Policy Title

Artificial Intelligence Policy

Synopsis

Ensure the legal and ethical use of Artificial Intelligence tools and technology.

Authority

Title 29 Chapter 90C Delaware Code, §9004C – General Powers, duties, and functions of DTI "2) Create, implement and enforce statewide and agency technology solutions, policies, standards and guidelines, including as recommended by the CIO"

Applicability

This policy is applicable to all users of the State of Delaware communications and computing resources. The Department of Technology and Information (DTI) is an Executive Branch Agency and has no authority over the customers in Legislative and Judicial Branches, as well as Local Education Agencies, and other Federal and Local Government entities that use these resources. However, all users, including these entities, must agree to abide by all policies and standards promulgated by DTI as a condition of access and continued use of these resources.

Effective Date

7/3/2025 (revised 10/30/2026)

Reviewed Date

11/3/2026

Expiration Date

None

POC For Changes

Chief Technology Officer

Approval By

State Chief Information Officer

Document Type

External Policy

Document Reference Number

OT-AI-001

Revision Number

1

Organization

State of Delaware, Department of Technology and Information, 801 Silver Lake Blvd., Dover, Delaware 19904, DTI.Delaware.gov, 302-739-9500

TABLE OF CONTENTS

TABLE OF CONTENTS 2
EXECUTIVE SUMMARY 3
DEFINITIONS 4
GENERAL POLICY STATEMENT 5
DEVELOPMENT AND REVISION HISTORY 10
APPROVAL SIGNATURE BLOCK 10
LISTING OF APPENDICES 10
RELATED POLICIES AND STANDARDS 10

EXECUTIVE SUMMARY

1. Artificial Intelligence ("AI") is a broad class of technology that allows computers and digital devices to learn, grow, analyze, and create. AI is rapidly becoming an increasingly essential function of day-to-day operations within the State Enterprise. Types of AI such as Generative Artificial Intelligence ("GenAI") refers to a specific subset of AI. GenAI is an AI technology that synthesizes new versions of text, audio, or visual imagery from large bodies of data in response to user prompts. GenAI models can be used in stand-alone applications or incorporated into other applications such as internet search engines or word processing applications. The following table shows categories of AI features, common capabilities, and examples (many of which are commonly used by many State of Delaware staff and constituents):

Feature Category	Core Capability	Common Real-World Applications
Natural Language Processing (NLP)	• Text Generation • Text Summarization • Language Translation • Sentiment Analysis	• Gathers information from public sources • Drafts emails, reports, or articles • Automatically translates complex documents • Analyzes feedback to detect mood/satisfaction • AI notetaking and transcription
Generative Media	• Image & Video Synthesis • Voice & Audio Generation	• Creates graphics, logos, and user interface design • Generates synthetic voiceovers and video content
Computer Vision	• Object Detection • Facial Recognition • Optical Character Recognition	• Powers self-driving vehicle navigation • Secures biometric authentication systems • Extracts editable text from scanned PDFs/photos.
Data Analytics & Prediction	• Predictive Modeling • Pattern Recognition • Recommendation Engines	• Forecasts system demands or predicts requests • Identifies fraudulent transactions in real-time • Personalizes feeds on Netflix, YouTube, or Spotify
Automation & Workflow	• Task Automation • Robotic Process Automation • Virtual Assistance • Cybersecurity response	• Auto-fills spreadsheets and databases • Syncs calendar invites and schedules meetings • Filters spam and blocks malware • Powers support chatbots for 24/7 support
Coding & Development	• Code Generation • Debugging & Code Explanation	• Writes functional code blocks in Python, SQL, etc. • Scans code for security vulnerabilities • Determines software defects

2. Artificial Intelligence has become embedded into mainstream technologies such that it has become almost impossible to separate information technology (and often operational technology) from artificial intelligence. For example, every time you use mapping products to reach a destination or use facial recognition to unlock your smartphone, you are using artificial intelligence. Commonly used functions like suggested movies on streaming services, suggested email addresses and proposed text are also engaging artificial intelligence. Smartwatches on your person and smart devices in your house are using AI. Our systems that control heating and cooling in buildings, temperature settings in our home appliances, and safety systems in facilities may include AI. Artificial intelligence is all around us and often usefully applied to make our lives easier, safer, and more informed. AI that is embedded in consumer devices and features in commercially available software is out of scope for this policy and not subject to the review and governance requirements. However, the state government use of all AI capabilities (consumer, commercial, or custom built) is subject to the ethical and responsible requirements of this policy. Prohibited uses of AI apply to all AI uses.

