

IT-17 Use of Artificial Intelligence in State of Ohio Solutions

State of Ohio Administrative Policy

No: IT-17 Information Technology

Effective: January 5, 2026

Issued By: Kathleen C. Madden, Director

I. Purpose

The purpose of this policy is to provide statewide planning, implementation, procurement, security, privacy, and governance requirements for the use of Artificial Intelligence (AI). The policy authorizes the implementation of AI, while establishing an operational framework that will assist in protecting Ohioans' Data and the Integrity and Quality of the information delivered through AI solutions. All defined terms are capitalized and a link to the glossary of definitions is found in section IV.

II. Scope

This policy applies to all state agencies, boards, and commissions under the authority of the Governor (collectively referred to as Agency or Agencies).

III. Policy

While AI can deliver significant business value to the State of Ohio, responsible implementation requires a deliberate and detailed approach. Agencies considering the implementation of AI must ensure that processes are in place to effectively manage the technology and achieve the desired results. This policy details the requirements for integrating AI technologies into state solutions.

A. AI Solution Development

As part of AI planning and implementation, Agencies must follow the iterative activities outlined below:

1. Defining a formal process for identifying, documenting, reviewing, and approving AI use cases. Agency use cases and solutions must align with the core AI

Principles.

2. Submission of Agency approved use cases to the AI Council as appropriate (refer to section F. for additional information).
3. Designing an approved use case pilot prior to a full production implementation.
4. Conducting any necessary data quality testing for pilot and full production of AI deployments, including:
 - a. Reviewing and testing any AI generated output for proper functionality and security.
 - b. Testing the Data sets for AI Models to determine errors related to bias and variance.
 - c. Testing activities must be properly documented.
5. Defining the hand-off criteria to determine when judgment and decisions from an AI solution are transitioned to a human.
6. Charging human operators with reviewing AI outputs for accuracy, appropriateness, privacy, and security before being acted upon or disseminated. AI outputs must not be assumed to be truthful, credible, or accurate.
7. Ensuring that a human verification process is in place for decisions made by AI that have a legal, financial, human resources, legislative, organizational, or regulatory impact.
8. Ongoing monitoring of AI generated output to validate that errors or Data bias are not introduced as the Model evolves.

B. Workforce Requirements

Agencies must ensure that the workforce understands the requirements for appropriate AI use as outlined below. To assist in this effort, the Ohio Department of Administrative Services (DAS), in coordination with Agencies, must establish AI training for the state's workforce.

1. **Authorization for Use:** The use of Generative AI for work purposes must be approved by the Agency director or designee and must be in alignment with the requirements defined by the AI Council (refer to section III.F. for additional details).
2. **Authorized Solutions:** Only State-Managed or Governed Data Ecosystem, and AI Council approved, Generative AI solutions can be used to conduct state business.
3. **Disclosing Use:** When Generative AI is used to create a deliverable for Agency use, employees, contractors, and temporary personnel must be required to disclose this information to their Agency (e.g., written documentation, research, correspondence, and software code).
4. **Importance of Verifying Accuracy:** Review, revise, and fact check via multiple sources any output from a Generative AI solution before use. The human user is responsible for any material created with AI support.

5. Ethical Considerations: The training must create awareness regarding the ethical considerations surrounding the use of AI, in particular, Generative AI.
 - a. AI outputs must not be used to impersonate individuals or organizations without their written permission.
 - b. Material that is inappropriate for public release must not be entered as input to AI solutions unless explicitly approved by the Agency director, chief legal counsel, chief information officer or designee for the intended use case.
 - c. Generative AI can make assumptions based on past stereotypes and the information provided may need to be corrected.
6. Secure Use: The security, privacy, and Data concerns surrounding the use of AI.

C. AI Procurements

When seeking to procure an AI solution, Agencies must adhere to the following requirements:

1. AI procurement solicitations offered by suppliers must align with the requirements of this policy.
2. All AI software services, even if they are free or part of a pilot or proof-of-concept project, must be reviewed by the Agency to ensure the software meets all necessary security and privacy requirements. This requirement applies to downloadable software, Software as a Service (SaaS), web-based services, browser plug-ins, and smartphone apps.
 - a. The following elements must be captured and evaluated for any AI solution during the procurement process:
 - i. Technical/design details of the AI system and algorithms
 - ii. How the AI system was trained (including personnel and documentation)
 - iii. How the AI system works (i.e., what are the inputs and outputs)
 - iv. Data sources (documentation of all Data sources)
 - v. Audit Logging
 - vi. Change Management details and documentation that impact the AI system algorithms (i.e., decisions, inputs, outputs)
 - vii. Testing practices and results
 - viii. Timeframe documentation (captures time periods of testing, governance approval, deployment, and other critical milestones of the AI solution)
 - b. New AI software requests must be submitted for review and possible approval to the AI Council (refer to section F.).
3. Agency contracts must prohibit suppliers from using State of Ohio materials or Data in Generative AI solutions, unless such use is explicitly approved by the Agency director or designee.

4. Procuring Agencies must ensure suppliers disclose the utilization of Generative AI when producing works owned by the state or the integration of Generative AI in products used by the state.
5. Procuring Agencies must submit to the AI Council the Supplier Assessment for Generative AI Solutions form, completed by the supplier, in the following circumstances:
 - a. statewide contracts for Generative AI solutions;
 - b. custom Generative AI solutions;
 - c. public facing Generative AI solutions; and
 - d. when requested by DAS.
6. Procuring Agencies must perform due diligence to ensure proper licensure of Model training Data for all Generative AI services using non-state Data.
7. All copyrightable works owned by the state that are created with the involvement of Generative AI must include an accompanying annotation sufficient to meet the requirements of the U.S. Copyright Office for Works Containing Material Generated by Artificial Intelligence (88 FR 16190). The annotation should include at least the Generative AI technology used and a description of how it was used to create the work.

