

Policies, Standards, and Guidelines			
Notice of Approval			
 Mississippi Department of Information Technology Services	Doc Ref Number: PSG-100-03		
	Title: Acceptable Use Policy for Artificial Intelligence		
	Document Type: ITS Agency	Page: 1 of 8	
	Domain: Enterprise	Status: Active	
	Effective Date: November 25, 2025	Revision Date: N/A	
Notice is hereby given, that the above specified document meets the requirements of the Mississippi Department of Information Technology Services Policies, Standards, and Procedures Program, thereby warranting approval for implementation, effective immediately.			
Signed by:  F577530FD3CA425... Executive Director Mississippi Department of Information Technology Services		November 25, 2025 Date of Signature	

	Doc Ref Number: PSG-100-03	
	Title: Acceptable Use Policy for Artificial Intelligence	
	Document Type: ITS Agency	Page: 2 of 8
	Domain: Enterprise	Status: Active
	Effective Date: November 25, 2025	Revision Date: N/A

1. **AUTHORITY**

The Mississippi Department of Information Technology Services (ITS) shall issue recommended strategies and goals for the effective and efficient use of information technology and services in state government. Miss. Code Ann. § 25-53-29(2). Additionally, ITS shall publish written planning guides, policies and procedures for use by agencies and institutions in planning future electronic information service systems. Miss. Code Ann. § 25-53-29(1)(b).

On January 8, 2025, Governor Reeves issued an Executive Order pertaining to Artificial Intelligence (AI). That Executive Order directed ITS, in accordance with the directives of Miss. Code Ann. § 25-53-1 *et seq.* to maximize the use and benefit from technologies and services, and to coordinate and develop policies pertaining to the responsible use of AI.

2. **PURPOSE**

This policy establishes requirements and guidelines for the responsible implementation and use of AI technologies within ITS to ensure security, privacy, transparency, and compliance in a manner that promotes and maintains public trust, minimizes risks, and maximizes the benefits of AI use in ITS operations.

3. **SCOPE**

This policy applies to all ITS users that plan, pilot, develop, acquire, use, deploy, and/or interact with AI systems within or as part of ITS operations. This policy governs the use of AI by ITS employees. The term “employee”, for the limited purpose of this policy, includes any person employed by ITS including fulltime, part-time, temporary, contractors, and any others authorized to use agency information systems. As with all state resources, all information system resources are to be used for state business purposes.

This policy covers all AI technologies, including but not limited to open-source (i.e., open to the public to modify, enhance, or inspect), proprietary (i.e., not made available to the public and users must purchase a license to rightfully use), and/or custom software, systems, tools, applications, utilities or solutions that include AI. AI categories covered by this policy include, but are not limited to, automation, predictive, generative, conversational, analytical, autonomous, cognitive, computer vision, decision-making, machine learning, natural language processing, etc. across all ITS divisions and functions of the agency.

4. **OVERVIEW**

Although AI can be used to modernize and transform the way ITS conducts business, including promoting a more efficient and productive working environment,

AI cannot replace human creativity and involvement and must be carefully used/deployed to mitigate potential risks and harm.

If used, AI shall be used in a responsible manner that enhances productivity and efficiency in ways that complement but does not replace ITS employee responsibilities.

5. AI PRINCIPLES

All AI use/deployment shall be rooted in the below principles and in a responsible manner that promotes and maintains public trust, minimizes risks, and maximizes benefits.

5.1 Innovation

5.1.1 AI should be leveraged to modernize and improve the delivery of state services and outcomes in an efficient manner that also protects and respects privacy, security, and confidentiality rights of the public and state information.

5.2 Responsible, Ethical, and Transparent Use

5.2.1 AI should be used responsibly and ethically to enhance productivity and efficiency in ways that complement employee efforts and in a manner that promotes and maintains public trust, considers impact, minimizes risks, and maximizes benefits.

5.2.2 Elements of transparency include: explainability, traceability, accountability, and openness. Examples may include:

- providing notice to those who may be impacted by AI use.
- how AI is used to support ITS business, disclosure of use of AI in content, interaction with AI versus human.
- decisions made by AI systems are understandable, traceable, and explainable including how systems are trained, and what data is used.
- being accountable in development and use of AI systems so that all can understand how and why.