3. AI offers many benefits however, like all technology, it can be misused and exploited. As AI advances, there are concerns that should be considered. In 2026, the attorney generals in 23 states (including Delaware) called for federal oversight of AI model safety testing, international cooperation to pace AI advancement and leaders empowered to make safer decisions "unburdened by profit maximization". There is also the concern that some AI-generated content is inaccurate, misleading, hallucinated, or of poor quality (often referred to as "AI Slop"). This policy shall evolve and AI use cases should be frequently reviewed against this policy to stay current.
4. AI must be used responsibly. This means using the:
   4.1. Right technology: use approved AI tools and technologies that have been assessed, deemed secure and private, funded (no freeware), and can be sustained (reliable firms and technologies).
   4.2. Right way: use the correct AI tool for the proper function. Functions include machine learning, predictive AI, generative AI, chatbots, image recognition, and agentic AI.
   4.3. Right goals and outcomes: usage of AI should be ethical, legal, secure, dependable, sustainable, and cost effective.
5. This policy establishes a risk-based framework to categorize AI systems, ensuring that oversight and controls are proportional to the potential risks and impacts on Delawareans.
6. This policy has several goals:
   6.1. Provide guidance and information as a framework to consider when a user is contemplating using AI for a State function and/or with State data.
   6.2. Outline the specific rules and permissible uses for AI testing, development, and deployment.
   6.3. Explain the guardrails for AI usage, which will protect State employees, data, and the constituents of the State.
7. State of Delaware organizations outside of the executive branch are encouraged to reference this policy and either adopt or adapt it to their own organizational environments.

DEFINITIONS

Artificial Intelligence (AI) – A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.

AI System Inventory – A comprehensive, regularly updated catalog of all AI systems procured, developed, or used by State agencies, documenting their purpose, data sources, risk level, and vendor.

Algorithmic Impact Assessment (AIA) – A formal study conducted prior to the deployment of a high-risk AI system to evaluate its potential effects on fairness, equity, privacy, and safety, and to identify mitigation strategies for potential harms.

Foundation Model – A model comprised of massive amounts of diverse data that can serve as the foundation of other specialized models.

Generative Artificial Intelligence (GenAI) – The class of AI models that emulate the structure and characteristics of input data to generate derived synthetic content. This can include images, videos, audio, text, and other digital content. Though AI has been around for a long time, generative AI is relatively new and made AI more consumer oriented, relevant, and helpful. Generative AI is not conscious, it does not "know" facts the way humans do, and it lacks common sense or public service ethics. It makes suggestions based on patterns found in the data used to "train" it (called the large language model or LLM). Generative AI is like a highly advanced, incredibly fast autocomplete tool. It looks for patterns in massive amounts of data to predict and generate text, summaries, or ideas.

High-Risk AI System – An AI system that has the potential to cause significant adverse legal, economic, or material effects on an individual's rights, safety, or access to essential services. DTI shall maintain a list of presumptive high-risk AI use cases, including but not limited to, those involving law enforcement, justice systems, public benefits eligibility, employment screening, and clinical diagnoses.

Large Language Model (LLM) – Advanced artificial intelligence systems designed to understand and produce human language through the processing of extensive textual data. They utilize deep learning algorithms, typically employing neural network architectures, to accomplish tasks such as language translation, text generation, and question answering. These models are trained on large datasets to achieve proficiency in comprehending and generating natural language.

Public AI – tools generally available to all users which can exist in both a paid and free format. Most general individual consumer GenAI products fall within this category. They do not usually require a subscription to another platform to access them. Public GenAI tools utilize commercially developed algorithms, publicly available data, and limited or no customizations for enterprises. A list of examples is available here.

Enterprise AI: tools that are organization-centric and are associated with a subscription to, or purchase of, a commercial product or service offering. This might include stand-alone AI products or AI functionality integrated into existing software and platforms. These tools may require an additional monthly cost. It is expected that any product falling into this category will be procured with a legal agreement that contains terms which protect State data and disallow unrestricted data sharing. Information that the tool processes, new knowledge it generates, and decisions it makes remain local to the State of Delaware's service environment. A list of examples is available here.

