State of Indiana Standard: *State Agency Artificial Intelligence Systems*

Version: 1.0 (2/2024)

Contents

State of Indiana Standard: *State Agency Artificial Intelligence Systems*

Version: 1.0 (2/2024)

1. Purpose

The purpose of this Standard is to implement the *State of Indiana Policy: State Agency Artificial Intelligence Systems*, enabling the efficient and ethical use of artificial intelligence by State Agencies.

2. Revision History

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

3. Definitions

Terms used and not defined in this section may be referenced in the Policy.

1. "Project Team" means the collection of individuals designated by the OCDO, Office of Technology, and relevant State Agency to guide AI Implementation Activities, as required under Sec. 4.1.

4. Standard

4.1 Readiness Assessment for AI Implementation Activities: Planning Phase

During the initial planning phase, prior to related procurements, the Agency Privacy Officer or designee shall submit the relevant proposal and readiness assessment documentation to the OCDO using the method prescribed for that purpose. The goal of the proposal and readiness assessment documentation is to understand and align stakeholders on aspects central to the successful deployment, maintenance, and operation of an AI System. Such documentation shall include the following information:

1. Objectives of the proposed AI System;
2. Regulatory obligations associated with the proposed AI System, including its training, testing, production input, and production output data; and
3. Availability of appropriate data, infrastructure, and staffing resources to conduct AI Implementation Activities, pre- and post-deployment.

The OCDO shall review related submissions and advise on readiness in accordance with this section. The Agency Privacy Officer shall await response from the OCDO prior to proceeding with proposed AI Implementation Activities.

Upon successful completion of the readiness assessment required by this section, a Project Team shall be convened by the Office of the Chief Data Officer, consisting of no more than three decisionmakers from each relevant State Agency.

4.2. Maturity Assessments: Pre-Deployment

Throughout the lifecycle of initial planning, design, and development phases, stakeholders shall consider targets outlined in the NIST AI RMF Core against the identified criteria and profile tier levels, and shall strive to meet or exceed them at the time of deployment.

Immediately prior to the deployment of an AI System, a maturity assessment shall be conducted. The maturity assessment will include a review of the NIST AI RMF Core subcategories, as found in Appendix A, in the context of the questions and profile tier selections described in *Sec. 4.4, Maturity Assessments: Criteria Considered*.

Upon completion, the assessment shall be reported to the OCDO using the method prescribed for that purpose. The OCDO shall review related submissions and advise on the efficient and ethical use of Data in accordance with the Policy. The Agency Privacy Officer shall await completion of the maturity assessment required by this section and favorable response from each member of the Project Team, based on their respective authorities, prior to proceeding with deployment of the AI System. The Project Team shall issue its overall determination in writing, including a description of any necessary remediation activities.

4.3. Maturity Assessments: Post-Deployment

Following initial deployment of the AI System, a review of the maturity assessment shall be conducted going forward at such time as significant changes are made to the same, or annually, whichever occurs first. Significant changes may include the following:

- New policies or procedures have been developed or implemented that affect how the AI System Processes information.
- Merging of the AI System's information with information from another process or system.
- Changes to the stakeholder management or ownership of the AI System, including infrastructure and access control changes.
- Modifications to the accessibility, information Processing, or information sharing processes in the AI System.
- Alterations to the character of the information in the AI System, such as the addition of new information fields to the AI System model.
- Significant modifications in the content or scope of AI System outputs are observed.

Upon completion, the assessment shall be reported to the OCDO using the method prescribed for that purpose. The OCDO shall review related submissions and advise on the efficient and ethical use of Data in accordance with the Policy.

4.4. Maturity Assessments: Criteria Considered

In the maturity assessment process, the following questions shall be asked with respect to each subcategory:

- Based on the name and description of this subcategory, does the AI System follow appropriate controls, policies, and procedures to meet this standard? (Y/N)
- What is your current profile? (See profile tier selections below.)
- Is the current profile selected acceptable? (Y/N)
- What is your target profile? (See profile tier selections below.)

PROFILE TIER SELECTIONS

TIER	DESCRIPTION
Tier 0: Non-Existent	Appropriate processes and controls do not exist, lack of awareness and knowledge.
Tier 1: Initial	Processes and controls are ad-hoc, not documented (informal), poorly controlled and not repeatable.
Tier 2: Developing	Processes and controls are managed and documented. Implementation and execution is inconsistent.
Tier 3: Defined	Processes and controls are standardized, well established, consistently used, repeatable, periodically reviewed and updated.
Tier 4: Advanced	Processes and controls are continuously assessed for improvements. Could be considered best in class or leading practice. Sharable and adopted by others.

