State of Indiana Policy: *State Agency Artificial Intelligence Implementations*

Version: 1.0 (2/2024)

Contents

1. Purpose

The proliferation of information technology enabled by artificial intelligence presents tremendous opportunity for Indiana State Government to continue to enhance service provision, policy-, and decision-making for the benefit of Hoosiers. At the same time, artificial intelligence presents significant risks that, if not managed effectively, can negatively impact the State of Indiana and our population. The National Institute of Standards and Technology's AI Risk Management Framework makes this clear:

> Artificial intelligence (AI) technologies have significant potential to transform society and people's lives – from commerce and health to transportation and cybersecurity to the environment and our planet. AI technologies can drive inclusive economic growth and support scientific advancements that improve the conditions of our world. AI technologies, however, also pose risks that can negatively impact individuals, groups, organizations, communities, society, the environment, and the planet. Like risks for other types of technology, AI risks can emerge in a variety of ways and can be characterized as long- or short-term, high- or low-probability, systemic or localized, and high- or low-impact.
>
> While there are myriad standards and best practices to help organizations mitigate the risks of traditional software or information-based systems, the risks posed by AI systems are in many ways unique. AI systems, for example, may be trained on data that can change over time, sometimes significantly and unexpectedly, affecting system functionality and trustworthiness in ways that are hard to understand. AI systems and the contexts in which they are deployed are frequently complex, making it difficult to detect and respond to failures when they occur. AI systems are inherently socio-technical in nature, meaning they are influenced by societal dynamics and human behavior. AI risks – and benefits – can emerge from the interplay of technical aspects combined with societal factors related to how a system is used, its interactions with other AI systems, who operates it, and the social context in which it is deployed.
>
> These risks make AI a uniquely challenging technology to deploy and utilize both for organizations and within society. Without proper controls, AI systems can amplify, perpetuate, or exacerbate inequitable or undesirable outcomes for individuals and communities. With proper controls, AI systems can mitigate and manage inequitable outcomes.
>
> AI risk management is a key component of responsible development and use of AI systems. Responsible AI practices can help align the decisions about AI system design, development, and uses with intended aim and values. Core concepts in responsible AI emphasize human centricity, social responsibility, and sustainability. AI risk management can drive responsible uses and practices by prompting organizations and their internal teams who design, develop, and deploy AI to think more critically about context and potential or unexpected negative and positive impacts. Understanding and managing the risks of AI systems will help to enhance trustworthiness, and in turn, cultivate public trust.

NIST AI 100-1.

The purpose of this Policy is to balance these interests, enabling the efficient and ethical use of artificial intelligence by State Agencies.

2. Applicability and Interpretation

This Policy shall apply to all AI Systems, excepting those governed by conflicting provisions in State or Federal law or regulation. For the sake of clarity:

1. it applies to AI Systems including, but not limited to, those that are open source, those developed by a State Agency, those developed by a third party under agreement with a State Agency, those purchased as commercial off-the-shelf solutions, and combinations thereof; and
2. it shall *not* be interpreted to apply to ad-hoc State employee use of web-based generative artificial intelligence applications where the use is not contemplated in a contract executed pursuant to IC 4-13-2, the Indiana Financial Reorganization Act of 1947.

Interpretation of this Policy, associated standards, procedures, guidance, and relevant law shall be at the discretion of the State Chief Privacy Officer, in consultation with relevant stakeholders.

3. Revision History

Version	Date	Name	Revision Description	Supersedes
1.0	2/2024	J. Cooper T. Cotterill	Initial version.	n/a

4. Authority

This Policy is promulgated by the Office of the Chief Data Officer pursuant to IC 4-3-26 as a component policy of the State of Indiana Policies on Information Privacy and Information Quality.

