

Artificial Intelligence Use, Assessment, Review, and Approval

190.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for Sheriff's Office use of artificial intelligence (AI) as well as to establish a process for assessing such technologies for use within the Office.

Additional guidelines for the use of Sheriff's Office information technology resources are found in the Information Technology Use Policy.

190.1.1 ISSUANCE/EFFECTIVE DATE

This policy was re-issued on Sep. 1, 2026 and shall become effective upon issuance (operational updates).

190.1.2 DEFINITIONS

Definitions related to this policy include:

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. 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 (15 U.S.C. 9401(3)).

Generative AI — an automated computing system that, when prompted with human prompts, descriptions, or queries, can produce outputs that simulate human-produced content, including, but not limited to, the following: (1) textual outputs, such as short answers, essays, poetry, or longer compositions or answers; (2) image outputs, such as fine art, photographs, conceptual art, diagrams, and other images; (3) multimedia outputs, such as audio or video in the form of compositions, songs, or short-form or long-form audio or video; and (4) other content that would be otherwise produced by human means (775 ILCS 5/2-101(N))

AI Model — a component of an information system that implements AI technology and uses computational, statistical, or machine-learning techniques to produce outputs from a given set of inputs.

Human-in-the-Loop (HITL) — a process by which AI-generated outputs undergo review by a qualified human prior to final use or application. This term may also refer to such a qualified human.

Prompt — a question, query, or other request for information presented to an AI system by a human or another computer system.

Training data — large groups of information used to teach AI systems to make accurate decisions and produce meaningful answers to prompts from humans or computer systems.

Cook County Sheriff's Office Administration

Policy Manual

Artificial Intelligence Use, Assessment, Review, and Approval

Example: electronic data from the Library of Congress available online could be used as training data for an AI system. This system could then respond to a prompt asking the AI to write a poem in the style of Robert Frost.

190.2 POLICY

The use of AI systems carries unique benefits within a law enforcement agency, providing ways to increase operational efficiency, enhance Sheriff's Office procedures, and improve the overall effectiveness of the Cook County Sheriff's Office Administration.

However, the prompts input into AI systems can present risks to both individuals and law enforcement agencies by making accessible to the public information such as Sheriff's Office tactics, investigative and training techniques, confidential information (e.g., confidential informants, protected information), active investigations, and security procedures. In addition, without safeguards in place, AI can produce unintended discriminatory or biased output as well as content that is inaccurate, misleading, or copyrighted. Therefore, the Sheriff's Office shall safeguard its use of such technology against any intentional or unintentional negative impacts, including the potential for the invasion of privacy, spread of inequity, and violation of rights. The Sheriff's Office shall implement a transparent and accountable system that fairly evaluates the benefits and risks of the use of such technology to that end.

It is the policy of the Sheriff's Office to develop, implement, and use AI ethically and responsibly in a way that minimizes potential risk and harm in accordance with the guidelines set forth below. In particular, the Sheriff's Office commits to the following principles:

- **Transparency** – The Sheriff's Office commits to using AI in such a manner that is, whenever practical, apparent to the public and individuals who may be impacted by AI use.
- **Accountability** – The Sheriff's Office commits to ensuring AI use is justified, monitored, and managed through an assessment system that accounts for the potential harm and benefits of each application.
- **Privacy** – The Sheriff's Office commits to using AI technology in a way that protects the privacy of individuals and the public to the greatest extent possible.
- **Bias Mitigation** – The Sheriff's Office commits to seek out and address any biases that may emerge in the use of AI technology.
- **Human Control** – The Sheriff's Office shall employ necessary safeguards to ensure it maintains control over its processes. Any input generated from an AI-enabled system shall not be the sole basis for critical decisions made within the Office. Any autonomous or semi-autonomous AI-enabled system shall be subject to regular review to ensure its performance is consistent with the Office's mission.

Any function carried out by a member of the Sheriff's Office using AI is subject to the same laws, rules, and policies as if carried out without the use of AI. The use of AI does not permit any law, rule, or policy to be bypassed or ignored.

Cook County Sheriff's Office Administration

Policy Manual

Artificial Intelligence Use, Assessment, Review, and Approval

The terms of this policy do not replace, amend, or supplement any terms or conditions of employment stated in any collective bargaining agreement that a union has effectively entered into with CCSO.

