

COMMONWEALTH OFFICE OF TECHNOLOGY		Page 1 of 6
Office of the Chief Information Officer Enterprise Policy (CIO)		
CIO-126: Artificial Intelligence Policy		
EFFECTIVE DATE: 10/06/2025	REVISED:	REVIEWED:

I. PURPOSE

The purpose of this policy is to outline the acceptable uses of generative artificial intelligence (AI) for executive branch employees of the government of the Commonwealth of Kentucky. The policy is created to govern the approved uses of generative AI and protect the safety, privacy, and intellectual property rights of the data of the Commonwealth of Kentucky.

II. DEFINITIONS

"Artificial Intelligence" or "AI" – means the use of machine learning and related technologies that uses data to train statistical models for the purpose of enabling computer systems to perform tasks normally associated with human intelligence or perception.

"Artificial intelligence system" – (a) Means any machine-based computing system that, for any explicit or implicit objective, infers from the inputs such system receives how to generate outputs, including but not limited to content, decisions, predictions, or recommendations, that can influence physical or virtual environments; and (b) Does not include an artificial intelligence system that is used for development, prototyping, and research activities before such artificial intelligence system;

"Consequential decision" – means any decision that has a material legal or similarly significant effect on the provision or denial of services, cost, or terms to any citizen or business.

"General-purpose artificial intelligence model" – (a) Means a model used by any form of artificial intelligence system that displays significant generality, is capable of performing a wide range of distinct tasks, and can be integrated into a variety of subsequent applications or systems; and (b) Does not include any artificial intelligence model that is used for development, prototyping, and research activities before such artificial intelligence model is released on the market.

"Generative Artificial Intelligence" or "Generative AI" – means an artificial intelligence system that is capable of producing and used to produce synthetic content, including audio, images, text, and videos.

"High-risk artificial intelligence system" – (a) Means any artificial intelligence system that is a substantial factor in the decision-making process or specifically intended to autonomously make, or be a substantial factor in making, a consequential decision; and (b) Does not include a system or service intended to perform a narrow procedural task, improve the result of a completed human activity, or detect decision-making patterns or deviations from previous decision-making patterns and is not meant to replace or influence human assessment without human review, or perform a preparatory task in an assessment relevant to a consequential decision.

COMMONWEALTH OFFICE OF TECHNOLOGY		Page 2 of 6
Office of the Chief Information Officer Enterprise Policy (CIO)		
CIO-126: Artificial Intelligence Policy		
EFFECTIVE DATE: 10/06/2025	REVISED:	REVIEWED:

III. POLICY

Generative AI is trained on large data sets of existing content. With this training and understanding, generative AI can understand the underlying structure and style of data, continue to learn, and apply knowledge across a wide range of tasks and domains. It can be applied to a wide range of use cases and incorporates cognitive flexibility, adaptability, and general problem-solving skills.

- A. State agencies may not use high-risk artificial intelligence systems.
- B. An AI tool may be used to generate information that will be an input to an overall process, but no consequential decision shall be rendered without human review.
- C. When making use of generative AI tools and capabilities, state agencies and users must adhere to the following general principles:
 1. Transparency: Users and agencies must be transparent about how they are using generative AI. This shall include a clear and conspicuous disclaimer every time AI is used.
 2. Accountability: Users and agencies are accountable to citizens of the Commonwealth, a department, agency or administrative body for the decisions that are made and materials created using generative AI.
 - a. In any instance where AI is utilized to render any decision, agencies and other users shall (1) disclose the role AI played in the decision-making process, (2) explain the required human oversight or validation of AI involvement in the decision-making process, and, for a consequential decision that involved generative AI, (3) provide a process for individuals to appeal the consequential decision.
 - b. In any instance where AI is used in the process of reaching a consequential decision, agencies and users shall explicitly and specifically document the principles, processes, and personnel utilized to prevent AI decision biases; identify and document biases and accounts for potential biases.
 - c. Users and agencies shall specifically designate who maintains ongoing responsibility for periodic review and update of processes to prevent against AI bias.
 3. Fairness: AI systems can reflect the cultural, economic, and social biases of the source materials used for training, and the algorithms used to parse and process that content can be a source of bias as well. The Commonwealth Office of Technology (COT) shall evaluate the AI system to ensure that the system provider or author has considered these concerns and has implemented privacy and security controls to ensure reasonable steps are taken to avoid potential bias.