5.3 Fairness

5.3.1 Use of AI systems should be fair and equitable in accordance with applicable state and federal laws and regulations. AI systems should be routinely tested and monitored to identify and mitigate bias, discrimination, and disproportionate impacts/outcomes.

5.4 Employee Oversight and Decision-Making

5.4.1 Employees must retain control over AI systems they use/deploy. Employees remain responsible for final decisions or deliverables made with AI support and/or outputs of AI systems. AI must complement employee expertise and judgment but not replace it. To do this, employee oversight should be integrated at various stages (as appropriate) to review, refine, or validate AI system results.

5.5 **Privacy and Data Protection**

- 5.5.1 AI systems must respect individual privacy, ensure data protection, comply with all applicable laws and regulations, and preserve individual privacy rights by design.
- 5.5.2 As the use of personally identifiable information (PII) or other Nonpublic data (i.e., information, other than PII, which may be sensitive, confidential, proprietary, and/or otherwise protected) can lead to unauthorized disclosures, legal liabilities, and other consequences, sensitive, confidential, or PII, PII and/or Nonpublic data must be handled with strict protection measures, with consent, where appropriate, and shall not be used with publicly available/accessible AI systems, services, or training models, including inputting PII/Nonpublic data in prompts.
- 5.5.3 Additional approval, processes, safeguards, and controls are required for AI systems involving PII/Nonpublic data.

5.6 **Safety and Security**

- 5.6.1 AI system safety, security, and resiliency must be evaluated to ensure the confidentiality, integrity, and availability of state data. Robust security measures must be implemented to protect AI systems from threats and mitigate AI-related risks. Regular risk assessments, vulnerability assessments, and continuous monitoring are essential.
- 5.6.2 AI systems must adhere to all applicable ITS and enterprise policy requirements. Incident response procedures and processes should be expanded to address AI system cybersecurity incidents, findings, mitigations, resolutions, and notification/reporting requirements.

5.7 **Accountability**

- 5.7.1 Agencies and their employees are accountable for the performance, impact, and consequences of AI use. AI systems should be reviewed on a regular basis for compliance with all applicable laws, regulations, policies, procedures, standards, guidelines, and best practices. Clear roles and responsibilities should be defined. AI use should also comply with the NIST Artificial Intelligence Risk Management Framework.

5.8 **Accessibility**

- 5.8.1 AI technologies should be designed and implemented to be inclusive and usable by individuals of all abilities and backgrounds. This includes ensuring AI interfaces are accessible to people with disabilities, providing multilingual support, and reducing barriers to AI adoption for underprivileged communities.

5.9 **Accuracy, Validity, and Reliability**

- 5.9.1 Mechanisms should be in place to ensure systems are working as intended with accurate output and performance.

5.10 **Auditability**

- 5.10.1 As appropriate, AI systems and outputs should be audited and monitored on a regular basis to ensure compliance with applicable laws, regulations, policies, standards, and best practices.

6. **ITS POLICY**

6.1 **Definitions**

- 6.1.1 “AI system” means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after use/deployment. For explicit or implicit objectives, this system infers, from the input it receives, how to generate outputs such as recommendations, content, predictions, or decisions that can influence either physical or virtual environments.
- 6.1.1.1 An AI system may be integrated into or operate in conjunction with other hardware or software.
- 6.1.1.2 As used throughout this policy, reference to “AI” shall have the same meaning as “AI system”.
- 6.1.2 “Personally Identifiable Information” or “PII,” means (1) any information that can be used to distinguish or trace an individual’s identity either alone, such as name, social security number, address, date of birth, or biometric records or (2) when combined with other information is linked or linkable to an individual, such as medical, educational, financial, and employment information.
- 6.1.3 “Nonpublic data” means information that is not subject to distribution to the public or information otherwise deemed to be sensitive, confidential, or protected. Examples include information exempt from disclosure by law, order, and/or that requires notice to parties prior to release or information that if were released, disclosed, misused, or accessed without authorization could cause harm, etc.
- 6.1.4 “Risk” means the combination of the probability of an occurrence or harm and the severity of that harm. An AI system is considered “high-risk” when it poses a risk to health, safety, financial, security, privacy, or an adverse impact on fundamental rights, including, but not limited to, materially influencing the outcome of decision making and/or any AI system that makes, or is a substantial factor in making, a consequential/high/significant impact or decision.
- 6.1.5 A high-risk AI system typically does not include:
- 6.1.5.1 The following technologies unless such technologies when used/deployed make or are a substantial factor in making a consequential decision, such as: (a) anti-fraud technology that does not use facial recognition technology; (b) anti-malware; (c) anti-virus; (d) artificial intelligence-enabled video games; (e) calculators; (f) cybersecurity; (g) databases; (h) data storage; (i) firewall; (j) internet domain registration; (k) internet website loading; (l) networking; (m) spam- and robocall-filtering; (n) spell-checking; (o)

