STATE *of* MISSOURI
ADMINISTRATIVE POLICY

POLICY: SP-19

POLICY TITLE: Acceptable Use for Artificial Intelligence

ISSUED: July 15, 2026

AUTHORIZED BY: Kenneth J. Zellers, Commissioner

I. Purpose and Benefits

This policy is designed to encourage responsible, safe, and secure exploration and use of Artificial Intelligence (AI) to benefit the consumers of Missouri services. It aims to foster public trust and confidence by ensuring that AI is used in a manner that is transparent, equitable, secure, and accountable. The use of AI must remain consistent with all applicable laws and regulations while upholding the privacy of all customers and Missourians.

II. Applicability

This policy applies to any State of Missouri employee, contractor, or third-party vendor accessing State networks or resources (hereafter 'user') who accesses, processes, or connects to any State data or IT resources (including but not limited to networks, applications, and systems) on behalf of the State. This definition does not include members of the public accessing publicly available State services. This policy applies regardless of the method, device, or location from which the connection is made.

III. Definitions

The following definitions are applicable to the words or phrases within this policy:

A. Artificial Intelligence (AI): A machine-based service that can make decisions, recommendations, predictions, or take action based on data inputs, where those decisions can influence virtual or real environments. This definition excludes standard, non-AI automated control systems, such as HVAC controllers or programmable logic controllers (PLCs), that operate on fixed, pre-programmed rules without adaptive decision-making.

B. Data Poisoning: A type of cyberattack in which an adversary intentionally compromises a training dataset used by an AI or machine learning (ML) model to influence or manipulate the operation of that model.

C. Drift: A phenomenon where an AI model's performance degrades over time due to changes in the data it is exposed to, causing its predictions or outputs to become less accurate or relevant.

D. Generative AI: Artificial intelligence (AI) service that generates text, images, audio, or other content based on learned patterns from large data sets.

E. Hallucination: When an Artificial Intelligence (AI) service generates inaccurate or nonsensical information.

F. Machine Learning (ML): A type of Artificial Intelligence (AI) in which computational systems use data to identify patterns or relationships and apply that analysis to generate outputs, improving in performance and accuracy through experience and exposure to additional data.

G. Model Bias: When an Artificial Intelligence (AI) service makes systematic errors or shows favor to certain groups, leading to unfair or discriminatory outcomes.

H. Prompt Injection: An attack that forces a generative model to produce unexpected output by manipulating the structure, instructions, or information contained in its prompt.

I. Third-Party Risk: The risk that data sent by the State of Missouri to third parties could be used for training, marketing, or other purposes not authorized by the State, potentially putting State data at risk.

J. Deterministic AI: A machine-based system that operates on predefined rules to produce consistent, predictable outputs for a given input, without the variability typically found in generative models. Examples include spellcheck, grammar-assistance tools, and standard search or autocomplete functions. Use of deterministic AI tools does not trigger the AI disclosure requirements described in Section V.

K. Open AI: Artificial intelligence systems where the underlying source code, model weights, and training data are made publicly accessible for review, use, and community development.

L. Closed AI: Proprietary artificial intelligence systems where the technology, code, training data, and model weights remain private and are strictly controlled by the developer or vendor.

IV. Guiding Principles

These principles form a blueprint of ethical behavior to guide State employees in using AI responsibly. Agencies must ensure that their AI applications are regularly tested against these requirements per Information Technology Services Division (ITSD) guidance. Mechanisms must be maintained to modify or deactivate AI applications that demonstrate performance inconsistent with their intended use or these principles.

A. Safe, Secure, and Resilient: AI services must undergo pre-deployment testing, risk identification, and mitigation. Ongoing monitoring must demonstrate the services are safe, effective, and resilient to attack, adhering to all State security standards. Specific objective testing criteria and standardized test protocols are maintained in supplementary ITSD technical procedure documents, which are updated as technology and threats evolve.

B. Transparent and Explainable: All content generated using AI for State use must be clearly identified as such. The public and impacted individuals must be provided with notice about the use of automated services and how they contributed to outcomes. The specific delivery mechanism for this notice (e.g., a phone script, website footer, or printed disclosure) is determined at the agency program level based on the tool and service channel used.

C. Privacy Enhanced: Access to data used in AI applications must be appropriately controlled, and privacy must be embedded into the design and architecture of any AI service. The quality and integrity of data used by AI services are paramount.

D. Fair and Unbiased: AI services must be developed and used in a way that is equitable and controls for biases that could lead to discriminatory results. AI Services should be user-centric and accessible to all people.

