Policy on the Acceptable and Responsible Use of Artificial Intelligence

Effective Date: April 1, 2025

1. Introduction

The Department of Innovation and Technology ("DoIT") is the primary agency responsible for Information Technology ("IT") within State of Illinois government (the "State"). DoIT has developed this Policy (the "Policy") for the acceptable and responsible use of artificial intelligence systems and technologies ("AI"), as defined below, within and on behalf of State governmental entities.

AI offers significant potential benefits to Illinois residents by both improving public services and enhancing State operational efficiency. This Policy is intended to balance allowing State use of AI while mitigating potential risks.

Entities associated with the development, deployment, and use of AI Systems (as defined below) may be broadly divided into two categories: (1) those who create AI Systems, including related algorithms, models, and data ("AI Creators"); and (2) those who use or consume those AI Systems ("AI Consumers"). While the compliance aims and obligations of both groups will have significant overlap, the requirements to achieve those aims and obligations may differ.

AI development, deployment, use, and governance must be aligned with State law and applicable privacy, ethical, and technology standards. The following is a structured approach adapted to meet the State's legal and ethical requirements.

2. Scope & Authority

This Policy applies to DoIT and the agencies under the jurisdiction of the Governor (each an "Agency" or collectively, "Agencies"), through the authority provided in the Department of Innovation and Technology Act (20 ILCS 1370/1-15(d)). For clarity, this Policy applies to Agencies—in their potential roles as AI Consumers, AI Creators, or both—by addressing any AI Systems that may be developed, deployed, or used by an Agency. This Policy will take effect immediately upon execution. Within 30 days of the effective date of this Policy, Utilizing Agencies must designate an employee to perform the functions required by the AI Policy, and provide a

report detailing all known AI Systems currently deployed, in active development, or in use, including whether such systems are allowed or will be allowed to use State data or has direct or indirect access to Protected Data (defined below). For AI Systems that on the effective date of the Policy are already deployed, in active development, or in use, Agencies shall have 90 calendar days to either bring such systems into compliance, or develop a plan with a definite timeline to bring such systems into compliance.

Many of the requirements and concepts below directly relate to each Agency's own mission and existing compliance obligations. Compliance with this Policy depends on the Agency's own determinations regarding its mission, specific needs, and existing compliance obligations related to protected or sensitive information collected, held, or used by the Agency. However, DoIT shall be available to assist with technical questions an Agency may have. When procuring any related technology products or services on an Agency's behalf, DoIT will provide technical support for the Agency's reporting requirements under this Policy.

3. Definitions

- **Artificial Intelligence ("AI"):** Refers to the use of computer programs that can perform tasks traditionally requiring human intelligence, such as problem-solving, decision-making, predictions, recommendations, ongoing learning, etc. The use of AI as covered by this Policy includes machine learning, natural language processing, deep learning, neural networks, large language models, algorithmic decision support, pattern recognition, anomaly detection, computer vision, generative AI, and similar functionality.
- **AI System:** Any software, system (physical or virtual), or application that uses AI in whole or in part to perform tasks (examples include virtual meeting assistants, digital voice assistants, customer service chatbots, facial recognition software, and writing assistant services, among many others).
- **Generative AI:** A type of AI model that emulates the structure and characteristics of input data to generate derived synthetic content, which may include images, videos, audio, text, other digital content, or various combinations of the above.
- **Utilizing Agency:** Means the specific Agency or Agencies that procure, develops, deploys, or uses any AI system contemplated under this Policy and whose responsibility it is that such AI Systems comply with this Policy.
- **Training Data:** refers to data used to build, tune, test, and validate an AI System. Some models will require use of Operational Data (defined below) to periodically or continuously train and/or re-train.
- **Operational Data**: refers to data input, used, or generated (either directly or indirectly) when an AI System is deployed and generating outputs in a live environment. Such data

would include user prompts, feedback or data related to user interaction and system telemetry, and drift monitoring. Operational data may be used for additional or as performance indicators related to retraining needs.

4. Ethical Requirements

AI Systems shall not:

a. **Discriminate:** AI Systems shall not be used, developed, or deployed in ways that could potentially discriminate against individuals or groups of people based on race, gender, religion, ethnicity, disability, economic status, or any other protected characteristic.

b. **Infringe Privacy:** AI Systems shall not violate relevant data privacy laws and regulations, but instead must ensure the secure and responsible handling of personal information and avoid copyright infringement.

c. **Mislead or Manipulate**: AI Systems shall not be used to spread false or misleading information, deceive users, or manipulate public opinion.

d. **Make Decisions without Oversight:** AI Systems shall not make decisions autonomously without oversight. AI Systems must have a "human in the loop" to ensure that all decisions are, ultimately, made by humans.