spreadsheets; (p) web caching; (q) web hosting or any similar technology.

6.2 Approval by ITS for use

- 6.2.1 All AI deployment, interaction, and/or use for PII/Nonpublic data or high-risk AI systems must be approved by ITS.
- 6.2.2 AI systems which pose significant risk or harm, violate state or federal laws, regulations, and executive order, or ITS policies and/or procedures shall not be deployed or approved for use.
- 6.2.3 Approved AI systems shall only be used for approved purposes and in accordance with all applicable laws, regulations, orders, policies, and procedures that govern state employment.

6.3 Data Used in AI Systems

- 6.3.1 Uploading, integrating, entering, incorporating, sharing, and/or using any PII/Nonpublic data with and/or into nonapproved AI systems including prompts is strictly prohibited.
- 6.3.2 Any use of PII/Nonpublic data with an AI system must be with an AI system previously approved by ITS and for an authorized purpose.
- 6.3.3 Any use of PII/Nonpublic data must comply with applicable legal, regulatory, order, and/or policy requirements, and should adhere to best security and privacy practices.
- 6.3.4 Data used in ITS approved AI systems must be encrypted, stored securely, and proper access and security controls in place. Additionally, any access to AI systems or outputs should be regulated to prevent misuse. AI systems should be designed to incorporate advanced security measures to prevent data breaches, leakage, tampering, or unauthorized access or use. AI-generated outputs of personal, sensitive, or confidential data shall be reviewed and approved by employees before being acted upon in critical areas such as hiring, finance, legal decision-making, etc.
- 6.3.5 AI systems approved by ITS for use with PII/Nonpublic data shall not be allowed to train any AI systems on that data.

6.4 Employee Oversight

- 6.4.1 All content created by AI systems must be reviewed by the employee before it is shared or published to internal/external parties or acted upon.
- 6.4.2 All content created and/or decisions/impacts by high-risk AI systems shall be reviewed and approved before it is shared or published to internal/external parties or acted upon.

6.5 Data Governance

- 6.5.1 Use of data must comply with applicable data governance procedures and processes related to data availability, quality, integrity, reliability, ownership, access, use, classification, and validation.

- 6.5.2 Use of AI must comply with applicable data protection and privacy laws, regulations, policies, and procedures.

6.6 Security/Privacy/Risk Assessment Requirement

- 6.6.1 AI systems that will use PII/Nonpublic data and/or are high-risk shall undergo routine risk assessments and testing, where applicable. These routine assessments may occur prior to and after use/deployment to ensure accuracy, fairness, security, privacy, and compliance with applicable legal requirements.
- 6.6.2 AI systems must adhere to the State of Mississippi Enterprise Security Policies and Standards, where applicable.

6.7 AI Tools used for Note Taking and Transcription

- 6.7.1 Only approved AI systems can be utilized to record, transcribe, and summarize internal meetings and conversations within ITS. ITS reserves the right to restrict the use of AI note taking and related transcription tools.
- 6.7.2 Notification shall be provided prior to any AI note taking and/or related transcription tool being utilized in a meeting or conversation.
- 6.7.3 ITS recommends employees inquire, as appropriate, about the use of such AI systems during external meetings and/or conversations outside of ITS and/or meetings hosted by non-ITS employees (i.e., external parties) prior to participation.