D. Security and Privacy

Agencies must ensure that AI solutions adhere to state IT security and privacy laws, policies, and standards. In addition, Agencies must comply with the following requirements:

1. Security: Agencies must implement the following security controls when designing AI solutions:
 - a. Conduct a risk assessment of a proposed AI solution, including considerations of exploitation by malicious actors or inadvertent uses by authorized users. Determine appropriate security controls to mitigate against such risk.
 - b. Establish controls to prevent adversarial learning attacks that try to influence or corrupt the Data Model by detecting abnormal network traffic.
 - c. Ensure that authentication and authorization controls align with state and Agency policy.
 - d. Confidential Data, including Personally Identifiable Information (PII) and Confidential Personal Information, must not be input into unconstrained Generative AI solutions and publicly accessible service or training Models.
2. Privacy: Agencies must protect the privacy of individuals when using AI solutions. This includes, but is not limited to, implementing the following privacy controls:
 - a. AI Models must not be used to collect or store PII without the consent of the individual.

- b. AI solutions must only collect, use, share, and store Data in accordance with federal and state privacy and personal Data laws and policies.
- c. The AI solution must disclose to the user that they are interacting with a State of Ohio AI solution and the Data sources for the information must be provided.

E. Data Governance

The State of Ohio Chief Data Officer (CDO) Council must be responsible for establishing and maintaining statewide Data governance requirements, including those for AI solutions. The requirements must define information management controls, procedures, and processes for Data set selection, evaluation, and preparation. The controls must address, but not be limited to, the following principles:

- 1. Data Availability, Quality, and Integrity are critical for AI systems. AI systems must not be trained with Data that is biased, inaccurate, incomplete, or misleading.
- 2. AI systems must only have access to the Data sources they need for the specific context.
- 3. Data must be regulated through established Data sharing agreements that identify the applicable federal and state laws and policies for the AI solution use case. The agreements must outline the acceptable terms for Data use, storage, and transmission.
- 4. Data sources used with AI Models must be properly parsed into multiple, randomized Data sets consisting of training, cross-validation, and test Data.
- 5. Data validation procedures must be in place to select, analyze, clean, and certify the Integrity of the Data sources that will be used for AI automation solutions.
- 6. Data Steward, Data Owner, and Data Custodian roles must be responsible for maintaining the Quality and Integrity of Agency AI Data Models.
- 7. Every proposed Generative AI solution's Data Model must receive Agency executive and data governance approval followed by the AI Council (refer to section F.) prior to implementation.

F. AI Council

DAS must establish a multi-Agency AI Council to govern the statewide use of Generative AI solutions. The AI Council must include representatives from the Governor's Office; DAS and Agency business, human resources, information technology, security, privacy, Data analytics, and legal functional areas; and the DAS Office of Opportunity and Accessibility.

The AI Council must provide oversight for the following:

1. Directing the establishment of and the ongoing use of a statewide sandbox environment to safely explore the use of Generative AI to enhance the experience of the workforce and Ohioans.
2. Examining the social, economic, and legal impacts of AI adoption on the workforce, Ohioans, and business operations.
3. Defining the legal requirements for the use of third-party AI services, contracts, licenses, agreements, and specific AI solution use cases.
4. Establishing the framework for evaluating and authorizing the use of AI technology (e.g., architecture frameworks, software, infrastructure, and relevant tools).
5. Developing and maintaining a statewide central repository that captures approved Generative AI use cases.
6. Documenting protocols and procedures for assessing and handling inquiries or incidents regarding AI system anomalies.
7. Auditing AI current and future solutions to ensure alignment with the requirements of this policy.

IV. Definitions

All defined terms are capitalized within the policy and the online glossary of definitions can be found at IT Policy Glossary - Department of Administrative Services.

V. Authority

ORC 125.18

VI. Resources

- IT-13 Data Classification - Department of Administrative Services
- IT-14 Data Encryption and Securing Confidential Data - Department of Administrative Services
- IT-19 Data Governance - Department of Administrative Services
- ITS-SEC-02 Enterprise Security Controls Framework - Department of Administrative Services
- State of Ohio IT Hub - Generative AI (Supplier Assessment for Generative AI Solutions Form)
- National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations
- AI Risk Management Framework - NIST
- NIST-AI-600-1, Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (PDF)
- NIST AI Resource Center

VII. Inquiries

Direct inquiries about this policy to:

State IT Policy Manager
Office of Information Technology
Ohio Department of Administrative Services
30 East Broad Street, 39th Floor
Columbus, Ohio 43215
1-614-644-6860 | DAS.State.ITPolicy.Manager@das.ohio.gov

State of Ohio Administrative Policies may be found online at Policy Finder - Department of Administrative Services

VIII. Revision History

This policy must be reviewed no less than every two years and updated as needed.

Date	Description of Change
12/04/2023	Original Policy
01/05/2026	Clarified the workforce requirements. Removed the references to underfitting and overfitting. Added a requirement that only state-managed or governed data ecosystem and AI Council approved, generative AI solutions can be used to conduct state business. Removed the data input requirement as it was replaced with the new authorized solutions requirement. Added requirements for when a Supplier Assessment for Generative AI Solutions form must be completed. Updated the data model requirements to require data governance approval. Replaced sensitive data with confidential data and updated the resources and terminology.
01/05/2028	Scheduled policy review.