e. **Violate Human Rights:** AI Systems shall not be used to undermine or cause harm to human rights.

f. **Access Protected, Sensitive, or Confidential Information:** AI Systems shall not, without written authorization signed by the Agency Head, directly or indirectly have access to: any information or data that is protected under law or regulation (including but not limited to, PIPA, HIPAA, CJIS, etc.) or that is sensitive, confidential, or otherwise prohibited from disclosure (all together, "Protected Data"). In the event a Utilizing Agency chooses to authorize an AI System to access Protected Data as outlined in this section 5(f), the Utilizing Agency must notify DoIT 30 calendar days prior to the date on which the AI System would first have direct or indirect access to Protected Data. The Utilizing Agency then further must ensure throughout the duration of such access and on an ongoing basis afterwards:

    i. that the AI System is and remains fully contained in, and its access to and use of the Protected Data occur entirely within, a separate, private environment;

    ii. that any Protected Data to which the AI System has direct or indirect access does not become part of a public model or dataset, in any form; and

    iii. that any AI System granted such access shall not reproduce or generate any output that embeds or otherwise includes the Protected Data, or make any decisions based on such Protected Data, except in both cases only as and to

the extent that the Utilizing Agency has strictly and explicitly defined in its written authorization.

5. Transparency and Accountability

a. **Clear Communication:** When users interact with an AI System, the Utilizing Agency shall disclose to those users that they are interacting with an AI System.

b. **Disclosures:** Agencies must disclose the use of AI in any products and services those Agencies rely upon. This disclosure must contain a full and clear description of how AI is used in the applicable products and services and must be communicated in writing to the users of those products and services.

c. **Explanation of Decision-making:** When an AI System is used to support decision making, the Utilizing Agency shall disclose and make available the role of the AI System in supporting decision making.

d. **Human Oversight:** AI Systems shall have appropriate and ongoing human oversight to review and intervene in cases of potential bias, errors, or potential adverse impacts. To achieve this, Utilizing Agencies shall define and assign clear oversight roles and responsibilities to applicable personnel for the entirety of an AI System's lifecycle to ensure its development, deployment, and/or use align with Illinois's legal and regulatory frameworks.

e. **Data Management:** Agencies shall only use high-quality, trusted, and vetted data sources.

    i. Agencies shall not allow the use of State of Illinois data in any way for AI-related purposes (including but not limited to model building and inference reference), without the express written consent of the Agency head.

    ii. In the event an Agency determines it will allow the use of State of Illinois data for AI-related purposes, the Agency must provide advance written notice to DoIT at least 30 calendar days before the Utilizing Agency makes any commitment to the procurement, development, or deployment of the AI System or allows any already deployed AI System to begin using State of Illinois data (whichever occurs first).

f. **Accountability:** Any Agency planning to use AI Systems shall, prior to such use, assess the AI System's adherence to this Policy and create a written report documenting the findings and conclusions of the assessment. This report will need signoff from the Agency head and must be provided to DoIT at least 30 calendar days before Utilizing Agency makes a commitment to the procurement, development, or deployment of an AI System (whichever occurs first).

6. Deciding on Human Involvement

a. **Workflow and Processes:** Utilizing Agencies shall establish documented protocols for human oversight and/or intervention in automated, or partially automated, AI processes. To ensure efficient oversight and intervention, Utilizing Agencies shall:

   i. Outline the scope of AI deployment by determining what to automate and what to assign to human review. Utilizing Agencies must have specific justifications for these decisions.

   ii. Consider Human-in-the-Loop intervals for automated processes.

   iii. Structure the workflow in such a way that prefers human oversight over intervention wherever possible.

7. Maintaining, Monitoring, Documenting, and Reviewing Agency Data Use and Access for AI Systems:

a. **Monitoring and Maintenance:** Utilizing Agencies shall implement continuous monitoring and maintenance protocols for use of and access to Agency data in AI Systems, ensuring they comply with Illinois law and any applicable laws and regulations applicable to an Agency's data over time.

b. **Change Management:** Utilizing Agencies shall extensively document AI Systems' design, development, deployment, and any modifications with the respect to the use of and access to Agency data, promoting transparency and accountability in line with Illinois law.

8. Reviewing Communication and Feedback Mechanisms:

a. **Communication:** Utilizing Agencies shall maintain transparent communication channels in writing with stakeholders, ensuring compliance with applicable Illinois law.

b. **Feedback:** Utilizing Agencies shall develop feedback mechanisms for stakeholders to report AI-related concerns or issues, especially those affecting legal rights within Illinois.

9. Organizational Awareness:

a. **Internal Communication:** Utilizing Agencies shall each promote organization-wide awareness of AI's legal, ethical, and operational aspects, emphasizing the importance of escalating issues to experts familiar with Illinois law.