This policy is not intended to preclude, dissuade, or interfere with CCSO employees' rights to engage in legally protected activities, including under applicable sections of the Illinois Public Labor Relations Act (5 ILCS 315/1 et seq.), such as discussing wages, benefits, or terms and conditions of employment, or engaging in collective bargaining or other lawfully protected union activity.

190.3 REVIEW AND ASSESSMENT OF AI TECHNOLOGY

All software considered or deployed for CCSO use, regardless of whether AI is present, is subject to multiple levels of review to determine compliance with CCSO security requirements, performance specifications, and adherence to CCSO operational policy requirements. Any software containing AI is subject to additional scrutiny to verify compliance with this policy and any other regulatory, legislative or policy requirements.

Permissible and prohibited features of AI technology may vary across use cases; these use cases are determined based on the AI technology's potential to cause harm, its capacity to generate disparate impacts across populations, and the risk of an information breach in a given use case. The Chief Information Officer (CIO) or the authorized designee shall develop procedures and processes for the review and assessment of AI technology to be used at the Sheriff's Office.

190.3.1 MINIMUM REQUIREMENTS ACROSS ALL USE CASES

Any AI technology employed at the Sheriff's Office is subject to the following minimum requirements:

- (a) The Sheriff's Office shall not employ AI technology that is known to release sensitive information, intentionally or unintentionally, to unauthorized entities. This sensitive information may include, but is not limited to:
 - Personally identifiable information
 - Private information
 - Confidential information regarding pending and actual law enforcement investigations
 - Identification of confidential informants
 - Information that would impact the physical safety of Sheriff's Office members, persons in its custody, contractors, vendors, and visitors
 - Information that would impact the physical security of the Sheriff's correctional facilities, law enforcement facilities, and other facilities under its direct or indirect control
 - Information that would impact that Sheriff's information network security and system architecture

Cook County Sheriff's Office Administration

Policy Manual

Artificial Intelligence Use, Assessment, Review, and Approval

- Information subject to legal privilege such as attorney client and deliberative process privileges.

The CIO or the authorized designee shall be informed of the information security effects of any AI technology employed by the Sheriff's Office, including:

- What data are gathered by the AI technology;
- Where data generated from user inputs and system outputs are stored;
- Who has access to the data stored; and
- How the data are used.

Refer to the Protected Information and Data Classification Policies for further guidance.

- (a) The Sheriff's Office shall not employ AI technology known to disparately affect an individual's rights or freedoms or the rights or freedoms of a community. The CIO or the authorized designee shall be informed of the potential for an AI technology to generate disparate impacts among people or groups based on a particular characteristic, specifically a protected classification under law. This includes performing regular internal audits of outputs and end products and reviewing and soliciting third-party reviews (e.g., academic studies, verified vendor quality control checks) as appropriate.
- (b) Training and transactional data shall only come from known and legal sources. The CIO or the authorized designee shall evaluate the training and transactional data to ensure that they are of sufficient quality for the application used and that they do not carry known bias or are capable of being influenced by malicious actors.

190.3.2 LIFE SAFETY USE CASE

A life safety use case involves applications of AI to aid members in protecting human life and personal safety in a first-responder capacity.

Example: While enroute to a call, a Sheriff's Police member receives information from an AI system that queries Sheriff's Office systems to determine if any identified individuals had previous involvement with the Office, whether any individuals had any medical issues recorded in any Sheriff's systems, and whether any individual is a FOID carrier.

Application of AI technology in a life safety use case are subject to the following additional requirements:

- (a) Any application of AI technology in a life safety use case must have a qualified HITL who shall evaluate a recommendation from an AI tool before an action is taken based on that recommendation. The qualified human shall be accountable for any decision made in these scenarios.
 - AI technology shall not replace human judgment in a life safety use case.
- (b) Members using AI technology in a life safety use case must be capable of performing all necessary tasks in the use case without the AI tool in the event that the tool does not function properly.

Cook County Sheriff's Office Administration

Policy Manual

Artificial Intelligence Use, Assessment, Review, and Approval

- (c) Application of AI technology in a life safety use case shall not be procured, used, or adopted without the approval of the Chief of Staff.

190.3.3 STRATEGIC PLANNING USE CASE

A strategic planning use case involves applications of AI to aid in decisions that affect the allocation of Sheriff's Office resources or the overall operating philosophy of different units within the Office.