5. Ownership

Please direct questions and concerns to the following owner(s) of this Policy, which will coordinate stakeholder communication as necessary:

1. The State Chief Privacy Officer

6. Definitions

1. “AI Implementation Activities” means the planning, design, development, deployment, operation, and monitoring, whether occurring independently or collectively, associated with an AI System.
2. “AI System” means an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI Systems are designed to operate with varying levels of autonomy.
3. “Agency Privacy Officer” means the associated individual in each State Agency designated under the *State of Indiana Policy: Information Privacy*.

4. "Data" means Government Information and Personal Information, collectively, as set forth in IC 4-3-26-7 and IC 4-1-6-1(2), respectively.
5. "External Partner" means an individual, or related employing organization, that is under contract or other similar agreement with a State Agency.
6. "NIST" means the National Institute of Standards and Technology established by 15 U.S.C. §272.
7. "NIST AI RMF" means the AI Risk Management Framework 1.0 (NIST AI 100-1), adopted January, 2023.
8. "OCDO" means the Office of the Chief Data Officer established by IC 4-3-26-9.
9. "Policy" means this *State of Indiana Policy: State Agency Artificial Intelligence Systems*
10. "Process" means any operation or set of operations performed, whether by manual or automated means, on Data or on sets of Data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of Data.
11. "State Agency" has the meaning set forth in IC 4-3-26-2.
12. "Violation" means all activities contemplated by the Policy that are not expressly allowed by the Policy.

7. Exceptions

All exceptions are considered policy deviations and may be granted in accordance with applicable law by the Chief Privacy Officer or designee. Administrative or technical requirements may indicate the need for exemption from this Policy, for specific matters. Following an appropriate risk assessment, the Chief Privacy Officer or designee, can acknowledge and/or escalate exception requests. Exceptions will be timely documented in the system designated by the OCDO for that purpose.

Requests for exceptions must use the appropriate form and be approved by the Agency Privacy Officer or designee, prior to submission. At a minimum, the request must document the following:

- the subcategory of the NIST AI RMF Core for which the exception is needed;
- the business justification and impact of the exception;
- the additional risks identified as a result of exception implementation; and
- the compensating controls that are planned or implemented to reduce the additional risk to an acceptable level.

All exceptions must be documented in accordance with this Policy. Exceptions must be reevaluated on a grouped and rolling biannual basis, in July and January. Exceptions granted in the three (3)-month period preceding an evaluation period will first be revaluated during the next reevaluation period.

8. Violations

8.1 Violation by State Employees

Violation of this Policy by an employee may subject the violating individual to removal from relevant AI Implementation Activities. Such a Violation will commence a review by the OCDO of all access related to

the violating individual. Violation of this Policy may constitute employee misconduct and will be addressed in accordance with applicable law and policy, including but not limited to the State Employee Handbook.

8.2 Violation by External Partner

Violation of this Policy by an External Partner may subject the External Partner to removal from relevant AI Implementation Activities. Such a Violation will commence a review by the OCDO of all access related to the External Partner and may avail the relevant State Agency to remedies under contract through which the External Partner is supporting the AI Implementation Activities.

This statement of penalties is not intended to be exhaustive, and the omission of any penalty does not negate the ability of any proper party, including a data subject, to bring an action for violation of law.

8.3 Violation of Obligations by a State Agency

Violation of this Policy may subject the violating State Agency to termination of relevant AI Implementation Activities.

9. Policy

9.1 Background

The Management Performance Hub empowers the legal exchange and utilization of Data by and between State Agencies. A core component of this responsibility is the application of controls that enable the efficient and ethical use of Data to inform service provision to, and decision-making for, Hoosiers. The Management Performance Hub exercises its policymaking function through the OCDO.

