State of North Carolina

North Carolina State Government Responsible Use of Artificial Intelligence Framework

August 2025

Table of Contents

Document Information

Department Name	N.C. Department of Information Technology
Owner	Secretary and State Chief Information Officer
Title	North Carolina State Government Responsible Use of Artificial Intelligence Framework
Publication Date	Aug. 21, 2025
Version	1.1

Date	Version	New or Revised Requirement	Description	Author
August 2024	1.0	New	Policy Creation	Privacy Office
August 2025	1.1	Revised	Amended Appendix B - Removed Govern, Map, Measure, Manage - Provided a link to NIST AI RMF Core Updated AI and GenAI definitions to match state approved definitions	Policy Office

Framework

Introduction

Artificial intelligence (AI) is a broad term used to describe an engineered system where machines learn from experience, adjusting to new inputs, and potentially performing tasks previously done by humans. More specifically, it is a field of computer science dedicated to simulating intelligent behavior in computers. It may include automated decision-making (International Association of Privacy Professionals, Glossary, https://iapp.org/resources/glossary, 2024).[1]

The state has leveraged certain AI technologies when building out its analytic capabilities to support improved insights. These technologies have the potential to transform society, drive economic growth, support scientific advancement, and help government serve people more effectively and efficiently. They also pose risks that can negatively impact people, organizations, and society.

The State Chief Information Officer supports the use of AI, where appropriate, to improve government innovation, operations, and services in a manner that benefits the people, fosters public trust, builds confidence in AI, protects our state's values, and remains consistent with all applicable laws.

Opportunities for designing, developing, acquiring, and using AI should be sought to improve state government while carefully considering potential risks and how they could best be assessed and managed.

Purpose

The North Carolina State Government Responsible Use of Artificial Intelligence Framework (AI Framework) is designed to encourage responsible exploration and use of AI to benefit the people of North Carolina, foster public trust and confidence in the use of AI, protect our state's values, and ensure that the use of AI remains consistent with all applicable laws, including those related to privacy, civil rights, and civil liberties.

The AI Framework consists of principles, practices, and guidance to agencies who are trying to reap the benefits of AI while reducing privacy and data protection risks when using specific types of artificial intelligence (AI) and supporting the privacy and protection of sensitive data provided to the state by North Carolinians.

Policy

State agencies must follow the common set of principles outlined in the AI Framework when considering the design, development, acquisition, and use of AI in government. The AI Framework is based on principles for AI that build on the Fair Information Practice Principles adopted by the state in May 2022, as well as privacy and security best practices for the use of AI.[2]

---

[1] IAPP's definition provides a high-level summary of AI definitions found in NIST's *The Language of Trustworthy AI: An In-Depth Glossary of Terms (*March 22, 2023).

[2] AI Framework principles are informed by the White House, Office of Science Technology and Policy, Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People, n.d., https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

Scope and Authority

This framework applies to the use of all AI by State Agencies. State Agencies shall have the same meaning as provided in N.C.G.S. § 143B-1320(a)(17).

The AI Framework applies to all systems that use, or have the potential to use, AI and have the potential to impact North Carolinians' exercise of rights, opportunities, or access to critical resources or services administered by or accessed through the state. This includes all AI designed, developed, acquired, or used by state agencies, unless specifically excluded by applicable law.

The AI Framework applies to both existing and new uses of AI; both stand-alone AI and AI embedded within other systems or applications; AI developed both by the agency or by third parties on behalf of agencies for the fulfilment of specific agency missions, including relevant data inputs used to train AI and outputs used in support of decision making; and agencies' procurement of AI systems or applications.

The AI Framework does not apply to basic AI embedded within common commercial products, such as predictive text in word processors or dynamic route adjustment based on real-time traffic conditions in map navigation systems, while noting that government use of such products must nevertheless comply with applicable law and policy to assure the protection of security, privacy, rights, and state values.