E. Valid and Reliable: Human oversight is required for the development, deployment, and use of all AI services used in the performance of job duties. Human oversight is necessary to ensure the use of AI does not negatively impact the rights, opportunities, or access to services for users of Missouri's services. Human oversight also ensures data generated by AI is reviewed for accuracy and is not corrupted by drift, bias, or hallucinations. Furthermore, agencies must ensure that input data is audited and verified to prevent poor quality from negatively affecting results obtained using AI assistance.

F. Accountable: Users of AI are accountable for its proper use. Agencies and the Office of Administration's ITSD (OA-ITSD) shall provide appropriate training to all relevant personnel. Users are responsible for ensuring there is no unauthorized publication or use of copyrighted material.

G. Governance: AI use must incorporate strong audit capabilities, with specific compliance protocols defined by ITSD and coordinated with agency IT units; stringent security measures; and sustainability practices, meaning practices that keep AI systems technically viable, maintainable, and supportable over time, in compliance with State oversight.

V. Key Responsibilities for All Users

All users are personally responsible for adhering to the following requirements when using any AI tool for State business:

A. Protect State Data: Do not introduce any confidential, sensitive, or protected State data into a public or non-State-issued AI tool. (Note: Use of this data within State-approved AI services is governed by Section VI and requires specific legal approval and guardrails.) This includes, but is not limited to:

1. Personally Identifiable Information (PII).
2. Protected Health Information (PHI).
3. Criminal Justice Information (CJI).
4. Federal Tax Information (FTI).
5. Controlled Unclassified Information (CUI).

6. State Tax Information.
7. Personnel Information.
8. Driver Privacy Protection Act (DPPA) Data.
9. Attorney-Client Privileged Communications.
10. Any internal, non-public State documents, strategies, or communications.
11. M365 Data Classification Guide (Missouri).
12. Statewide Intellectual Property.

B. **Meeting Transcription and Notetaking Tools:** AI-based meeting transcription or notetaking tools, including automated transcription bots, must not be used in meetings where confidential, restricted, or protected data is discussed unless the tool is a State-approved enterprise service with appropriate data protections in place. The decision to approve such tools for a given data tier rests with the agency; users may not independently determine that a transcription tool is appropriate for a sensitive meeting.

C. **Assume Human Oversight:** Users are responsible for the final work product and must assume that AI-generated content requires rigorous human review. Always review, edit, and fact-check any output from an AI tool before use. Do not assume AI-generated content to be accurate, complete, or free from bias or hallucinations.

D. **Disclose AI Use:** When AI has been used to in whole or in part with the assistance of AI technology it must be disclosed. The author reviewed and edited the final product and takes full responsibility for the content." AI-generated drafts, including drafts not used in a final product, are subject to State record retention schedules and may be responsive to Sunshine Law requests or legal discovery; users must label AI-assisted drafts accordingly and must not delete them outside of normal retention practices.

E. **Review for Accuracy and Bias:** Critically evaluate AI-generated content for factual errors, nonsensical information (hallucinations), and potential bias.

F. **Respect Copyright and Intellectual Property:** The user is responsible for ensuring that their use of AI does not infringe on copyrights. Do not include, insert, or input third-party copyrighted material without permission, and do not use AI-generated output in a way that violates intellectual property rights.

G. **Report Issues:** If a user discovers that an AI tool is producing biased, inaccurate, or insecure results, the user must report the issue to their supervisor and the ITSD Help Desk immediately. Escalation Process: Cease use of the tool for that specific workflow, submit a ticket detailing the prompt and the erroneous output, and await clearance from ITSD before resuming use of the tool for that task.

H. **Prohibit Malicious Misuse:** Users shall not use any AI tool, State-approved or otherwise, to scan, probe, or test State or third-party systems for security vulnerabilities without explicit written authorization from ITSD Cybersecurity; to create non-consensual deepfake images, audio, or video of any individual; or to engage in social engineering, impersonation, or other deceptive practices.

VI. Use of State-Approved AI Services

This section applies to AI tools that have been formally procured, vetted, and issued by the State of Missouri for official business.

A. Agency and Office of Administration Responsibilities

1. **Risk Management:** Before deployment, agencies, in coordination with ITSD, must use the National Institute of Standards and Technology (NIST) AI Risk Management Framework (AI RMF 1.0) to assess and manage risks associated with the AI service. This assessment must be reviewed by the agencies in coordination with ITSD on an ongoing basis (defined as at least annually, or immediately following any major system update or reported security vulnerability).