GENERAL POLICY STATEMENT

AI shall be responsibly used by State of Delaware employees, contractors, and vendors that handle State of Delaware data such that it is ethical, secure, and sustainable.

ETHICAL

1. The State of Delaware promotes the responsible use of AI tools for appropriate purposes and with minimal risks to the State. Any use of AI, via platforms, tools, and software, must be consistent with this policy and related policies like the Acceptable Use Policy and the standards set forth in Title 29, Chapter 58 of the Delaware Code.
    - Use of AI on State devices must be limited to State purposes.
    - Use of AI tools on personal devices or personal accounts to circumvent State policies or safeguards is strictly prohibited. If a user accesses AI on a personal device or through a personal account for State business, this policy still applies.
    - State users should act responsibly when using AI. State users should independently verify all AI outputs to avoid promoting false data via hallucinations, biased results, or other problematic outcomes.
    - Content, such as text, audio, images, or video, generated exclusively by using GenAI must be clearly identified on any internal or outward-facing communication. This disclosure must be clear and conspicuous to the intended audience. For public-facing chatbots, an initial disclosure stating the user is interacting with an AI is required.
    - AI systems shall be accessible and compliant with DTI standards.

2. Results created by GenAI are not above questioning or reproach. GenAI works from foundation models and large language models, which are not "truth" models. Some GenAI tools may be trained on data or present data that is inherently biased or inaccurate and, therefore, untrustworthy. Also, some AI tools have documented histories of presenting users with fabricated content, referred to as "hallucinations." Unknowingly relying on a hallucination may create significant liability for the State and be legally actionable.

User training is a critical way to minimize some of the risks associated with AI and all users of AI should complete the Delaware-required AI training. Prior to use and publication, all AI results shall be reviewed by a human operator (Human in the Loop).

3. AI notetakers and AI transcription is a common AI use case however; AI can often make mistakes on interpretation and attribution. This is a concern as AI-created notes and transcripts are records and subject to the Freedom of Information Act (FOIA). Records (including records produced with AI) must be created and stored in state-approved tools and repositories. Official records generated with the assistance of AI must be thoroughly reviewed, edited, and approved by a human operator.

4. Any content created by AI notetakers and AI transcription should be clearly labeled as AI-generated content for example, "This document has been created with artificial intelligence and can be inaccurate and/or incorrect."

5. AI can assist users with content creation, but a human expert should review, edit, and approve every single output before it is used or published (human in the loop). AI lacks context and doesn't understand agency culture, local political sensitivities, or the nuances of specific constituent needs. Users are the editor, the gatekeeper, and the ethical compass. The final product (whether a presentation or an email) comes from the user and the user is always accountable.

6. All AI outputs should be fact checked by reviewing the links provided to verify that the content came from reliable sources, is trustworthy and is correctly presented. AI can be confidently and seemingly authoritatively biased and incorrect. Because AI learns from historical internet data, it can inadvertently repeat or amplify societal biases that may exist in the LLM used for training.

7. AI shall not be used for the following explicit uses which may violate Delaware's acceptable use policy:
   - **High-Risk Autonomous Decision-Making:** Using AI for fully automated decisions without human oversight in life-altering domains (e.g., automatic diagnoses; approving state services such as permits, licenses, or benefits; or auto-filtering or rejecting job applicants). All high-risk decisions made with the assistance of AI must include a clear and accessible process for a human review and appeal by the affected individual.
   - **Malicious Cyber Operations:** Writing malware, discovering software vulnerabilities for exploitation, generating phishing/spear-phishing emails, or automating cyberattacks.
   - **Disinformation & Impersonation:** Generating synthetic deepfakes, propaganda, or deceptive media intended to deceive readers, execute identity theft, or impersonate real individuals without consent.
   - **Unregulated Professional Advice:** Offering binding legal, financial, or medical guidance without qualified human review or professional licensing.
   - **Generation of Harmful Content:** Producing content contrary to Delaware's acceptable use policy, promoting self-harm or suicide, facilitating hate speech, creating biases towards any protected class, or providing actionable guides for constructing weapons or dangerous substances.
   - **Plagiarism & Intellectual Property Violations:** Generating content designed to evade detection systems for copyright infringement or academic dishonesty.

