Effective Date: 9/23/2026

I. POLICY
As per RS 39:15.3, the Office of Technology Services (OTS) shall establish and coordinate all information technology systems and services affecting the management and operations of the executive branch agencies of state government.

II. PURPOSE
The State of Louisiana recognizes the growing significance of Artificial Intelligence (AI) in enhancing government operations and services. The purpose of this policy is to establish guidelines for the responsible, ethical, and effective use of AI technologies within the State of Louisiana. This policy aims to ensure responsible use, protect privacy and security, maintain public trust, support innovation and efficiency, prevent bias and discrimination, and ensure compliance with applicable laws and regulations.

III. SCOPE
This policy applies to all state government agencies and entities under the authority of the Office of Technology Services (OTS), in accordance with Act 712 of the 2014 Regular Legislative Session. It governs the use of AI technologies in any form, including but not limited to machine learning algorithms, automated decision-making systems, generative AI and large language models, and cognitive computing applications.

This policy should not be interpreted as superseding existing state law or Office of Technology Services policy. Rather, any use of AI should operate within existing technology processes and procedures, in addition to the requirements outlined in this policy. Agencies should consult their assigned Agency Relationship Manager when there is a perceived conflict between this policy and existing state law or other OTS policy.

IV. APPLICABITLIY
This policy applies to all consolidated state agencies and individual users of state-governed information technology resources, assets, and systems. This policy does not govern the personal use of AI on personal devices for non-business use.

This policy does not apply to AI features premised on machine learning without a generative component, such as fraud and spam filters or autocorrect software for spelling.

V. DEFINITIONS
- **Artificial Intelligence (AI)** - computer systems capable of performing tasks that typically require human intelligence, including but not limited to machine learning, natural language processing, and computer vision.

- **Generative AI** - tools or systems used to create models that can generate new and original content, such as images, music, or text, based on patterns and examples from existing data.
- **Deep learning** – model, tool or system used to recognize complex patterns in pictures, text, sounds, and other data to produce insights and predictions.
- **Machine Learning** - computer systems or tools that are able to learn and adapt without following explicit instructions, by using algorithms and statistical models to analyze and draw inferences from patterns in data.
- **Ethical AI** - AI systems that are designed, developed, and deployed in a manner that is consistent with ethical principles, including fairness, transparency, accountability, and privacy.
- **Responsible AI** - AI systems that are used in a manner that considers the potential social, economic, and ethical implications, and takes steps to mitigate risks and maximize benefits.
- **Using Agency** - An Agency using or procuring AI systems or services.
- **Hallucination** - A response generated by AI that contains false or misleading information which is presented as fact.
- **AI Incident** - Any event in which an AI system is manipulated, or fails in a way that compromises safety, security, fairness, compliance, or organizational objectives. This encompasses adversarial manipulation such as prompt injection, data poisoning, or jailbreak attacks; the generation of harmful or unsafe outputs; model or data drift that degrades performance or reliability; security or vendor breaches, compromise, or misuse of data; and any action that conflicts with regulatory or organizational standards.

VI. GUIDELINES

Using Agencies are responsible for educating and ensuring all users comply with this policy and any applicable data sharing agreements.

- Users may employ AI systems to enhance the efficiency and effectiveness of public services.
- Users are prohibited from the following, without prior authorization:
    - Entering confidential, proprietary, and restricted state data (e.g., passwords, credit card numbers, health records) into commercially available AI systems.
    - Using AI to independently make business decisions including, but not limited to, the following categories:
        - Enrollment
        - Employment
        - Program Eligibility
        - Finances
        - Legal and Regulatory Compliance
        - Law Enforcement
        - Welfare
    - Using AI to bypass security controls (e.g., jailbreaking) or to create, modify, distribute, or execute malicious code.
    - Using AI to create or generate:
        - Illicit content.
        - Content that is unlawful material, or information that lacks broad factual verification or consensus.