10. Data Usage and Privacy

a. **Data Collection:** Utilizing Agencies shall ensure that data collected for use by AI Systems must be relevant, accurate, and necessary for the intended purpose.

b. **Data Use:** When using AI Systems that rely on analysis of large amounts of data to provide insights, the Utilizing Agency is responsible for the quality and governance of the training data it selects to be used to support the AI System.

11. Fairness and Bias Mitigation

a. **Corrective and Preventative Actions:** Utilizing Agencies shall conduct and document regular reviews to ensure that their AI Systems are free from potential biases, with the Utilizing Agencies taking necessary corrective and preventative actions upon bias detection.

b. **Documentation:** Utilizing Agencies must document all processes and changes made to their algorithms and ensure diverse and representative training data.

12. AI System Security Reporting

a. **Awareness:** All employees, contractors, and relevant stakeholders should be made aware of the reporting process and its importance in ensuring the security of AI Systems. This can be achieved through regular training, email reminders, and onboarding sessions.

b. **Reporting Method:** Any concerns or potential violations may be sent directly to the DoIT Security team using the designated email: DoIT.Security@illinois.gov.

13. Compliance and Reporting

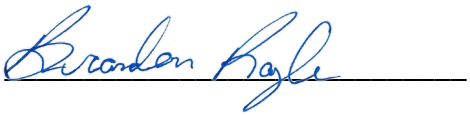
Non-compliance with these guidelines may result in exposure to risk and liability to the State. Concerns or potential violations related to AI Systems should be reported as outlined above.

Reports and notices required by this Policy should be submitted to the DoIT Security team at the email address listed in Section 14.

14. Contact Information

For questions or clarifications regarding this document, please contact DoIT Legal (DoIT.GeneralCounsel@illinois.gov) and DoIT Security (DoIT.Security@illinois.gov).

Approved and adopted by (Signature): On (Date):



3/31/2025

Brandon Ragle
Acting Secretary & State CIO
Illinois Department of Innovation and Technology

APPENDIX - AI System Security Reporting Process

Objective: To ensure a structured and prompt reporting mechanism for any concerns or potential violations related to AI applications, ensuring the security and integrity of AI Systems and data.

a. **Awareness:** All employees, contractors, and relevant stakeholders shall be made aware of the reporting process and its importance in ensuring the security of AI Systems. This can be achieved through regular training, email reminders, and onboarding sessions.

b. **Reporting Method:** Utilizing Agencies shall report any concerns or potential violations to the DoIT Security team using the designated email: DoIT.Security@illinois.gov. When submitting a report, the following information must be provided:

   i. **Personal Details:** Name, Position, Contact Information.

   ii. **Date and Time:** When the concern or potential violation was observed.

   iii. **Description:** A detailed account of the concern or potential incident. This includes the AI System's name, version, and specific functionalities in question.

   iv. **Evidence:** Any screenshots, logs, or relevant data that can support the report.

   v. **Impact Assessment:** A brief estimation of potential consequences or risks if applicable.

   Note: *If the violation is suspected to be malicious or involves sensitive information, ensure you provide just enough information to alert the team without exposing sensitive details over email.*

c. **Acknowledgment:** Upon receiving a report, the DoIT Security team will promptly acknowledge its receipt, ideally within 24 hours. This acknowledgment reassures the reporter that the concern is being addressed.

d. **Evaluation:** The DoIT Security team will evaluate the report to determine its severity, potential impact, and necessary actions. This may involve:

   i. Collaborating with the AI development or operations teams.

   ii. Consulting external AI security experts, if necessary.

   iii. Performing forensic investigations.

e. **Feedback Loop:** Once an evaluation is completed and necessary actions are taken, the DoIT Security team will provide feedback to the reporter. This feedback will cover the outcome of the evaluation and any measures taken in response.

f. **Remediation:** If a genuine security concern or violation is identified, the DoIT Security team will:

   i. Coordinate with relevant teams to fix the issue.

ii. Revise current AI security guidelines and policies, if needed.

iii. Conduct an incident review to identify lessons learned and to avoid similar issues in the future.

g. **Documentation:** Maintain a record of all reports, evaluations, actions taken, and outcomes. This not only ensures compliance and transparency but also helps in refining the AI security posture over time.

h. **Continuous Improvement:** Periodically review and refine the reporting process based on feedback and emerging AI security challenges. Ensure stakeholders are informed of any changes to the reporting process.

i. **Confidentiality:** All reports will be treated with utmost confidentiality. The identity of the reporter should be protected unless they give explicit consent for disclosure.

Timely use of this structured reporting process will create an environment where concerns related to AI Systems are tracked and swiftly addressed, ensuring the continued security and reliability of State systems.