SECURE

8. Information is shared with an AI tool by user prompts, uploaded inputs, or a series of instructions or questions for the tool. Generally, providing access to information constitutes sharing data with the tool. The sharing of data potentially makes confidential or sensitive information public, as the tool may use data shared to further develop its knowledge base. In some cases, data that has been sanitized could be linked to personal information and become exposed. Any customer or employee personal information, State proprietary information or intellectual property, or otherwise confidential or sensitive information entered into a GenAI

tool may appear to an unrelated non-State user. Therefore, users of GenAI must avoid entering any information into a GenAI tool which they do not want to be made public or is otherwise restricted by law or policy.

9. Improper AI use can present significant threats to State cybersecurity. Like with any resource, risks can be reduced by deploying end user training to ensure safe use. State agencies are required to complete responsible AI training before granting a user permission to use AI. Similarly, users will be required to complete any AI training mandated by DTI before accessing the respective AI solutions on State systems. Using AI without proper training may result in a finding that the user has violated the DTI Acceptable Use Policy.

10. Use of information classified as Confidential or above with Enterprise AI tools must be explicitly approved by a division level approved and trained data steward of the implementing agency and documented in the approved business case. Without approval, AI use for confidential and above data classifications of State information is strictly prohibited.

11. Public AI models often use your inputs to train future versions, meaning your data could accidentally be exposed to others. If a piece of information is not suitable for a public billboard, do not type it into a commercial or public AI tool. Unless explicit Cabinet level approval is granted, only publicly available, test, or synthetic data should be used with AI systems.

12. Personal Identifiable Information (PII) of constituents, draft policies, internal memos, or sensitive security details should not be used with AI. In a healthcare setting, much of the data, especially patient or client data, is governed by HIPAA. This includes AI transcripts and AI notetakers. Unless the AI is explicitly approved for use by your agency, do not use it.

13. Users of Delaware AI tools (such as Google Gemini, OpenAI ChatGPT, Microsoft Copilot, or AWS Bedrock) shall enroll and subscribe to the Delaware AIDR (Artificial Intelligence Detection and Response) solution that applies statewide policies and detects/counters malicious AI agents and activities.

14. Enterprise AI must integrate with and use the State of Delaware's Identity and Access Management (IAM) Solution (ID.Delaware.GOV).

SUSTAINABLE

15. AI tools and technologies that are purchased or used should be from approved sources. The AI market is volatile and many products of today may not be around tomorrow. Technologies should not be used to create long term vendor dependency or lock in.

16. In situations where the AI is supporting critical functions or processes, ensure business continuity such as operations can occur if the AI falters or needs to be taken offline.

17. AI models vary in cost and efficiency. Use the most efficient model to support the AI task.

18. AI technology can be ethically sourced by environmentally conscious companies. Where possible, use AI technology that supports sustainable energy and other resources.

COMPLIANCE AND OVERSIGHT

19. For a State agency to implement or use Enterprise AI tools, it must pursue an approved business case through DTI. This business case must include a risk classification (e.g., low, moderate, high) and, for high-risk systems, a completed Algorithmic Impact Assessment. The following are the AI risk categories:

- **Low risk**: Informational in nature (such as a chat bot or enterprise AI tool like Gemini or ChatGPT to search the Internet or public large language models) using well-established and proven technologies on data that is public or open to the users that have access to the tool (such as an internal chat bot that helps an organization's users navigate internal documentation). Subject to agency-specific policies, public GenAI tools (such as OpenAI ChatGPT, Google Gemini, or Microsoft CoPilot) can be used for low-risk activities providing no state data is used or uploaded into those tools.

  Note: Any Public GenAI use with State data with classification of Confidential and above is strictly prohibited. Public GenAI tools and AI model source code should only be accessed or downloaded from reputable, known sources to avoid interacting with modified or malicious AI models.
- **Moderate risk**: AI tools that may change or delete data for productivity-related actions for areas that are deemed as low risk to the public and do not involve consequential or life-altering decision making. Examples could include using Microsoft Co-Pilot to draft emails, Gemini to draft graphics or create documents, or Claude to develop or debug software. Only approved enterprise AI tools should be used for moderate risk activities.
- **High risk**: Autonomous AI and/or AI tools that support decision making for life-altering domains (e.g., automatic diagnoses, approving state services such as permits, licenses, or benefits, or auto-rejecting job applicants).