Example: The Sheriff's Office wants to provide effective levels of public safety support to a particular area within Cook County. The Sheriff's Office needs to accurately predict the rate and types of calls for service in that area in order to determine whether current personnel resources are sufficient to cover that area.

Application of AI technology in a strategic planning use case are subject to the following additional requirements:

- (a) Any application of AI technology in a strategic planning use case must have a qualified HITL who shall evaluate a recommendation from an AI tool before an action is taken based on that recommendation. The qualified human shall be accountable for any decision made in these scenarios.
- (b) AI technology shall not be the sole information used to direct an allocation of policing resources.
- (c) AI technology shall not be used to predict or assign likelihood of an individual or group of individuals to offend or reoffend in a manner that is the sole reason for the allocation of resources.
- (d) Application of AI technology in a strategic planning use case shall not be procured, used, or adopted without the approval of the Chief of Staff or the authorized designee.

190.3.4 INVESTIGATIVE USE CASE

An investigative use case involves applications of AI to aid members in investigating criminal activity

Example: The Sheriff's Office is investigating a complex conspiracy case with multiple participants and victims with varying levels of involvement. The case includes complex financial transactions, a large amount of identified evidence and other complex interactions between the individuals identified. The Sheriff's Office utilizes a software program that helps organize the evidence and records in a comprehensible manner.

Applications of AI technology in an investigative use case are subject to the following additional requirements:

- (a) Any application of AI technology in an investigative use case must have a qualified HITL who shall evaluate a recommendation from an AI tool before an action is taken based on that recommendation. The qualified human shall be accountable for any decision made in these scenarios.
- (b) AI technology shall not be used as the sole basis for any charge, arrest, or detention. If AI technology generates an investigative lead, other reliable investigation techniques

Cook County Sheriff's Office Administration

Policy Manual

Artificial Intelligence Use, Assessment, Review, and Approval

shall be used to confirm AI output prior to charging, arresting, or detaining a person based on that lead.

- (c) Application of AI technology in an investigative use case shall not be procured, used, or adopted without the approval of the Chief of Staff or the authorized designee.

190.3.5 ADMINISTRATIVE USE CASE

An administrative use case involves applications of AI to aid the Sheriff's Office in routine information processing; responding to non-emergency, non-sensitive public requests; and administrative decisions pertaining to members of the public.

Example: The Sheriff's Office implements a chatbot on its public-facing website allowing a user from the general public to pose questions regarding how to request an appearance by the Sheriff at an upcoming public event.

Administrative use cases are subject to the following additional requirements:

- (a) The CIO or the authorized designee should regularly audit the end product of any application of AI technology in an administrative use case that does not have a qualified HITL for quality control and bias mitigation.
- (b) Application of AI technology in an administrative use case shall not be procured, used, or adopted without the approval of the CIO or the authorized designee. The CIO or the authorized designee shall promptly inform the Chief of Staff of such approval and why the application fits an administrative use case.

190.3.6 SPECIAL USE CASES

If the application of AI does not fall under a use case defined by this policy, the CIO or the authorized designee shall, in consultation with the Chief of Staff or the authorized designee as appropriate, develop minimum requirements for a special use case. Considerations for developing these requirements include, but are not limited to:

- How the use case is addressed without AI tool(s) and the potential benefits of using AI;
- The potential of the AI technology to cause harm to members and/or the public;
- The risk of an information breach presented by the use of the AI technology; and
- The capacity of the AI technology to generate disparate impacts across legally protected groups of people.

Application of AI technology under a special use case shall not be procured, used, or adopted without the approval of the Chief of Staff.

190.3.7 MULTIPLE USE CASES

Applications of AI technology falling under multiple use cases shall be evaluated against all applicable requirements.

For every use case, the CIO or the authorized designee shall perform a minimal risk analysis, privacy impact analysis, and disparate impact analysis. These analyses shall include a description of appropriate risk mitigation measures to take in applying AI technology for each use case.

Cook County Sheriff's Office Administration

Policy Manual

Artificial Intelligence Use, Assessment, Review, and Approval

Procedures for risk assessment and the risk assessment tool will be available to the public via the CCSO website.