        - Spoofs or fraud, including deepfake, impersonation, misinformation, phishing, or social engineering to harm individuals.
- Users must review and verify AI input and output for relevance before use to ensure it aligns with its intended purpose and to mitigate risks such as hallucinations, misinformation and bias.
- Any content produced in whole or in part by an AI system should be clearly labeled as AI-generated to ensure transparency and accountability.
- AI output used for decision making must be supplemented with human verification to ensure accuracy and factuality. An identified human owner is required to review and approve any AI-assisted output prior to use, and accountability for the decision rests with that designated role.
- State-approved systems, accounts, and equipment are the only authorized means for using AI when conducting state business.
- Users must not infringe on any copyright or intellectual property laws.
- Users must use the "opt-out" option on data collection and model training features that AI systems offer, if available.
- All AI-generated outputs created on behalf of the State of Louisiana are the property of the State. Users waive any rights of ownership or authorship in such outputs.
- Users must not use state email or other state identifying information to register unsupported or unapproved tools.
- Users must report the unauthorized use or disclosure of confidential, proprietary, and restricted state data in AI systems to the OTS Information Security Team, by calling 844-692-8019 or by emailing infosecteam@la.gov.

VII. PRIVACY AND SECURITY

Agencies leveraging AI, including the use of third party products which include AI functionality or third party vendors providing services for the state, must protect the privacy and security of data in accordance with the OTS Information Security Policy and any applicable state and federal laws and policies. Additionally, Agencies must implement measures to prevent unauthorized access, use, or sharing of confidential, proprietary, and restricted state data used by those AI systems.

VIII. DATA GOVERNANCE

All state agencies are responsible for ensuring that the use of AI technologies including, but not limited to meeting notetaker tools, complies with applicable agency data governance policies and practices. Agencies must adhere to established data classification standards, record retention schedules, and Louisiana public records laws when utilizing AI generated content or recordings. Any data collected, generated, or processed through AI tools must be managed and preserved in accordance with agency requirements and state statutes. Agencies should evaluate both AI inputs and outputs for proper classification and retention before inclusion, dissemination, or deletion.

Data Quality

All datasets intended for use in AI systems must undergo a documented review prior to deployment. This review shall assess accuracy, completeness, integrity, timeliness, and relevance. Where errors, omissions, duplications, biases, or other deficiencies are identified, appropriate cleansing and remediation measures must be performed before the dataset is approved for use in any AI system.

IX. Responsibilities
Agencies shall submit all software, applications, tools, and services utilizing AI for business operations to OTS for review prior to procurement and implementation. Agencies should consult their assigned Agency Relationship Manager for information on the submittal process. Agencies are strictly required to ensure their use of AI is in accordance with OTS policies, standards and procedures and all applicable state and federal laws and regulations.

X. EXCEPTIONS
In limited circumstances, exceptions to this policy may be granted. An exception is defined as a deviation from one or more specific requirements of this policy due to operational necessity, technical limitations, or compelling business needs.

Agencies seeking an exception to this policy must submit a written request to the Office of Technology Services (OTS). The request must include: The specific policy requirement(s) for which the exception is sought; a clear business justification and description of the operational need; the scope and duration of the requested exception; and a risk assessment and proposed compensating controls.

Final approval authority resides with the State Chief Information Officer (CIO) or their designee. Approved exceptions must be documented, time-bound, and subject to periodic review.

XI. EXPIRATION
This policy remains in effect until superseded or rescinded by the State Chief Information Officer.

XII. REFERENCES
- National Institute of Standards and Technology (NIST) U.S. Artificial Intelligence Safety Institute
- NIST AI Risk Management Framework
- Office of Technology Services Information Security Policy
- U.S. Government Accountability Office (U.S. GAO) AI Accountability Framework
- AI.gov Action Plan
- Executive Order Number JML 25-103: State Government's Use of AI