NEW YORK STATE OF OPPORTUNITY. | Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

New York State Information Technology Policy	**No:** NYS-P24-001
IT Policy: **Acceptable Use of Artificial Intelligence Technologies**	**Updated:** 01/08/2024 **Issued By:** NYS Office of Information Technology Services **Owner:** Chief Data Office

1.0 Purpose and Benefits

The purpose of this policy is to establish guidelines for the acceptable use of Artificial Intelligence (AI) technologies, as defined here within, by State Entities (SE). Through the responsible use of AI, SEs can drive innovation, increase operational efficiencies, and better serve New Yorkers while protecting privacy, managing risk, and promoting accountability, safety, and equity. Agencies are encouraged to responsibly adopt AI technologies and should consider this policy a tool to aid in that adoption.

2.0 Authority

Section 103(10) of the State Technology Law provides the Office of Information Technology Services (ITS) with the authority to establish statewide technology policies, including technology and security standards. *Section 2 of Executive Order No. 117*[1], issued January 2002, provides the State Chief Information Officer with the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in NYS ITS Policy, *NYS-P08-002 Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines*.

[1] All references to Executive Order 117 refer to that which was originally issued by Governor George E. Pataki on January 28, 2002 and continued by Executive Order 5 issued by Governor Eliot Spitzer on January 1, 2007, Executive Order 9 issued by Governor David A. Patterson on June 18, 2008, Executive Order 2 issued by Governor Andrew M. Cuomo on January 1, 2011 and Executive Order 6 issued by Governor Kathy Hochul on October 8, 2021.

3.0 Scope

3.1 Agencies

This policy applies to "State Entities" defined as "State Government" in Executive Order 117[1] or "State Agencies" as defined in Section 101 of the State Technology Law. This includes employees and all third parties (such as local governments, consultants, vendors, and contractors) that use or access any Information Technology (IT) Resource for which the SE or ITS has administrative responsibility, including systems managed or hosted by third parties on behalf of the SE or ITS. While an SE may adopt a different policy, it must include the requirements set forth in this one. Where a conflict exists between this policy and an SE's policy, the more restrictive policy will take precedence.

Non-SEs, including authorities, boards, and other New York State governmental organizations are strongly encouraged to adopt this policy or use this policy for guidance or as a model.

3.2 Definitions and Covered Use

This policy applies to all technology systems that deploy AI technology, hereafter referred to as "AI systems." For the purposes of this policy, AI is defined as a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.

The definition includes but is not limited to systems that use machine learning, large language model, natural language processing, and computer vision technologies, including generative AI.[2] The definition does not include basic calculations, basic automation, or pre-recorded "if this then that (IFTT)" response systems.

This policy applies to all new and existing AI systems that are developed, used or procured by SEs, that when used could directly impact the public.[3]

The policy does not govern SE's regulatory or other actions regarding non-agency uses of AI.

[2] Detailed definitions can be found in the "Definitions of Key Terms" section of this Policy.

3 "Directly impact the public" can be reasonably determined by the SE, in consultation with ITS, when the use of an AI system would control or meaningfully influence the outcome of activities that, for example, impact the safety or rights of the public. Examples of such activities include but are not limited to assessments or decisions about individuals including in law enforcement, housing, hiring and employment, financial, educational, or healthcare contexts, decisions regarding access to or eligibility for government benefits or about child welfare, or the functioning of emergency services or critical infrastructure.

4.0 Information Statement

4.1 Use of AI

The SE may use AI systems to further their mission and meet critical business needs. The use of AI, even if not subject to this policy, must be in compliance with applicable New York State and ITS policies and standards and New York and federal law. Particular attention should be made to the use of Open-Source AI to ensure compliance with ITS-P19-005: Acceptable Use of Open Source Software, where applicable. Additionally, SEs must maintain awareness of how the AI system uses personally identifiable, confidential, or sensitive information to ensure such use complies with applicable laws, rules, regulations, notices, and policies. SEs are required to have SE leadership approval prior to adopting new AI systems. Such approval should include SE executive legal and operational leadership, including the SE's ethics officer.[4]

The SE must identify an Information Owner for each AI system that meets the criteria set forth in Section 3.2. For examples of acceptable and unacceptable uses of AI systems, please see Appendix A to this policy.