Today, many initiatives that involve the Processing of Data are conducted using AI. While the State of Indiana wishes to realize the benefits of AI to empower positive innovation to advance the Hoosier condition, it is incumbent on governance leaders in Indiana to apply appropriate controls, thereby ensuring that proposed uses of AI realize its positive benefits while avoiding its negative risks. As has been discussed in *Sec. 1, Purpose*, a core objective of this Policy is to enable the deployment of trustworthy AI Systems by Indiana State Government. Again, the NIST AI RMF makes this clear:

> For AI systems to be trustworthy, they often need to be responsive to a multiplicity of criteria that are of value to interested parties. Approaches which enhance AI trustworthiness can reduce negative AI risks. This Framework articulates the following characteristics of trustworthy AI and offers guidance for addressing them. Characteristics of trustworthy AI systems include valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair with harmful bias managed. Creating trustworthy AI requires balancing each of these characteristics based on the AI system's context of use… Neglecting these characteristics can increase the probability and magnitude of negative consequences.

NIST AI 100-1.

To this end, AI Implementation Activities and their resulting AI Systems are subject to the following principles and controls.

9.2. Adoption of the NIST AI Risk Management Framework

It is the policy of the State of Indiana that a State Agency conducting AI Implementation Activities and operating an AI System do so in accordance with the NIST AI RMF.

The NIST AI RMF Core is made up of four primary categories: Govern, Map, Measure, and Manage, each with multiple subcategories that guide the user to achieving the aim of deploying trustworthy AI Systems. In partnership with relevant stakeholders, the Agency Privacy Officer of a State Agency conducting AI Implementation Activities shall ensure that the resulting AI System is assessed in accordance with this Policy, as implemented by the *State of Indiana Standard: State Agency Artificial Intelligence Systems.*

For the sake of clarity, the Agency Privacy Officer shall be responsible for submitting readiness and maturity assessment documentation to the OCDO at designated milestones during the planning and pre-deployment phases of AI Implementation Activities. Post-deployment assessments are triggered by specified occurrences. Reference the Standard for detailed instruction.

9.3. Notice to Individuals

A core tenant of the NIST AI RMF is transparency, which involves the extent to which information about an AI System and its outputs is available to individuals interacting with the AI System. After deployment of the AI System, transparency is greatly enhanced by providing relevant notice to users.

The Indiana Fair Information Practice Act requires agencies to provide notice to individuals in certain circumstances. For instance, when personal information is collected, a notice must articulate, among other things, the statutory authority which supports collection, how the agency will use the information, and whether disclosure by the data subject is mandatory or voluntary. Given the unique issues presented by AI, an AI System requires a 'just-in-time' notice to adequately inform the user of otherwise-concealed processes associated with the interaction.

In this context, the just-in-time notice enables the disclosure of specific information practices and is posted or presents itself at the point of information collection or interaction with the AI System. For instance, in the event a State Agency uses AI to make a recommendation to a user through a web browser, the just-in-time notice makes clear to the user that AI is involved and details relevant Data Processing that might otherwise be unclear.

Relevant notices must be reviewed and approved by the State CPO, in accordance with *State of Indiana Policy: Information Privacy.*

9.4 Additional OCDO Activities

1. In accordance with OCDO policies and procedures, the OCDO shall require an Indiana enterprise data catalog scan of the state-owned or -licensed source system related to the AI System.

2. The OCDO shall work in conjunction with the Department of Administration and Office of Technology to ensure that appropriate contractual controls are imposed on External Partners related to AI Implementation Activities and resulting AI Systems.
3. At its discretion, the OCDO shall promulgate, and may audit conformance to, standards, procedures, and guidance in furtherance of this Policy.

10. References

1. *NIST AI Risk Management Framework 1.0 (NIST AI 100-1)*, https://doi.org/10.6028/NIST.AI.100-1.
2. *NIST AI RMF Playbook,* https://airc.nist.gov/AI_RMF_Knowledge_Base/Playbook.
3. State of Indiana Policy: *Information Privacy 2.0,* https://www.in.gov/mph/cdo/files/20230811-FINAL-State-of-Indiana-Information-Privacy-Policy.pdf.
4. State of Indiana Standard: *State Agency Artificial Intelligence Systems,* https://www.in.gov/mph/cdo/files/State-of-Indiana-State-Agency-AI-Systems-Standard.pdf.