2. **Testing and Security Review:** All State-approved AI services must pass the same security and technology standards review as any other software or platform implemented within the State government. This includes regular testing for vulnerabilities, resilience, reliability, and accuracy. Specific objective testing criteria and audit protocols for this review are maintained in supplementary ITSD technical procedure documents and coordinated with agency IT units.

3. **Data Quality Management:** Agencies, under the standards and guidelines established by of the Office of Administration, are responsible for ensuring that the quality of the data used in AI tools is continuously monitored and assessed to maintain accuracy, completeness, consistency, timeliness, relevance, and objectivity. Agencies shall employ best practices—such as auditing, verification, and data cleansing—to alleviate data quality issues (e.g., the "garbage in-garbage out" effect) and ensure the reliability of AI outcomes.

4. **Training:** OA-ITSD shall provide core training on AI risks and security (e.g., KnowBe4). Agencies are responsible for training personnel on the specific business use cases and workflows for the AI tools they deploy. Agency legal departments shall review third-party vendor contracts and Business Associate Agreements (BAAs) to ensure that those agreements are appropriately amended to cover the use of Generative AI tools offered by those vendors and used by the State. ITSD shall provide appropriate training to all personnel responsible for the design and development of AI.

B. User Responsibilities and Permissible Use

The permissible use of a State-approved AI tool is for its intended and authorized purpose within the scope of a user's official duties. All users of State-approved tools must adhere to the following responsibilities, in addition to the key responsibilities for all users outlined in Section V:

1. **Adhere to Training:** Users must complete all required agency and OA training for the specific AI tool they are using. Users must also execute the Generative AI User Acceptance Agreement (UAA) before being granted

access to any State-approved AI tool.

2. **Use for Authorized Purpose:** State-approved AI tool may only be used for assigned job duties and in accordance with the training and authorization provided. The use of AI tools for official State business is strictly limited to State-approved AI. Users must obtain approval from their Agency Director (or designee) before using any restricted data (as defined in the Data Classification Guide Missouri 01SEP25 (2).docx) in an AI tool. Restricted data may be used only when proper guardrails are in place and with individual agency approval. State-approved enterprise AI tools operate within a contracted, closed-tenant environment governed by Business Associate Agreements (BAAs) or equivalent contractual data protections, meaning State data is not used to train public models. This protection is what permits the careful, approved use of restricted data within these tools, while use of such data remains strictly prohibited in any public or non-State-issued AI tool. These responsibilities are specific to State-approved tools and apply in addition to the general rules in Section V.

3. **Report Malfunctions or Concerns:** If a user finds that a State-approved AI tool is producing inaccurate, biased, outdated, or otherwise problematic results, they must report the issue promptly to their supervisor and the ITSD Help Desk to ensure it can be addressed systemically.

4. **Data Hygiene:** Users must ensure they are cleaning up websites or internal sources by not leaving draft AI prompts, unverified AI outputs, or residual AI-generated code in shared State workspaces.

VII. Guidance for Non-State-Issued AI Tools (e.g., ChatGPT, Gemini, Midjourney)

This section governs the use of publicly available, commercial, or free AI tools that have not been formally approved and provided by the State of Missouri. The State operates on a strict 'trust but verify' ethos regarding these tools. Use of these tools is considered high-risk, and outputs must always be rigorously cross-checked. Any use for State business must be approached with extreme caution and is limited to the permissible uses listed below.

A. Any information entered into a public AI tool can be stored, shared, and used by the third party to train their models. Control of that data is lost permanently. There is no expectation of privacy or security for information entered into these tools.

B. Prohibited Uses (Users SHALL NOT):

1. Introduce any data defined as confidential, sensitive, or protected in Section V of this policy into publicly available commercial AI tools.
2. Use these tools to create official government records or formal written communications on behalf of the agency without rigorous human review and explicit supervisor approval.
3. Input any State-owned intellectual property, draft legislation, or pre-decisional policy documents.

4. Generate code for use in State applications or services without a thorough security review by ITSD.
5. Use the tools for any activity that would violate State law, existing policies, or professional codes of conduct (e.g., copyright infringement, discrimination, or privacy violations).

C. Permissible Uses (Users MAY, with caution):

1. Brainstorming and ideation on general, non-sensitive topics.
2. Summarizing publicly available articles or research papers.
3. Improving grammar and style on non-sensitive, non-confidential text (e.g., improving the phrasing of a sentence for a general-purpose presentation).
4. Learning about AI capabilities in a way that does not involve State data or resources.

VIII. Enforcement

Violations of this policy may result in disciplinary action, up to and including termination of employment, and/or legal action where applicable.

IX. References

NIST AI Risk Management Framework (AI RMF 1.0) - https://www.nist.gov/itl/ai-risk-management-framework.