Pursuant to N.C.G.S. § 143B-1376 - Statewide Security and Privacy Standards, the State Chief Information Officer (CIO) is responsible for the security and privacy of all state information technology systems and associated data. The State CIO manages all executive branch information technology security and shall establish a statewide standard for information technology security and privacy to maximize the functionality, security and interoperability of the state's distributed information technology assets, including, but not limited to, data classification and management, communications and encryption technologies.

Nothing in this framework shall be construed to impair or otherwise affect: (i) the authority granted by law to a department or agency, or the head thereof; or (ii) the functions of an agency relating to budgetary, administrative, or legislative proposals. This framework should be implemented consistent with applicable law and subject to the availability of appropriations. It is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the State of North Carolina, its agencies, or entities, its officers, employees, or agents, or any other person.

Principles and Practices

State government should use AI to support operations to benefit North Carolinians and the public good. Agencies should consider AI in instances where it can help further the agency's mission, enhance service delivery, and improve efficiency and effectiveness. The overarching goal for state government in exploring and using technology, including technology that includes AI, should always be to benefit the people of North Carolina.

These seven principles and associated practices form a blueprint of ethical behavior to guide the state in using AI responsibly to harness its benefits to serve the public while minimizing potential harm. Agencies need to ensure that their AI applications are regularly tested against these principles.

Mechanisms should be maintained to modify, supersede, disengage, or deactivate existing applications of AI that demonstrate performance or outcomes that are inconsistent with their intended use or these principles.

The principles and associated practices are:

1. **Human-centered:** Human oversight is required for all development, deployment, and use of AI. The state should use AI to benefit North Carolinians and the public good. Human oversight should ensure that the use of AI does not negatively impact North Carolinians' exercise of rights, opportunities, or access to critical resources or services administered by or accessed through the state.

2. **Transparency and Explainability:** When AI is used by the state, the user agency shall provide notice to those who may be impacted by its use. This notice should identify the use of an automated system, explain why it is used, and how this use contributes to outcomes that impact individuals. This notice should be accessible and written in plain language. Notice should include clear descriptions of the data, the role automation plays in decision-making, and the ability to trace the cause of possible errors.

3. **Security and Resiliency:** Systems utilizing AI must undergo pre-deployment testing, risk identification and mitigation, and ongoing monitoring that demonstrates the systems are safe and effective, in keeping with standards for security review for all technology implemented within state government. Systems need to be assessed for resilience to attack, adherence to security standards, and alignment with general safety, accuracy, reliability, and reproducibility.

4. **Data Privacy and Governance:** Any use of AI by the state must maintain the state's respect for individuals' privacy and its adoption of the Fair Information Practice Principles throughout the AI lifecycle (development, testing, deployment, decommissioning). This means that privacy is embedded into the design and architecture of IT and business practices. Preservation of privacy should be the default and access to data should be appropriately controlled. Individuals developing or deploying AI systems should be conscious of the quality and integrity of data used by those systems.

5. **Diversity, Non-discrimination, and Fairness:** AI should be developed with consultation from diverse communities, stakeholders, and domain experts to identify concerns, risks, biases, and potential impacts of the system. AI needs to be developed to be equitable and control for biases that could lead to discriminatory results. AI systems should be user centric and accessible to all people.

6. **Auditing and Accountability:** Users of AI must be accountable for implementing and enforcing appropriate safeguards for the proper use and functioning of their applications of AI, and shall monitor, audit, and document compliance with those safeguards. Agencies shall provide appropriate training to all agency personnel responsible for the design, development, acquisition, and use of AI.

7. **Workforce Empowerment:** Staff are empowered in their roles through training, guidance, collaborations, and opportunities that promote innovation that aligns with state or agency missions and goals. This can help state government make best use of AI tools to reduce administrative burdens on staff where feasible and improve overall public service.

Requirements

To properly identify and assess opportunities and risks related to AI, the state must have a comprehensive inventory of AI tools and follow a common framework for risk assessment.