190.3.8 CHIEF OF STAFF APPROVAL AND REPORTING PRIOR TO PROCUREMENT, UTILIZATION AND ADOPTION

1. Before procuring, utilizing, or adopting new AI technology in its operations, the CIO or the authorized designee shall conduct a risk assessment of the AI technology prior to:
 - (a) Seeking funds for the new technology, including applying for a grant, accepting local, state, or federal funds or other public/private donations of any kind;
 - (b) Acquiring the new technology;
 - (c) Using or adopting existing technology:
 - i. For a novel purpose;
 - ii. In novel circumstances, that may substantially change the data collected, including the content of the data, its granularity, and the purpose of data collection or use;
 - iii. For a purpose not previously approved by the Chief of Staff; or
 - iv. For a purpose not practiced before the approval of this policy
 - (d) Entering into agreement to acquire, share or otherwise use technology.
2. When reporting to the Chief of Staff, in accordance with the procedure above, the CIO or the authorized designee should describe:
 - (a) The operational need(s) the AI technology will address, including how use of the AI technology will improve on current practices or operations;
 - (b) How the CCSO intends to use the AI technology;
 - (c) The use case ascribed to the AI technology, why the AI technology was ascribed it, and the rationale for continuing with the procurement, utilization or adoption requested;
 - (d) The legislative authority for the collection of personal information, if applicable;
 - (e) How the AI technology operates, including the source of the training data, what information will be collected, how/where information will be stored, how it will be disposed of, retention periods for the information collected, and evidence of the validity, accuracy and security of AI technology under consideration, based on industry standards;
 - (f) The steps the CCSO will take to ensure AI technology is used only in accordance with any and all applicable privacy laws and other legal requirements.
 - (g) An evaluation of the AI technology's vendor, including its record in regard to data security and ethical practices;
 - (h) The results of any privacy impact or other assessments that have been conducted;

Cook County Sheriff's Office Administration

Policy Manual

Artificial Intelligence Use, Assessment, Review, and Approval

- (i) The feedback received from any consultations used with regard to procurement, utilization or adoption of the AI technology;
- (j) An analysis of possible unintended consequences of the proposed use of the AI technology from legal and human rights perspectives;
- (k) Where applicable, a legal analysis of potential challenges to the admissibility of evidence generated or impacted by the AI technology in criminal proceedings;
- (l) Any reports and documentation used in the evaluation of AI technology;
- (m) A mitigation plan to:
 - i. Mitigate the risks posed by the implementation of the AI technology, including risks of biased policing, infringement of privacy or other rights, chilling effects on freedom of expression, and risks of abuse or unauthorized access to information, and including the mitigation of any bias or quality issues in the training data used by the AI technology;
 - ii. Ensure that any use of the AI technology can and will be audited to ensure adequate and lawful use, in accordance with the purposes approved by the Chief of Staff, and to monitor errors; and,
 - iii. Notify any applicable legal authority of any significant privacy breaches or other significant malfunctions that may result in harm to individuals, communities or CCSO members, or may affect criminal proceedings;
- (n) The estimated cost of acquiring and implementing AI technology, including cost of training personnel on the operation of the technology and cost of training any models or other systems used within the AI implementation, and any additional costs anticipated from the implementation; and
- (o) Proposed indicators that will be tracked by the CIO or the authorized designee for the purposes of determining whether the AI technology is achieving its intended goal and whether its use has had any unintended consequences, until it is determined by the Chief of Staff that monitoring is no longer required.

190.3.9 MONITORING AND REPORTING

The CIO shall:

1. Monitor the indicators approved by the Chief of Staff from the initiation of the adoption and use of AI technology until 24 months after full implementation of AI technology; and
2. Report to the Chief of Staff every 24 months regarding the use of all AI technology in the Office. Reporting should include:
 - (a) How AI technology has generally been deployed or utilized within the Office, including with respect to compliance with applicable privacy laws and other legislative and legal requirements;
 - (b) The performance of specific AI technologies as measured by the indicators approved by the Chief of Staff;

Cook County Sheriff's Office Administration

Policy Manual

Artificial Intelligence Use, Assessment, Review, and Approval

- (c) What concerns the CCSO has seen raised by members of the public or internally by CCSO staff and what has been done to address those concerns;
- (d) Whether it is recommended that the CCSO continue using specific AI technologies in the same manner in the future; and
- (e) Any recommended modifications to the use of AI technologies in the Office.