  Note: Fully autonomous AI decision-making for life-altering domains is prohibited.

20. An Algorithmic Impact Assessment (AIA) is a structured, multi-disciplinary governance review used to evaluate the design, purpose, risks, and real-world effects of an AI or automated decision-making system before and during its deployment. The review of the AIA shall include DTI's analysis of purpose, scope, security configurations, access controls, integration with the State's identity solution, and encryption of State data at rest. State agencies should demonstrate a sustained funding model to maintain enterprise AI tools. The following are AIA tasks that must be completed in the business case for all high risk AI use cases prior to approval:

    - Define Scope & Context: Establish why the AI is being used and who is impacted
    - Analyze Data & Design: Evaluate inputs, bias, and technical security and safety
    - Identify Risks & Harm: Determine potential negative impacts on individuals, systems, and the agency and/or whole of state
    - Implement Mitigations: Address and lower high-impact risks associated with lifecycle management and deployment; include a means to immediate stop the AI if performance exceeds established parameters (aka, Killswitch).
    - Document & Monitor: Ensure traceability and continuous oversight (operational and security)

21. Before procuring or deploying any high-risk AI system or tool, agencies must submit the Algorithmic Impact Assessment to the AI Governance Committee for review (once prior to procurement and again prior to operational deployment). All contracts with AI vendors must include specific terms that address data ownership, privacy, security, indemnification against AI-generated errors, and requirements for the vendor to disclose training data sources and bias mitigation efforts.

22. Use of AI tools and models that are designed specifically for malicious purposes, or that originate from or are hosted outside of the United States and its territories, is strictly prohibited. If users are concerned about a specific tool's acceptability, they are encouraged to verify viability with their agency's Information Resources Manager or Information Security Officer.

23. DTI shall establish an inter-agency AI Governance Committee, composed of representatives from various executive and other branch agencies with expertise in technology, data privacy, education, law, and civil rights. A higher education representative will be included. The Committee will be responsible for advising the CIO, reviewing the AI System Inventory, reviewing Algorithmic Impact Assessments for high-risk systems, and recommending policy updates.

24. All State agencies must report their use of AI systems to DTI for inclusion in the statewide AI System Inventory. The inventory shall be reviewed and updated at least annually.

25. DTI reserves the right to access, monitor, and log the use of AI applications on any State-issued devices or on State managed networks to ensure compliant use of these systems. DTI reserves the right to terminate or suspend service immediately or to otherwise disconnect, remove, block, filter, or restrict an employee's use of service if DTI determines that such use violates this policy. If DTI believes that an employee has used an AI tool in an impermissible fashion, DTI may forward the relevant information, including the employee's identity, to that person's Information Security Officer.

26. If there is ambiguity or confusion regarding any part of this policy, notify the sponsor defined in the header of this policy. If you are unsure of the category of AI, or whether a product is in fact AI, please contact your Information Resource Manager (IRM) or Information Security Officer (ISO) to partner with the policy sponsor for classification.

27. Requirements for AI system developers either as state personnel or state-contracted vendors:
    - Quality Management System (QMS): Maintain procedures for compliance, design controls, and testing. The procedures shall explain the applied software development life cycle.
    - Code Management: Manage the AI-generated software code in the agency-approved code repository (such as the DTI software repository). Document how the code was generated, including prompts, in the documentation notes.
    - AI developed software code shall follow the SDLC (software development life cycle) process including development in an appropriate development (DEV) environment, testing in a test (TEST) environment, and promotion to productive use in a production (PROD) environment.
    - Continuously monitor real-world system behavior and immediately report serious safety or security incidents to supervisory authorities.
    - Bias and Fairness Testing: For AI systems that affect protected classes and demographics relevant to the State of Delaware, developers must test for and document potential biases in the AI model's outputs. Mitigation strategies must be documented and implemented before deployment.

DEVELOPMENT AND REVISION HISTORY

Date	Revision
7/3/2025	Rev 0 – Initial version
2/12/2026	Rev 0 – Applied an accessible format
11/3/2026	Rev 1 – Expanded from GenAI to all AI

APPROVAL SIGNATURE BLOCK

Robert Osmond

Digitally signed by Robert Osmond
Date: 2026.11.03 13:25:21 -05'00'

LISTING OF APPENDICES

NA

RELATED POLICIES AND STANDARDS

NA