4.5 Notice to Individuals

Reference the Policy for State Agency notice obligations.

5. 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 Policy: *State Agency Artificial Intelligence Systems*, https://www.in.gov/mph/cdo/files/State-of-Indiana-State-Agency-AI-Systems-Policy.pdf.

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

APPENDIX A – NIST AI RMF CORE

GOVERN

CATEGORY	SUBCATEGORY
GOVERN 1: Policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks are in place, transparent, and implemented effectively.	**GOVERN 1.1:** Legal and regulatory requirements involving AI are understood, managed, and documented.
	GOVERN 1.2: The characteristics of trustworthy AI are integrated into organizational policies, processes, procedures, and practices.
	GOVERN 1.3: Processes, procedures, and practices are in place to determine the needed level of risk management activities based on the organization's risk tolerance.
	GOVERN 1.4: The risk management process and its outcomes are established through transparent policies, procedures, and other controls based on organizational risk priorities.
	GOVERN 1.5: Ongoing monitoring and periodic review of the risk management process and its outcomes are planned and organizational roles and responsibilities clearly defined, including determining the frequency of periodic review.
	GOVERN 1.6: Mechanisms are in place to inventory AI systems and are resourced according to organizational risk priorities.
	GOVERN 1.7: Processes and procedures are in place for decommissioning and phasing out AI systems safely and in a manner that does not increase risks or decrease the organization's trustworthiness.
GOVERN 2: Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks.	**GOVERN 2.1:** Roles and responsibilities and lines of communication related to mapping, measuring, and managing AI risks are documented and are clear to individuals and teams throughout the organization.
	GOVERN 2.2: The organization's personnel and partners receive AI risk management training to enable them to perform their duties and responsibilities consistent with related policies, procedures, and agreements.
	GOVERN 2.3: Executive leadership of the organization takes responsibility for decisions

	about risks associated with AI system development and deployment.
GOVERN 3: Workforce diversity, equity, inclusion, and accessibility processes are prioritized in the mapping, measuring, and managing of AI risks throughout the lifecycle.	**GOVERN 3.1:** Decision-making related to mapping, measuring, and managing AI risks throughout the lifecycle is informed by a diverse team (e.g., diversity of demographics, disciplines, experience, expertise, and backgrounds).
	GOVERN 3.2: Policies and procedures are in place to define and differentiate roles and responsibilities for human-AI configurations and oversight of AI systems.
GOVERN 4: Organizational teams are committed to a culture that considers and communicates AI risk.	**GOVERN 4.1:** Organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of AI systems to minimize potential negative impacts.
	GOVERN 4.2: Organizational teams document the risks and potential impacts of the AI technology they design, develop, deploy, evaluate, and use, and they communicate about the impacts more broadly.
	GOVERN 4.3: Organizational practices are in place to enable AI testing, identification of incidents, and information sharing.
GOVERN 5: Processes are in place for robust engagement with relevant AI actors.	**GOVERN 5.1:** Organizational policies and practices are in place to collect, consider, prioritize, and integrate feedback from those external to the team that developed or deployed the AI system regarding the potential individual and societal impacts related to AI risks.
	GOVERN 5.2: Mechanisms are established to enable the team that developed or deployed AI systems to regularly incorporate adjudicated feedback from relevant AI actors into system design and implementation.
GOVERN 6: Policies and procedures are in place to address AI risks and benefits arising from third-party software and data and other supply chain issues.	**GOVERN 6.1:** Policies and procedures are in place that address AI risks associated with third-party entities, including risks of infringement of a third-party's intellectual property or other rights.
	GOVERN 6.2: Contingency processes are in place to handle failures or incidents in third-party data or AI systems deemed to be high-risk.

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

APPENDIX A – NIST AI RMF CORE

MAP

CATEGORY	SUBCATEGORY
MAP 1: Context is established and understood.	**MAP 1.1:** Intended purposes, potentially beneficial uses, context-specific laws, norms and expectations, and prospective settings in which the AI system will be deployed are understood and documented. Considerations include: the specific set or types of users along with their expectations; potential positive and negative impacts of system uses to individuals, communities, organizations, society, and the planet; assumptions and related limitations about AI system purposes, uses, and risks across the development or product AI lifecycle; and related test, evaluation, verification, and validation ("TEVV") and system metrics.[1]
	MAP 1.2: Interdisciplinary AI actors, competencies, skills, and capacities for establishing context reflect demographic diversity and broad domain and user experience expertise, and their participation is documented. Opportunities for interdisciplinary collaboration are prioritized.
	MAP 1.3: The organization's mission and relevant goals for AI technology are understood and documented.
	MAP 1.4: The business value or context of business use has been clearly defined or – in the case of assessing existing AI systems – re-evaluated.
	MAP 1.5: Organizational risk tolerances are determined and documented.
	MAP 1.6: System requirements (e.g., "the system shall respect the privacy of its users") are elicited from and understood by relevant AI actors. Design decisions take socio-technical implications into account to address AI risks.