190.3.10 PROTECTION OF CCSO DATA AND TRAINING DATA USAGE

All third-party vendors providing AI system services to CCSO must review and comply with the Sheriff's Information Technology Special Conditions (ITSC) before the commencement of any data transactions. The third-party vendor providing AI system services to the Sheriff's Office must provide a standards and procedures manual that includes procedures for the auditing, security, encryption, sanitization, and destruction of data that is the exclusive property of CCSO.

All data provided to or used by an AI system or model created or maintained by an authorized third-party will remain the exclusive property of CCSO. All data generated as an output and/or product by a third-party AI system or model will remain the exclusive property of CCSO.

Training data generated as a result of processing data that is the exclusive property of CCSO must be deidentified and sanitized. Authorized third-party vendors shall deidentify and sanitize CCSO data used as an input or generated as an output before being utilized as training data.

Refer to the Sheriff's Information Technology Special Conditions (ITSC) for further guidance.

190.3.11 AUDIT PROCEDURES FOR THIRD-PARTY AI SYSTEMS

All third-party vendors authorized to provide AI system services to CCSO must establish procedures to allow the CIO to audit the processing of data that is the exclusive property of CCSO.

Authorized third-party vendors must provide the following services in compliance with this Policy:

- Implement an auditing system to monitor and document all CCSO data inputs and outputs.
- Provide authorized CCSO personnel access to internal audits of the AI system tasked with processing data that is the exclusive property of CCSO.
- Notify and consult with the CIO regarding unauthorized access to CCSO data, cybersecurity breaches involving CCSO data, updates to the AI system software that may impact the transaction of CCSO's data, and compliance issues with local, state, and federal law.

190.4 USE OF AI

Members seeking to acquire or use AI technology must first submit a written request to the CIO. The CIO or the authorized designee will then conduct a written analysis based on the assessment framework defined in this policy, and, if the CIO approves, the request and analysis will be submitted to the General Counsel. If the General Counsel approves, the request and analysis will be submitted to the Chief of Staff for approval.

Cook County Sheriff's Office Administration

Policy Manual

Artificial Intelligence Use, Assessment, Review, and Approval

The CCSO process and procedure for analysis of AI technology applies to all AI technology, including free-to-use software or tools.

If a technology has already been approved for use, no additional approval is required. However, all members who use such technology may be subjected to training before use. The CIO or Chief of Staff may revoke authorization for use of a pre-approved technology that presents with added AI capabilities or may restrict the use of those AI capabilities, if, in their judgement, those AI capabilities present risks that cannot be effectively mitigated to comply with this policy or other CCSO policies.

The use of Sheriff's Office AI systems by Sheriff's Office members shall be limited to official work-related purposes, and members shall only access and use AI systems for which they have been authorized and received proper training.

Members shall use AI-generated content as an informational tool and not as a substitution for human judgment or decision-making. Members should not represent AI-generated content as their own original work.

AI-generated content should be considered draft material only and shall be thoroughly reviewed prior to use. Before relying on AI-generated content, members should:

- (a) Obtain independent sources for information provided by AI and take reasonable steps to verify that the facts and sources provided by AI are correct and reliable.
- (b) Review prompts and output for indications of bias and discrimination and take steps to mitigate its inclusion when reasonably practicable (see the Bias-Based Policing Policy).
- (c) Include a statement in the final document or work product that AI was used to aid in its production. See the subsection entitled Attribution, Accountability, and Transparency of Ownership for further guidance.

190.4.1 HUMAN-IN-THE-LOOP (HITL) PROCESS

AI systems should be subject to a HITL process by which AI-generated outputs are reviewed by humans prior to each use in an official capacity. HITL review processes shall be documented by the departments involved and shall demonstrate how the HITL review was conducted to adhere to the principles outlined in this document.

Any review of a HITL process should include, at a minimum, an assessment of the following:

- The relative performance of the AI system involved;
- The relative performance of the human element of the system; and
- The effectiveness of the human-AI interaction in the overall system.

190.4.2 PRIVACY CONSIDERATIONS

Information not otherwise available to the public, including data reasonably likely to compromise an investigation, reveal confidential law enforcement techniques, training, or procedures, or risk the safety of any individual if it were to become publicly accessible, should not be input into a

Cook County Sheriff's Office Administration

Policy Manual

Artificial Intelligence Use, Assessment, Review, and Approval

AI system unless contractual safeguards are in place to prevent such information from becoming publicly accessible. Members should instead use generic unidentifiable inputs, such as "suspect" or "victim," and hypothetical scenarios whenever possible.