AI Inventory

Agencies must keep an inventory of the tools or applications using AI (including the types of AI) being used, by whom, and for what purposes.[3]

Agencies' inventories should be reported to the North Carolina Department of Information Technology for transparency and updated, at a minimum, through the annual application portfolio management process. Decisions about AI use should include considerations of continuity.

AI Risk Assessment

Agencies must use the NIST AI Risk Management Framework (AI RMF) to assess and manage risk to individuals, organizations, and society associated with AI before deployment and on a continuing basis once AI is deployed.

The NIST AI RMF was developed in collaboration with the private and public sectors and is an essential tool in improving the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems.

The Enterprise Security and Risk Management Office (ESRMO) and the Office of Privacy and Data Protection (OPDP) will provide guidance concerning risk assessments for AI in enterprise-level platforms, services, and applications. AI risk needs to be assessed and documented.[4]

[3] The use of an AI inventory aligns with Executive Order 13960 Promoting the Use of Trustworthy AI in the Federal Government establishes principles for the use of AI in the Federal Government, which establishes a common policy for implementing the principles and directs agencies to catalogue their AI use cases.
[4] A Privacy Threshold Analysis (PTA) is the initial tool used by the state to identify and document risk.

Appendix A – Glossary

Algorithm: A set of computational rules to be followed to solve a mathematical problem. More recently, the term has been adopted to refer to a process to be followed, often by a computer (NIST Glossary of AI Terms, March 2023).

Artificial Intelligence (AI): A machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments. *(European Union AI Act,* June 2024)

AI Prompt: An instruction or command given to an artificial intelligence tool to carry out a task or function.

Confidential Information: Refers to all information about the organization, its operations, clients, or employees that is subject to reasonable efforts by the organization to maintain its confidentiality and that is not typically disclosed by custom or law to people who are not affiliated with the organization but does not qualify as a trade secret.

Generative AI: The class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content. This can include images, videos, audio, text and other digital content. (*NIST Special Publication 800-218A*, July 2024)

Hallucination: Generated content that is nonsensical or unfaithful to the provided source content (*NIST Glossary of AI Terms,* March 2023).

Machine Learning: The study or the application of computer algorithms that improve automatically through experience. Machine learning algorithms build a model based on training data in order to perform a specific task, like aiding in prediction or decision-making processes, without necessarily being explicitly programmed to do so (*NIST Glossary of AI Terms*, March 2023).

Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity – such as name, Social Security number, biometric data records – either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).

Trustworthy AI: 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 (*NIST Glossary of AI Terms*, March 2023).

Appendix B – NIST AI Risk Management Framework

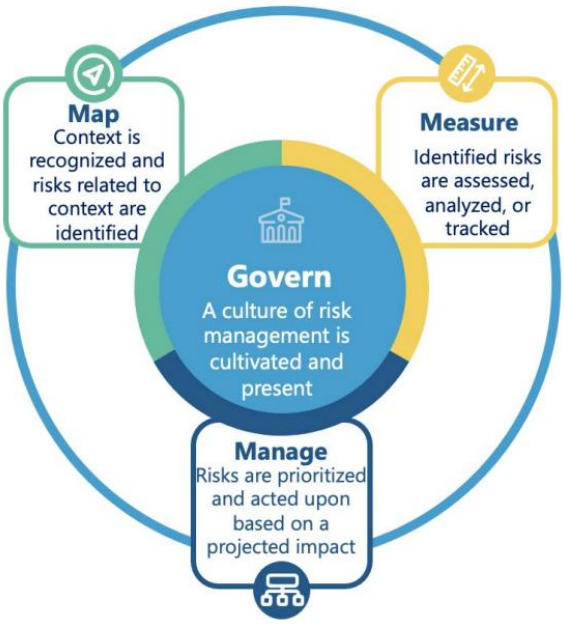
Risk management is central to responsible development and use of AI technologies.