[1] For more information regarding TEVV, reference NIST AI 100-1, Appendix A: *Descriptions of AI Actor Tasks from Figures 2 and 3.*

MAP 2: Categorization of the AI system is performed.	**MAP 2.1:** The specific tasks and methods used to implement the tasks that the AI system will support are defined (e.g., classifiers, generative models, recommenders).
	MAP 2.2: Information about the AI system's knowledge limits and how system output may be utilized and overseen by humans is documented. Documentation provides sufficient information to assist relevant AI actors when making decisions and taking subsequent actions.
	MAP 2.3: Scientific integrity and TEVV considerations are identified and documented, including those related to experimental design, data collection and selection (e.g., availability, representativeness, suitability), system trustworthiness, and construct validation.
MAP 3: AI capabilities, targeted usage, goals, and expected benefits and costs compared with appropriate benchmarks are understood.	**MAP 3.1:** Potential benefits of intended AI system functionality and performance are examined and documented.
	MAP 3.2: Potential costs, including non-monetary costs, which result from expected or realized AI errors or system functionality and trustworthiness – as connected to organizational risk tolerance – are examined and documented.
	MAP 3.3: Targeted application scope is specified and documented based on the system's capability, established context, and AI system categorization.
	MAP 3.4: Processes for operator and practitioner proficiency with AI system performance and trustworthiness – and relevant technical standards and certifications – are defined, assessed, and documented.
	MAP 3.5: Processes for human oversight are defined, assessed, and documented in accordance with organizational policies from the GOVERN function.
MAP 4: Risks and benefits are mapped for all components of the AI system including third-party software and data.	**MAP 4.1:** Approaches for mapping AI technology and legal risks of its components – including the use of third party data or software – are in place, followed, and documented, as are risks of

	infringement of a third party's intellectual property or other rights.
	MAP 4.2: Internal risk controls for components of the AI system, including third-party AI technologies, are identified and documented.
MAP 5: Impacts to individuals, groups, communities, organizations, and society are characterized.	**MAP 5.1:** Likelihood and magnitude of each identified impact (both potentially beneficial and harmful) based on expected use, past uses of AI systems in similar contexts, public incident reports, feedback from those external to the team that developed or deployed the AI system, or other data are identified and documented.
	MAP 5.2: Practices and personnel for supporting regular engagement with relevant AI actors and integrating feedback about positive, negative, and unanticipated impacts are in place and documented.

MEASURE

CATEGORY	SUBCATEGORY
MEASURE 1: Appropriate methods and metrics are identified and applied.	**MEASURE 1.1:** Approaches and metrics for measurement of AI risks enumerated during the MAP function are selected for implementation starting with the most significant AI risks. The risks or trustworthiness characteristics that will not – or cannot – be measured are properly documented.
	MEASURE 1.2: Appropriateness of AI metrics and effectiveness of existing controls are regularly assessed and updated, including reports of errors and potential impacts on affected communities.
	MEASURE 1.3: Internal experts who did not serve as front-line developers for the system and/or independent assessors are involved in regular assessments and updates. Domain experts, users, AI actors external to the team that developed or deployed the AI system, and affected communities are consulted in support of assessments as necessary per organizational risk tolerance.

MEASURE 2: AI systems are evaluated for trustworthy characteristics.	**MEASURE 2.1:** Test sets, metrics, and details about the tools used during TEVV are documented.
	MEASURE 2.2: Evaluations involving human subjects meet applicable requirements (including human subject protection) and are representative of the relevant population.
	MEASURE 2.3: AI system performance or assurance criteria are measured qualitatively or quantitatively and demonstrated for conditions similar to deployment setting(s). Measures are documented.
	MEASURE 2.4: The functionality and behavior of the AI system and its components – as identified in the MAP function – are monitored when in production.
	MEASURE 2.5: The AI system to be deployed is demonstrated to be valid and reliable. Limitations of the generalizability beyond the conditions under which the technology was developed are documented.
	MEASURE 2.6: The AI system is evaluated regularly for safety risks – as identified in the MAP function. The AI system to be deployed is demonstrated to be safe, its residual negative risk does not exceed the risk tolerance, and it can fail safely, particularly if made to operate beyond its knowledge limits. Safety metrics reflect system reliability and robustness, real-time monitoring, and response times for AI system failures.
	MEASURE 2.7: AI system security and resilience – as identified in the MAP function – are evaluated and documented.
	MEASURE 2.8: Risks associated with transparency and accountability – as identified in the MAP function – are examined and documented.
	MEASURE 2.9: The AI model is explained, validated, and documented, and AI system output is interpreted within its context – as identified in the MAP function – to inform responsible use and governance.

