




State of Ohio Administrative Policy

Use of Artificial Intelligence in State of Ohio Solutions

No:
IT-17
Information Technology

Effective:
December 4, 2023

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. The first occurrence of a defined term in the policy is in bold, italic type, and is hyperlinked to the definition 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 shall 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 shall 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 shall 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 the degree of **Underfitting**, **Overfitting**, and errors related to bias and variance.
 - c) Testing activities shall 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 shall 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:** The Ohio Department of Administrative Services (DAS), in coordination with Agencies, shall establish AI training for the state's workforce that addresses the implications of and appropriate use of AI, which includes:

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. **Disclosing Use:** When Generative AI is used to create a deliverable for Agency use, employees, contractors, and temporary personnel shall be required to disclose this information to their Agency (e.g., written documentation, research, correspondence, and software code).
3. **Data Input Restrictions:** If a state employee, contractor, or temporary personnel is authorized to use a **Generative AI** tool for state business, they are required to only enter data into the tool that is considered a public record.
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 shall create awareness regarding the ethical considerations surrounding the use of AI, in particular, Generative AI.

- a) AI outputs shall not be used to impersonate individuals or organizations without their written permission.
 - b) Material that is inappropriate for public release shall not be entered as input to AI tools 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 shall 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, shall 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 shall 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 the of AI solution)
 - b) New AI software requests shall be submitted for review and possible approval to the AI Council (refer to section F.).
 3. Agency contracts shall 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 shall 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 shall perform due diligence to ensure proper licensure of Model training Data for all Generative AI services using non-state Data.
 6. 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 shall ensure that AI solutions adhere to state IT security and privacy laws, policies, and standards. In addition, Agencies shall comply with the following requirements:
1. Security: Agencies shall 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) **Sensitive Data**, including **Personally Identifiable Information (PII)** and **Confidential Personal Information**, shall not be input into unconstrained Generative AI tools and publicly accessible service or training Models.
 2. Privacy: Agencies shall protect the privacy of individuals when using AI solutions. This includes, but is not limited to, implementing the following privacy controls:
 - a) AI Models shall not be used to collect or store PII without the consent of the individual.
 - b) AI solutions shall only collect, use, share, and store Data in accordance with federal and state privacy and personal Data laws and policies.
 - c) The AI solution shall disclose to the user that they are interacting with a State of Ohio AI solution and the Data sources for the information shall be provided.
- E. **Data Governance:** The State of Ohio **Chief Data Officer (CDO) Council** shall be responsible for establishing and maintaining statewide Data governance requirements, including those for AI solutions. The requirements shall define information management controls, procedures, and processes for Data set selection, evaluation, and preparation. The controls shall address, but not be limited to, the following principles:

1. Data **Availability**, Quality, and Integrity are critical for AI systems. AI systems shall not be trained with Data that is biased, inaccurate, incomplete, or misleading.
2. AI systems shall only have access to the Data sources they need for the specific context.
3. Data shall 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 shall outline the acceptable terms for Data use, storage, and transmission.
4. Data sources used with AI Models shall be properly parsed into multiple, randomized Data sets consisting of training, cross-validation, and test Data.
5. Data validation procedures shall 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 shall 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 approval followed by the AI Council (refer to section F.) prior to implementation.

- F. **AI Council:** DAS shall establish a multi-Agency AI Council to govern the statewide use of Generative AI solutions. The AI Council shall 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 shall 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

- A. **Artificial Intelligence (AI)**. Interdisciplinary field, usually regarded as a branch of computer science, dealing with Models and systems for the performance of functions generally associated with human intelligence, such as reasoning and learning.¹
- B. **AI Principles**. As defined by Gartner, the core AI Principles include:
 - 1. Fair (minimize bias)
 - 2. Accountable (purposeful and ethical – human feedback loop)
 - 3. Secure and Safe (Data privacy, security framework, risk management)
 - 4. Explainable and Transparent (build trust)
 - 5. Human-Centric and Socially Beneficial (service to the public)²
- C. **Availability**. Ensuring timely and reliable access to and use of information.³
- D. **Chief Data Officer (CDO) Council**. The CDO Council serves as Ohio's data governance and analytics recommending body, providing support to the State CDO to help guide and advance Ohio's strategic data roadmap. The CDO Council membership consists of the State CDO, who serves as the council's chair, and agency CDOs.
- E. **Confidential Personal Information**. Personal information that falls within the scope of Section 1347.15 of the Ohio Revised Code and that an agency is prohibited from releasing under Ohio's public records law.
- F. **Data**. Coded representation of quantities, objects, and actions. The word, "Data," is often used interchangeably with the word, "information," in common usage and in this policy.
- G. **Data Custodian**. A person responsible for the safe custody, transport, and storage of state Data, as well as the implementation of any applicable federal, state, or Agency Data protection requirements.
- H. **Data Owner**. A person responsible for ensuring that all Data and Data products within their domain are protected and managed appropriately pursuant to law, policy, and procedures. The Data Owner is also responsible for authorizing access and/or sharing of their Data, in consultation with their designated legal and privacy representatives.
- I. **Data Steward**. A person responsible for the day-to-day management of a dataset and serves as the subject matter expert who understands and communicates the meaning and use of information.