> Responsible AI practices can help align the decisions about AI system design, development, and uses with intended aim and values.… 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 RMF 1.0, January 2023, Executive Summary, p.1)

The NIST AI RMF Core is reproduced below to serve as a starting point for AI risk assessment. NIST will continue to update this framework and provide additional guidance. Always consult NIST directly to ensure access to the most current version of the NIST AI RMF to guide risk assessment.

NIST AI RMF Core

The NIST AI RMF Core provides outcomes and actions that enable dialogue, understanding, and activities to manage AI risks. This is the foundation for Working Groups to create the processes to evaluate and mature AI use cases. The graphic below provides a visual understanding of what is involved in AI risk management.



NIST AI RMF 1.0, January 2023, Part 2: Core and Profiles, 5. AI RMF Core, https://doi.org/10.6028/NIST.AI.100-1.

Appendix C – Further Reading

Advanced Technology Academic Research Center, From Ethics to Operations: Current Federal AI Policy, January 5, 2022, https://atarc.org/wp-content/uploads/2022/01/Current-Federal-AI-Policy-Assessment-FINAL.pdf.

City of San Jose, Government AI Coalition, accessed March 17, 2024, https://www.sanjoseca.gov/your-government/departments-offices/information-technology/ai-reviews-algorithm-register/govai-coalition.

Congressional Research Service, Artificial Intelligence: Overview, Recent Advances, and Considerations for the 118th Congress, August 4, 2023, https://crsreports.congress.gov/product/pdf/R/R47644.

Daniel Atherton, Reva Schwartz, Peter C. Fontana, Patrick Hall, The Language of Trustworthy AI: An In-Depth Glossary of Terms, March 2023, (National Institute of Standards and Technology, Gaithersburg, MD), NIST. Artificial Intelligence AI 100-3. https://doi.org/10.6028/NIST.AI.100-3.

European Union Artificial Intelligence Act, June 13, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

Executive Order 13960, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government.

Ezzell, Amber, Future of Privacy Forum Generative AI for Organizational Use: Internal Policy Checklist, July 2023, https://fpf.org/wp-content/uploads/2023/07/Generative-AI-Checklist.pdf.

Fennessy, Caitlin, International Association of Privacy Professionals, Regulators' Rulebook for AI: Bit by Bit, August 2, 2023, https://iapp.org/news/a/regulators-rulebook-for-ai-bit-by-bit/.

GSA, AI Guide for Government: A Living and Evolving Guide to the Application of Artificial Intelligence for the U.S. Federal Government, December 3, 2020, https://coe.gsa.gov/coe/ai-guide-for-government/understanding-managing-ai-lifecycle/index.html.

International Association of Privacy Professionals, Global AI Legislation Tracker, August 25, 2023, https://iapp.org/media/pdf/resource_center/global_ai_legislation_tracker.pdf.

International Association of Privacy Professionals, Glossary, n.d., https://iapp.org/resources/glossary/.
Microsoft, Governing AI: A Blueprint for the Future, May 2023. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW14Gtw.

NIST, U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools, August 9, 2019, https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf.

NIST, AI Risk Management Framework – Resources, Launched March 2023, accessed March 17, 2024, https://www.nist.gov/itl/ai-risk-management-framework/ai-risk-management-framework-resources.

NIST, Special Publication 800-218A, Secure Software Development Practices for Generative AI and Dual-Use Foundation Models, July 2024, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218A.pdf

NIST, Trustworthy and Responsible AI Resource Center, Glossary, March 2023, https://airc.nist.gov/AI_RMF_Knowledge_Base/Glossary.

North Carolina Department of Information Technology Enterprise Security and Risk Management Office, Statewide Information Security Manual, January, 2022, https://it.nc.gov/documents/statewide-policies/statewide-information-security-manual/download?attachment

State Archives of North Carolina, Functional Schedule for North Carolina State Agencies Glossary, n.d., https://archives.ncdcr.gov/functional-glossary-key/download?attachment.

White House, Office of Science Technology and Policy, Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People, n.d., https://www.whitehouse.gov/ostp/ai-bill-of-rights/.