COMMONWEALTH OFFICE OF TECHNOLOGY		Page 3 of 6
Office of the Chief Information Officer Enterprise Policy (CIO)		
CIO-126: Artificial Intelligence Policy		
EFFECTIVE DATE: 10/06/2025	REVISED:	REVIEWED:

- a. Agencies shall establish a procedure to review AI system performance at a frequency commensurate with the sensitivity and criticality of the business use case. The sensitivity and criticality of all use cases will be determined by the agency in partnership with COT to consider both technical and business aspects. The agencies shall monitor the output and adopt methods to detect and document potential bias, such as ensuring data collections include a wide and representative range of demographics.
 - b. Agencies must use the AI system in compliance with statutes, regulations, COT policies and agency policies and procedures.
4. Privacy: Users and agencies must protect the privacy of individuals when using AI. This means that AI models shall not be used to collect or store personal information without express written consent of the individual. Similarly, employees shall not input, and AI models should not collect or store, information generally recognized as confidential or proprietary without express written consent of each individual or business that owns the confidential or proprietary information. Individual or business consent is not required when the data is collected by the Commonwealth according to statute or regulation. COT shall evaluate the AI system to ensure that separation of data exists to prevent unintended disclosure of state data in any public or shared AI model. This process should prevent inclusion of internal, confidential, private, controlled, or restricted data in a publicly accessible training model to prevent any inadvertent inclusion of personally identifiable information. Employees shall refrain from entering any individual or business's confidential or proprietary information into third party AI models that are available to the general public and are not developed, maintained, or administered in accordance with this policy.
5. Security: COT shall take steps to prioritize personal privacy and the protection of the data of individuals and businesses. COT will utilize established privacy and security control standards, such as the privacy and security controls developed by the National Institute of Standards and Technology, to ensure that baseline data protection standards, as defined in COT enterprise IT policies and Kentucky Information Technology Standards, are met.
6. Training: COT shall mandate a minimum level of AI training for users and agencies responsible for the business processes that are incorporating generative AI. The training shall outline compliance with applicable statutes and regulations, COT Enterprise policies, and the Executive Branch Code of Ethics as defined in KRS Chapter 11A. Agencies shall (1) ensure that employees complete any COT-mandated training for AI users and (2) provide supplemental training as needed to ensure that usage of AI meets agency standards and applicable laws and regulations. In instances where an agency utilizes AI in connection with either generative or decision-making tasks, the agency shall document the AI training provided to employees connected to those tasks.

COMMONWEALTH OFFICE OF TECHNOLOGY		Page 4 of 6
Office of the Chief Information Officer Enterprise Policy (CIO)		
CIO-126: Artificial Intelligence Policy		
EFFECTIVE DATE: 10/06/2025	REVISED:	REVIEWED:

7. Use: There are unresolved legal issues surrounding generative AI and the data inputs used to create AI models. AI systems may be trained using copyrighted material that has been sourced without regard for copyright or licensing terms. Sources of inputs to models must be reviewed and usage risk evaluated. COT shall evaluate the AI system to ensure that reasonable privacy and security controls are in place to ensure the integrity of the AI model. Agencies shall specifically document internal policies and procedures that govern, based on specific use cases, what data can be ingested by the model for the agencies' use.