¹ Reznik, Leon, NIST Trustworthy & Responsible AI Resource Center Glossary <https://airc.nist.gov/AI_RMF_Knowledge_Base/Glossary>.

² Choudhary, Farhan, Svetlana Sicular. "A Comprehensive Guide to Responsible AI," Gartner, 28 July 2022, <<https://www.gartner.com/document/4017080?ref=solrAll&refval=371095535>>.

³ "NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations," U.S. Department of Commerce National Institute of Standards and Technology, April, 2013 <<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>>.

- J. **Generative AI.** A kind of AI capable of generating new content such as code, images, music, text, simulations, 3D objects, videos, and so on. It is considered an important part of AI research and development, as it has the potential to revolutionize many industries, including entertainment, art, and design.⁴
- K. **Integrity.** Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.⁵
- L. **Model.** For the purposes of this policy, a Model is something that is trained on a broad set of unlabeled Data that can be used for different tasks, with additional fine-tuning.⁶
- M. **Overfitting.** Overfitting occurs when a Model tries to predict a trend in Data that is too noisy. Overfitting is the result of an overly complex Model with too many parameters. A Model that is overfitted is inaccurate because the trend does not reflect the reality of the Data. An overfitted Model is a Model with a trend line that reflects the errors in the Data that it is trained with, instead of accurately predicting unseen Data.⁷
- N. **Personally Identifiable Information (PII).** Information that can be used directly or in combination with other information to identify a particular individual. It includes:
 - 1. a name, identifying number, symbol, or other identifier assigned to a person,
 - 2. any information that describes anything about a person,
 - 3. any information that indicates actions done by or to a person,
 - 4. any information that indicates that a person possesses certain personal characteristics.⁸
- O. **Quality.** Degree to which the characteristics of Data satisfy stated and implied needs when used under specified conditions.
- P. **Sensitive Data.** Sensitive Data is any type of Data that presents a high or moderate degree of risk if released, disclosed, modified, or deleted without authorization. There is a high degree of risk when unauthorized release or disclosure is contrary to a legally mandated confidentiality requirement. There may be a moderate risk and potentially a high risk in cases of information for which an Agency has discretion under the law to release Data, particularly when the release must be made only according to Agency policy or procedure. The Data may be certain types of Personally Identifiable Information that is also sensitive such as medical information, social security numbers, and financial account numbers. It includes Federal Tax Information under IRS Special Publication 1075, Protected Health Information under the

⁴ Arham, Islam, NIST Trustworthy & Responsible AI Resource Center Glossary <https://airc.nist.gov/AI_RMF_Knowledge_Base/Glossary>.

⁵ “NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations,” U.S. Department of Commerce National Institute of Standards and Technology, April 2013 <<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>>.

⁶ “Gartner Experts Answer the Top Generative AI Questions for Your Enterprise,” Gartner, 24 August 2023, <<https://www.gartner.com/en/topics/generative-ai>>.

⁷ Ranschaert, Erik, NIST Trustworthy & Responsible AI Resource Center Glossary <https://airc.nist.gov/AI_RMF_Knowledge_Base/Glossary>

⁸ Based on Ohio Revised Code Section 1347.01 (E).

Health Insurance Portability and Accountability Act, Criminal Justice Information under Federal Bureau of Investigation’s Criminal Justice Information Services (CJIS) Security Policy, and the Social Security Administration Limited Access Death Master File. Sensitive Data may also be other types of information not associated with a particular individual such as security and infrastructure records, trade secrets and business bank account information.

Q. [Underfitting](#). Underfitting occurs when a statistical Model cannot adequately capture the underlying structure of the Data.⁹

V. Authority

ORC 125.18

VI. Resources

Document Name	Location
Ohio Administrative Policy IT-13, Data Classification	https://das.ohio.gov/technology-and-strategy/policies/it-13
Ohio Administrative Policy IT-14, Data Encryption and Securing Sensitive Data	https://das.ohio.gov/technology-and-strategy/policies/it-14
Ohio IT Standard ITS-SEC-02, Enterprise Security Controls Framework	https://das.ohio.gov/technology-and-strategy/policies/its-sec-02-enterprise-security-controls-framework
National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations	https://csrc.nist.gov/publications/sp
NIST Trustworthy & Responsible AI Resource Center	https://airc.nist.gov/home

VII. Inquiries

Direct inquiries about this policy to:

State IT Policy Manager
 Office of Information Technology
 Ohio Department of Administrative Services

⁹ Ranschaert, Erik, NIST Trustworthy & Responsible AI Resource Center Glossary <https://airc.nist.gov/AI_RMF_Knowledge_Base/Glossary>.

30 East Broad Street, 39th Floor
Columbus, Ohio 43215

1-614-466-6930 | DAS.State.ITPolicy.Manager@das.ohio.gov

State of Ohio Administrative Policies may be found online at
<https://das.ohio.gov/technology-and-strategy/policies>

VIII. Revision History

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

Date	Description of Change
12/04/2023	Original Policy
12/04/2025	Scheduled policy review.