6.8 Prohibited AI Uses

- 6.8.1 AI shall not be assumed to be truthful, credible, or accurate.
- 6.8.2 AI shall not be treated as the only source of reference.
- 6.8.3 AI shall not be used to issue official statements unless approved in writing by ITS executive management.
- 6.8.4 AI shall not be solely relied upon to make final decisions.
- 6.8.5 AI shall not be used to impersonate individuals or organizations.
- 6.8.6 AI shall not be used for any activities that are harmful, illegal, or in violation of state or federal laws, regulations, or state policy.
- 6.8.7 AI must not be used to manipulate or generate deceptive, harmful, or misleading content, including, but not limited to, deepfakes or misinformation.
- 6.8.8 AI shall not be used for unauthorized purposes.
- 6.8.9 AI shall not replace employee judgment in areas requiring ethical, critical, or sensitive decisions, such as compliance oversight, high-risk decisions or outcomes, or matters involving sensitive information.
- 6.8.10 AI systems deemed to be a security threat or that pose high-risks and are nonapproved shall not be used.
- 6.8.11 AI systems developed, hosted, or owned by foreign adversaries (as defined by NDAA 2026 15 C.F.R. § 7.4) as designated under federal

law (e.g., NDAA 2026 Section 1628, CISA advisories) shall not be used.

7. TRAINING/EDUCATION

7.1 Employees must complete AI training as provided by ITS.

8. MONITORING AND AUDIT

8.1 AI systems use, performance, outcomes, and impact shall be regularly monitored to ensure alignment with this policy, ITS values and goals, ITS business purposes, and approved usage.

9. REPORTING

9.1 Any AI-related issues, concerns, or questions should be documented and directed to the ITS employee's supervisor.

10. ACCEPTABLE USE/PERMITTED SOLUTIONS/APPLICATIONS

10.1 ITS will maintain a list of approved AI systems and approved uses.

11. PUBLIC RECORDS AND RECORD RETENTION

11.1 Use of AI systems may result in creation of a public record subject to the Mississippi Public Records Act, and applicable state retention rules, policies, and procedures. Therefore, employees must ensure that any record created using AI systems must be maintained in accordance with such applicable rules, regulations, and policies.

12. COMPLIANCE AND POLICY EXCEPTIONS

12.1 Violations of this policy, including disclosure of sensitive, personal, or confidential information as well as using AI systems in an unauthorized manner, may result in disciplinary action up to and including termination.

12.2 ITS reserves the right to terminate or suspend an employee's use of AI systems immediately or to otherwise disconnect, remove, block, filter, or restrict an employee's use of AI systems if ITS determines that such use violates this policy.

12.3 Any exception to this policy must be approved, in writing, by the Executive Director or their designee.

13. AMENDMENTS

13.1 This policy may be updated periodically. ITS users will be notified of updates and must be in compliance with the amended policy prior to use of any approved AI systems.

14. ATTACHMENTS

14.1 Executive Order No. 1584 (2025).

15. RESPONSIBLE PARTY/DIVISION

15.1 Strategy

Date Issued:	11/25/2025
Date Reviewed:	N/A
Date Revised:	N/A

STATE OF MISSISSIPPI

Office of the Governor



EXECUTIVE ORDER NO. 1584

WHEREAS, the State of Mississippi (“the State”) recognizes that artificial intelligence technologies (“AI”) are already being utilized by state agencies, that such emerging technologies will transform the way the State conducts business and provides services to its citizens, and that such technologies must also be carefully deployed to mitigate potential risks and harms; and

WHEREAS, the State aspires to fully harness AI to modernize the delivery of services to its citizens in a more efficient and effective manner, while at the same time protecting and respecting the privacy, security and confidentiality rights of all Mississippians; and

WHEREAS, to address AI, state agencies should identify and prepare for potential risks and harms as they deploy AI tools and systems throughout state government. To this end, the State needs to support stakeholders as they gather information and decide what, when, where, and how to utilize and oversee the use of these technologies; and