Protected information should only be input into AI systems that have been approved for such use and comply with applicable privacy laws and standards (see the Protected Information Policy).

190.4.3 ATTRIBUTION, ACCOUNTABILITY, AND TRANSPARENCY OF OWNERSHIP

All images and videos created by AI systems must be attributed to the appropriate AI system. Wherever practicable, attributions and citations to the CCSO should be embedded in the image or video (e.g., via digital watermark, cryptographic signature).

If text generated by an AI system is used substantively in a final product, attribution to the relevant AI system is required.

If a significant amount of source code generated by an AI system is used in a final software product, or if any amount is used for an important or critical function, attribution to the appropriate AI system is required via comments in the source code and in product documentation.

All attributions should include the name of the AI system used plus an HITL assertion (which should include the department or group who reviewed/edited the content).

Departments shall interpret "substantive use" thresholds to be consistent with the principles outlined in this document as well as relevant intellectual property laws.

Example attribution statement: "Some material in this brochure was generated using ChatGPT 4.0 and was reviewed for accuracy by a member of the Department of Corrections before publication."

190.4.4 USE OF AI IN EMPLOYMENT ACTIONS

The Sheriff's Office may use AI tools for employment actions, including for recruitment, hiring, promotion, renewal of employment, selection for training or apprenticeship, discharge, discipline, tenure, or the terms, privileges, or conditions of employment. In compliance with the Illinois Human Rights Act (IHRA), the use of AI must not be used in any manner that has the effect of subjecting employees to discrimination on the basis of protected classes under the IHRA or to use zip codes as a proxy for such protected classes (IL Public Act 103-0804/775 ILCS 5/2-102(L)). The use of AI in employment actions, including those mentioned in this section, must be disclosed appropriately, including attributions under the subsection titled "Attribution, Accountability, and Transparency or Ownership". Refer to the Prohibition Against Discrimination and Harassment policy for further guidance as necessary.

190.5 PROHIBITED USE

Members shall not use AI systems to rationalize a law enforcement decision, or as the sole basis of research, interpretation, or analysis of the law or facts related to a law enforcement contact or investigation.

Cook County Sheriff's Office Administration

Policy Manual

Artificial Intelligence Use, Assessment, Review, and Approval

Members shall not create user accounts in their official capacity or input work-related data (including information learned solely in the scope of their employment) into publicly available AI systems unless the system has been approved by the Sheriff or the authorized designee for the intended use.

Members shall not use AI systems to create content that could be mistaken for actual, identifiable people (e.g., elected officials, celebrities, missing persons) unless used for legitimate law enforcement activity. Such use requires prior approval from the Chief of Staff or the authorized designee.

190.6 PUBLIC RECORDS AND RECORDS MANAGEMENT

All records generated, used, or stored by AI vendors or solutions shall be retained and disclosed pursuant to federal, state, and local laws and internal CCSO policy. These laws include, but are not limited to, the Illinois Freedom of Information Act (5 ILCS 140/1 et seq.) and the Local Records Act (50 ILCS 205/1 et seq.).

Refer to the Records Maintenance and Release and Freedom of Information Act Policies for further guidance.

190.7 PUBLIC ENGAGEMENT

The Chief of Strategy, Public Policy, and Communications or the authorized designee, in consultation with the Bureau of Information Technology, will make available via the Sheriff's Office website:

1. Information about the Cook County Sheriff's Office's use of AI technology, including the methodologies, standards, and principles it adheres to when procuring and adopting new AI technology for official use;
2. Information pertaining to how the public can obtain contracts and other records relating to the use of AI technology; and
3. A copy of this policy.

190.8 TRAINING

The CIO or the authorized designee should ensure that all members authorized to use AI have received appropriate initial training that is suitable for their role and responsibilities prior to their use of AI and receive periodic refresher training. Training should include but is not limited to the following:

- (a) A review of this policy
- (b) The need for human oversight of AI outputs
- (c) The interpretation, review, and verification of AI output
- (d) Checking AI output for bias or protected information
- (e) Ethical use of AI technology; and
- (f) Data security and privacy concerns