	MEASURE 2.10: Privacy risk of the AI system – as identified in the MAP function – is examined and documented.
	MEASURE 2.11: Fairness and bias – as identified in the MAP function – are evaluated and results are documented.
	MEASURE 2.12: Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented.
	MEASURE 2.13: Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented.
MEASURE 3: Mechanisms for tracking identified AI risks over time are in place.	**MEASURE 3.1:** Approaches, personnel, and documentation are in place to regularly identify and track existing, unanticipated, and emergent AI risks based on factors such as intended and actual performance in deployed contexts.
	MEASURE 3.2: Risk tracking approaches are considered for settings where AI risks are difficult to assess using currently available measurement techniques or where metrics are not yet available.
	MEASURE 3.3: Feedback processes for end users and impacted communities to report problems and appeal system outcomes are established and integrated into AI system evaluation metrics.
MEASURE 4: Feedback about efficacy of measurement is gathered and assessed.	**MEASURE 4.1:** Measurement approaches for identifying AI risks are connected to deployment context(s) and informed through consultation with domain experts and other end users. Approaches are documented.
	MEASURE 4.2: Measurement results regarding AI system trustworthiness in deployment context(s) and across the AI lifecycle are informed by input from domain experts and relevant AI actors to validate whether the system is performing consistently as intended. Results are documented.
	MEASURE 4.3: Measurable performance improvements or declines based on consultations with relevant AI actors, including affected

	communities, and field data about context-relevant risks and trustworthiness characteristics are identified and documented.

MANAGE

CATEGORY	SUBCATEGORY
MANAGE 1: AI risks based on assessments and other analytical output from the MAP and MEASURE functions are prioritized, responded to, and managed.	**MANAGE 1.1:** A determination is made as to whether the AI system achieves its intended purposes and stated objectives and whether its development or deployment should proceed.
	MANAGE 1.2: Treatment of documented AI risks is prioritized based on impact, likelihood, and available resources or methods.
	MANAGE 1.3: Responses to the AI risks deemed high priority, as identified by the MAP function, are developed, planned, and documented. Risk response options can include mitigating, transferring, avoiding, or accepting.
	MANAGE 1.4: Negative residual risks (defined as the sum of all unmitigated risks) to both downstream acquirers of AI systems and end users are documented.
MANAGE 2: Strategies to maximize AI benefits and minimize negative impacts are planned, prepared, implemented, documented, and informed by input from relevant AI actors.	**MANAGE 2.1:** Resources required to manage AI risks are taken into account – along with viable non-AI alternative systems, approaches, or methods – to reduce the magnitude or likelihood of potential impacts.
	MANAGE 2.2: Mechanisms are in place and applied to sustain the value of deployed AI systems.
	MANAGE 2.3: Procedures are followed to respond to and recover from a previously unknown risk when it is identified.
	MANAGE 2.4: Mechanisms are in place and applied, and responsibilities are assigned and understood, to supersede, disengage, or

	deactivate AI systems that demonstrate performance or outcomes inconsistent with intended use.
MANAGE 3: AI risks and benefits from third-party entities are managed.	**MANAGE 3.1:** AI risks and benefits from third-party resources are regularly monitored, and risk controls are applied and documented.
	MANAGE 3.2: Pre-trained models which are used for development are monitored as part of AI system regular monitoring and maintenance.
MANAGE 4: Risk treatments, including response and recovery, and communication plans for the identified and measured AI risks are documented and monitored regularly.	**MANAGE 4.1:** Post-deployment AI system monitoring plans are implemented, including mechanisms for capturing and evaluating input from users and other relevant AI actors, appeal and override, decommissioning, incident response, recovery, and change management.
	MANAGE 4.2: Measurable activities for continual improvements are integrated into AI system updates and include regular engagement with interested parties, including relevant AI actors.
	MANAGE 4.3: Incidents and errors are communicated to relevant AI actors, including affected communities. Processes for tracking, responding to, and recovering from incidents and errors are followed and documented.