D. The responsibilities of state agencies when using AI include the following:

1. Responses generated from generative AI outputs shall be subject to human review for accuracy, appropriate usage, privacy of data, and security before being acted upon or disseminated.
2. Responses generated from generative AI shall not:
 - a. be used verbatim,
 - b. be assumed to be credible or accurate,
 - c. be treated as the sole source of reference,
 - d. be used to issue official statements (e.g., policy, legislation, or regulation),
 - e. be relied upon to make final decisions,
 - f. be used to impersonate individuals or organizations.
3. Confidential information or internal data:
 - a. Material that is not available to the public shall not be entered as input to generative AI. All information that is provided to any AI application shall be subjected to the same standards as referenced in the CIO-060 Acceptable Use Policy, CIO-061 Social Media Policy, ENT-101 Enterprise Data Classification Standard, and ENT-102 Enterprise Data Classification Process and shall be treated as publicly available information.
 - b. Material that is copyrighted shall not be entered as input to generative AI.
 - c. Generative AI shall not be used for any activities that are illegal or in violation of state policy, COT policy, or agency policy.
4. Agencies shall require all vendors, in response to a request for proposal and as part of any awarded contract, to affirmatively disclose in writing every use of generative AI and/or integrations with generative AI system. The vendor shall disclose all parts of contracted work that is, was, or will be performed with the assistance of AI.
5. Agency contracts shall prohibit vendors from using Commonwealth confidential or internal data in generative AI queries or for building or training proprietary generative AI programs unless explicitly approved in writing by the agency head with consultation from the COT Chief Information Security Officer.

COMMONWEALTH OFFICE OF TECHNOLOGY		Page 5 of 6
Office of the Chief Information Officer Enterprise Policy (CIO)		
CIO-126: Artificial Intelligence Policy		
EFFECTIVE DATE: 10/06/2025	REVISED:	REVIEWED:

6. Vendors using Generative AI to build software exclusively for the Commonwealth must demonstrate control over all data input into the system.
7. Software Code Development:
 - a. Software code generated by generative AI shall only be implemented after COT has identified and mitigated all business and security risks related to its use. The agency shall conduct code reviews and engage COT, or an independent third party, to complete a thorough security risk assessment prior to deploying AI generated code.
 - b. All software code written by generative AI shall be clearly annotated.
8. Agency leaders are responsible for establishing procedures for their organization's use of AI and obtaining approval of those procedures by COT. All executive branch agencies shall establish an AI governance structure, including policy and procedure that:
 - a. Is sufficient to ensure that no such system:
 1. Results in any unlawful discrimination against any individual or group of individuals; or
 2. Contains factual errors, inconsistent or illogical information, or random or irrelevant output, and misinterpreted patterns.
 - b. All AI systems shall comply with the following:
 1. All statutes, regulations, COT policies, agency policies, and procedures;
 2. Human monitoring for technical compliance, and legal and ethical compliance; and
 3. Risk management procedures and regular and ongoing review at a frequency based on the sensitivity and criticality of the system, and in compliance with any applicable regulatory guidelines.

IV. COMPLIANCE AND DISCIPLINARY ACTION

Each agency must ensure that staff within their organizational authority are made aware of and comply with this policy. The agency is responsible for enforcing it. Failure to comply with this policy may result in corrective or disciplinary action up to and including dismissal. COT may require additional service charges from the agency for remediation efforts due to non-compliance with this policy.

COMMONWEALTH OFFICE OF TECHNOLOGY		Page 6 of 6
Office of the Chief Information Officer Enterprise Policy (CIO)		
CIO-126: Artificial Intelligence Policy		
EFFECTIVE DATE: 10/06/2025	REVISED:	REVIEWED:

V. APPLICABILITY

All executive branch agencies and non-executive branch agencies using COT-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government. Organizations may modify this policy to fulfill their responsibilities but must obtain approval from COT through an exception request. Staff should refer to their internal policy, which may have additional information or clarification.

VI. REFERENCES

Helpful references can be found on the Enterprise IT Policies webpage.

Artificial Intelligence Risk Management Framework (AI RMF 1.0):
<https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>.