WHEREAS, the State acknowledges AI cannot completely replace human creativity or involvement and wishes to promote the responsible use of AI tools and systems in a manner that aligns and is consistent with the State’s policies, goals, values, and missions while maintaining citizen trust and balancing the benefits, risks, and potential harms of AI; and

WHEREAS, as the use of AI has implications for state, national, and personal security and privacy, it is necessary to ensure the use of AI is conducted in a responsible, ethical, transparent and beneficial manner; and

WHEREAS, the Mississippi Department of Information of Technology Services (“ITS”) is uniquely situated in the State to aid in the development of principles, guidelines and criteria relating to emerging technologies, enterprise security, information technology acquisitions, *etc.* pursuant to Title 25, Chapter 53 of the Mississippi Code.

NOW, THEREFORE, I, Tate Reeves, by the authority vested in me as Governor by the Constitution and laws of the State of Mississippi, do hereby order and direct as follows:

- I. *Definitions.* For the purposes of this Executive Order, the following terms shall be defined as indicated below:
- A. The term "artificial intelligence" has the meaning set forth in 15 U.S.C. § 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human- based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.
 - B. The term "generative AI" refers to AI that is capable of and used to produce new content, including, audio, code, images, text, and video, according to the data inputs and machine learning model it is trained on.
 - C. The terms “artificial intelligence” and “generative AI” as defined herein shall be collectively referred to as “AI”.
 - D. The term “state agency” has the meaning set forth in Miss. Code Ann. § 25-53-3 to include all the various state agencies, officers, departments, boards, commissions, offices and institutions of the State, excluding Institutions of Higher Learning.

II. *Directive.* In accordance with the directives of Miss. Code Ann. § 25-53-1 to maximize the use and benefit from technologies and services, and to improve the efficiency of providing common technology services across agency boundaries, ITS is directed and empowered to:

- A. Conduct an inventory of all AI technologies being planned, piloted, acquired, developed, and/or utilized by each state agency. In order to facilitate such inventory, ITS shall develop a standardized form, and such form shall be provided by ITS to each state agency for completion. Such completed forms shall be given protection under Miss. Code Ann. § 25-61-11.2;
- B. Evaluate the processes, guidelines (including procurement) and/or uses of AI currently in place at each state agency; and
- C. Coordinate with state agencies to develop policy recommendations for each agency’s responsible use of AI, including principles, guidelines, and criteria to govern the acquisition, development and utilization of AI by state agencies.

Such policy recommendations for the acquisition and use of AI shall be rooted in principles of fairness, innovation, privacy, security and safety, transparency, accountability, accessibility, validity, and reliability with safeguards to protect against potential harms and risks.

III. *Stakeholder Engagement.* ITS shall facilitate statewide coordination on the responsible, ethical, and productive use of AI in state government. ITS may engage Mississippi government stakeholders and/or other industry experts in AI to advise and/or provide recommendations, as needed, on best practices, uses, strategies, and other related tasks.

IV. *State Cooperation.* State agencies shall, to the extent consistent with Mississippi law, collaborate with ITS, including, but not limited to, completing the requested inventory of AI technologies on the form to be provided by ITS, furnishing assistance and information as requested by ITS, and specifying to ITS a designated agency staff person for AI coordination.

V. *Implementation and Effective Date.* This Executive Order shall be implemented to the maximum extent possible consistent with applicable law. Nothing in this Executive Order shall be construed as impairing or otherwise affecting the authority granted by law to any state agency, or the head thereof, except to the extent expressly set forth in this Executive Order. This Executive Order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any private party against the State, any of its agencies, departments, or entities, its officers, employees, or agents, or any other person. This Executive Order shall be effective upon execution and remain in force until amended, superseded or rescinded.



IN TESTIMONY WHEREOF, I have hereunto set my hand and caused the Great Seal of the State of Mississippi to be affixed.

DONE at the Capitol in the City of Jackson, the 8TH day of January, in the year of our Lord two thousand twenty-five, and of the Independence of the United States of America, the two hundred and forty-ninth.

Tate Reeves
TATE REEVES
GOVERNOR

BY THE GOVERNOR:

Michael Watson

MICHAEL WATSON
SECRETARY OF STATE