4.2 Human Oversight

AI systems aid and enhance human decision making that may impact the public. SEs must ensure that decisions that impact the public are not made without oversight by appropriate staff, who make the final decisions. Automated final decision systems are not permitted.

SEs shall take steps to ensure that where AI systems are used to aid in decision making that impacts the public, the outcomes, decisions, and supporting methodologies of such AI systems are documented appropriately.[5] The Information Owner is responsible for periodically assessing the outputs of their in-production AI systems to validate continuing reliability, safety, and fairness.

4.3 Fairness and Equity, and Explain Ability

Use of AI systems should be fair and equitable in accordance with applicable State and Federal laws, rules, and regulations. Systemic, computational, and human biases should be identified and remediated.

All AI systems should be explainable to the maximum extent practicable.

4.4 Transparency

Transparency is an important principle of AI governance. Where members of the public interact directly with SE systems that use AI technology, the use of such AI technology should be disclosed by the SE.[6]

---

4 For more information on this topic, please consult the National Institute of Standards and Technology (NIST) AI Risk Management Framework (RMF), available at https://www.nist.gov/itl/ai-risk-management-framework.
5 For more information, please consult the NIST AI RMF.
6 For example, if an SE is using an AI-enabled chatbot to answer questions from members of the public, the user should be made aware that they are interacting with a machine rather than with a human.

4.5 AI Risk Assessment and Management

The SE must perform a Risk Assessment for each AI system that meets the criteria set forth in Section 3.2. The Risk Assessment should include a review of all security, privacy, legal, reputational, and competency risks as well as the additional risks listed in this policy. SEs should adopt applicable elements of the current version of the National Institute of Standards and Technology (NIST) AI 100-1 Artificial Intelligence Risk Management Framework (RMF) and accompanying NIST Artificial Intelligence Risk Management Framework Playbook to address and meet the characteristics of trustworthy AI.[7]

In addition to the use of the NIST AI 100-1 AI RMF and Playbook, SEs must perform the Risk Assessment following the requirements set forth in NYS-S14-001: Information Security Risk Management. SEs should also refer to the NYS-S14-002: Information Classification Standard for guidance on how to rate risks for an AI Risk Assessment.

4.6 AI Inventory

ITS shall create and maintain an inventory that identifies AI systems in use and in scope under this policy.

ITS shall make such an inventory publicly available to the extent practicable and will separately issue guidance to SEs on the manner and composition of information to be furnished to ITS under this section. SEs will submit new and existing AI systems that meet the requirements of the guidance within 180 days of the issuance of the guidance.

4.7 Privacy

SEs should develop polices and controls to ensure the appropriate use of AI systems, particularly when the SE identifies a need to use the AI system to process personally identifiable, confidential, or sensitive information. Examples may include:

- A privacy impact assessment;
- Privacy-oriented settings, including data minimization, such as only processing data that is necessary during the development and use the AI system;
- Data retention settings that follow the requirements of federal and state standards;
- Ensuring the accuracy of data put into the AI system and the AI system's outputs;
- Disposal of the data once the purpose of using the data has been fulfilled, when possible, in compliance with applicable state and federal laws;
- Providing data subjects with control and transparency in relation to data processing.

7 Characteristics of trustworthy AI systems are that they are valid and reliable, safe, secure, resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair with harmful bias managed. For more information, please consult the NIST AI RMF.

