitive tasks.

**Generative AI (Gen AI)** - any system that learns patterns and relationships from massive amounts of data, which enables them to generate new content that may be similar, but not identical, to the underlying training data. The systems generally require a user to submit prompts that guide the generation of new content. (Adapted slightly from U.S. Government Accountability Office Science and Tech Spotlight: Generative AI)

**Large Action Model (LAM)** - An artificial intelligence model that can understand and execute complex tasks by translating human intentions into action. While LLMs are adept at generating text based on input prompts, LAMs focus on understanding actions and orchestrating sequences of actions to accomplish specific goals.

**Large Language Model (LLM)** – A type of AI program that can recognize and generate text, among other tasks. LLMs are trained on huge sets of data — hence the name "large." LLMs are built on machine learning: specifically, a type of neural network called a transformer model.

**Reinforcement Learning from Human Feedback (RLHF)** - A type of algorithm, used to fine-tune human preferences.

**AI Hallucinations** - a phenomenon where an AI system perceives patterns or objects that are nonexistent or imperceptible to human observers, creating outputs that are nonsensical or altogether inaccurate.

**Algorithmic Discrimination** – The use of automated systems to inflict unjustified different treatment or impact disfavoring people based on their race, gender, age, religion, disability, or sexual orientation.