4.8 Security

AI systems must comply with NYS-P03-002: Information Security Policy, NYS-P14-001 Acceptable Use of Information Technology Resources, and all associated standards which can be found at https://its.ny.gov/policies. Any additional controls required by applicable Federal or State law, rule, or regulation (e.g., IRS Publication 1075) must also be incorporated. AI systems must be developed and reviewed in alignment with NYS-S13-001: Secure Systems Development Lifecycle. In addition, SEs should ensure there are adequate security controls including encryption and pseudonymization, where appropriate depending on the risk throughout the data lifecycle.

4.9 Technology

The commercial and open-source landscape of AI is rapidly evolving, and SEs should take steps to periodically ensure that their AI systems continue to meet their business requirements in light of this. Open standards, model lifecycle management, and regular retraining of AI systems are all important elements that SEs should consider.

ITS supported agencies must submit an engineering consultation request through ITS's Information Technology Service Management (ITSM) system and abide by the NYS-P08-001: Plan to Procure when considering AI systems.

4.10 Intellectual Property

The legal landscape regarding intellectual property protections of AI systems and their outputs is evolving. SEs should confer with their counsel's office regarding the intellectual property implications of using AI systems, including for example, using copyrighted materials as inputs into an AI system or the extent to which a work created by an AI system may contain copyrighted elements.[8]

5.0 Compliance

This policy shall take effect upon publication. Compliance is required with all enterprise policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is required.

If compliance with this policy is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, SEs must request an exception from ITS.

6.0 Definitions of Key Terms

Except for terms defined in this policy, all terms shall have the meanings found in http://www.its.ny.gov/glossary.

8 For additional guidance see generally: https://www.federalregister.gov/documents/2023/03/16/2023-05321/copyright-registration-guidance-works-containing-material-generated-by-artificial-intelligence

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Chief Data Office
Reference: NYS-P24-001
NYS Office of Information Technology Services
State Capitol, ESP, P.O. Box 2062
Albany, NY 12220
Email: cdo@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website: https://its.ny.gov/policies

8.0 Revision History

This policy document should be reviewed consistent with the requirements set forth in NYS-P08-002 Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines.

Date	Description of Change	Reviewer
01/08/2024	Issued policy	Chief Data Office

9.0 Related Documents

Appendix A – Acceptable and Unacceptable use of AI Examples

All use of AI must comply with State policies, standards, procedures, and guidelines, as well as Executive Orders, any applicable license agreements, and Federal and State, laws, rules, and regulations, ITS technical standards and policies *(see* NYS-S23-001: Establishing Technology Solutions & Standards*)*, as well as the principles in this policy.

Below are illustrative examples of acceptable and unacceptable use of AI. This is not a comprehensive list of all potential AI use.

Situation	Acceptable sample use of AI	Unacceptable sample use of AI
Machine Learning	Using AI systems to provide insights in support of human decision making. Using a secured and well tested AI system to automate processes with periodic auditing.	Letting AI make decisions, without thorough testing to confirm accuracy and without review by human. Inputting personally identifiable, confidential, or sensitive information into an AI system where that AI system uses that information to build upon its model and/or may disclose that information to an unauthorized recipient.
Content generation (e.g., text, image, code, etc.)	Secured use of approved and vetted data with content suggestions reviewed and approved by human users. Generating code with AI for developers to review and test before use.	Use of non-vetted data to generate content without human review and without disclosure. Use of AI to generate content with the intent to deceive users.
Risk, pattern, outlier identification (e.g., Fraud Prevention and Detection)	Use of AI to detect any potential risks, patterns, or outliers, then informing human users for action. Using AI to detect anomalies in data and/or systems and create system alerts and take	AI system automatically takes actions that impact the public without human oversight.

Situation	Acceptable sample use of AI	Unacceptable sample use of AI
	automated actions to ensure system security.	
Natural Language Processing (NLP) (e.g., AI-empowered Chatbot, mobile device assistance, automatic translation etc.)	Using automatic speech recognition with outputs clearly labelled as AI-generated accordingly. Using AI-empowered automatic translation for reasonable accommodation needs.	Using an AI-powered chatbot that is not identified as such and that intentionally deceives users.