Generative Artificial Intelligence Use

350.1 PURPOSE AND SCOPE

Best Practice

The purpose of this policy is to provide guidelines for department use of generative artificial intelligence (GenAI). This policy does not apply to artificial intelligence that is integrated into facial recognition applications, voice recognition applications, biometric access controls, or software that redacts documents or video or similar applications.

Additional guidelines for the use of department information technology resources are found in the Information Technology Use Policy.

350.1.1 DEFINITIONS

Best Practice

Definitions related to this policy include:

Generative artificial intelligence (GenAI) - A type of artificial intelligence that is algorithmically trained on one or more large data sets and designed to generate new and unique data (e.g., text, pictures, video) in response to a prompt (generally questions, instructions, images, or video) input by the user.

350.2 POLICY

Best Practice

The use of GenAI systems carries unique benefits within a law enforcement agency, providing ways to increase operational efficiency, enhance department procedures, and improve the overall effectiveness of the agency.

However, the prompts input into GenAI systems can present risks to both individuals and law enforcement agencies by making accessible to the public information such as department tactics, investigative and training techniques, confidential information (e.g., confidential informants, protected information), active investigations, and security procedures. In addition, without safeguards in place, GenAI can produce unintended discriminatory or biased output as well as content that is inaccurate, misleading, or copyrighted.

It is the policy of the Department to develop, implement, and use GenAI ethically and responsibly in a way that minimizes potential risk and harm in accordance with the guidelines set forth below.

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

350.3 RESPONSIBILITIES

Best Practice

350.3.1 AGENCY HEAD

Best Practice

The agency head or an authorized designee shall approve all GenAI systems, their acceptable uses, and their authorized user groups prior to the use, implementation, or development for any department functions.

350.3.2 AI COORDINATOR

Best Practice

The agency head or the authorized designee shall appoint an AI coordinator. The AI coordinator shall report to the Division Commander or the authorized designee.

The responsibilities of the AI coordinator include but are not limited to:

a) Evaluating potential GenAI systems and recommending those GenAI systems that appear to be appropriate and trustworthy to the agency head or the authorized designee. The trustworthiness of GenAI systems should be evaluated by balancing the following characteristics:

   1. Validity and reliability - The system's apparent ability to meet the intended purpose and fulfill the needs of the Department consistently over time.

   2. Safety - Any apparent risk to human life, health, property, or the environment that could result from the department's use of the system.

   3. Security and resiliency - The system's capability to prevent unauthorized access and misuse and its ability to return to normal function should misuse occur.

   4. Accountability and transparency - The ability to track and measure the system's use and activity through histories, audit logs, and other processes to provide insight about the system and identify potential sources of error, bias, or vulnerability.

   5. Explainability and interpretability - The ability of the user to understand the purpose and impact of the system, how and why the system reached the resulting output, and what the output means for the user.

   6. Privacy - The ability of the system to protect confidentiality and meet applicable privacy standards for the types of data intended to be input into the system (e.g., state privacy laws, Criminal Justice Information Services (CJIS), Health Insurance Portability and Accountability Act (HIPAA)).

   7. Fairness - The ability of the system to operate in a way that avoids or minimizes bias and discrimination.

b) Ensuring appropriate contractual safeguards are in place to manage third-party use of department data and to restrict the use of input in AI training data sets. If the input of protected information is necessary for the proper use of the GenAI system, an information-exchange agreement in compliance with applicable rules and standards (e.g., CJIS requirements) should be used to outline the roles, responsibilities, and data ownership between the Department and third-party vendor.

c) Coordinating with others within the Department and City or County, such as the information technology or legal departments, as appropriate to ensure GenAI systems are procured, implemented, and used appropriately.

d) Maintaining a list or inventory of department-approved GenAI systems and, when appropriate for department transparency, making the list or inventory available to the public.

e) Developing and maintaining appropriate procedures related to the use of GenAI systems, including procedures for editing and fact-checking output.

f) Ensuring any public-facing GenAI systems notify the user that GenAI is being used.

g) Developing and updating training for the authorized users of each department-approved GenAI system.

h) Ensuring access to department GenAI systems is limited to authorized users and establishing requirements for user credentials such as two-factor authentication and appropriate password parameters.

i) Conducting audits at reasonable time intervals for each of the GenAI systems utilized by the Department to evaluate the performance and effectiveness of each approved system and to determine if it continues to meet the Department's needs and expectations of trustworthiness. The coordinator should arrange for audits to be conducted by an external source, as needed.

j) Ensuring each GenAI system is updated and undergoes additional training as reasonably appears necessary in an effort to avoid the use of outdated information or technologies.

k) Keeping abreast of advancements in GenAI and any GenAI-related legal developments.

l) Reviewing this policy and department practices and proposing updates as needed to the agency head.

m) Developing procedures in coordination with the *Brady* information coordinator and the Records Head for the compilation and potential release of any discovery or records related to the use of GenAI systems consistent with *Brady* and applicable state open record laws.

350.4 USE OF GENERATIVE AI

Best Practice

The use of department GenAI systems by department members shall be limited to official work-related purposes, and members shall only access and use GenAI 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 GenAI and take reasonable steps to verify that the facts and sources provided by GenAI 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 GenAI was used to aid in its production.

350.4.1 PRIVACY CONSIDERATIONS

Best Practice

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 GenAI 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 GenAI systems that have been approved for such use and comply with applicable privacy laws and standards (see the Protected Information Policy).

350.5 PROHIBITED USE

Best Practice

Members shall not use GenAI 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.

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 GenAI systems unless the system has been approved by the agency head or the authorized designee for the intended use.

350.6 TRAINING

Best Practice

The AI coordinator should ensure that all members authorized to use GenAI have received appropriate initial training that is suitable for their role and responsibilities prior to their use of GenAI 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 GenAI outputs
   c) The interpretation, review, and verification of GenAI output
   d) Checking GenAI output for bias or protected information
   e) Ethical use of GenAI technology
   f) Data security and privacy concerns

Generative Artificial Intelligence Use

IMPLEMENTATION GUIDANCE

The following information is provided to assist you in implementing this policy and should be deleted before the policy is issued to agency personnel.

Generative Artificial Intelligence Use

GENERATIVE ARTIFICIAL INTELLIGENCE USE

The purpose of this policy is to provide agencies guidelines for using generative artificial intelligence (GenAI) products or services.

BACKGROUND NOTES

GenAI applications and services offer productivity gains for organizations by answering questions, summarizing sources, and producing written output that appears human-made. GenAI resources provide fast and impressive results. However, GenAI comes with risks for public safety agencies (e.g., inaccurate or potentially biased output) that require active monitoring by members.

This policy deliberately offers a general framework rather than a detailed list of procedural specifics because the technology continually evolves with new features and capabilities. The policy touches upon the risk areas and mitigations identified as the most important to effectively and safely use GenAI:

- Prohibited uses of GenAI

- The need for members to use only approved GenAI resources

- Member responsibilities, particularly the need to perform a thorough review and verification of GenAI-provided content before using it for work-related purposes

- The need to review GenAI output for potentially introduced bias

- Protected information and privacy concerns

- The need for an AI coordinator (who may be an information technology resource)

The nation's courts and legislatures are taking a keen interest in GenAI. Lexipol will monitor proposed legislation across the states regarding the use of GenAI in the public safety sphere and will update the policy as needed. We encourage agencies to work closely with their legal counsel and information technology providers regarding this policy and the use of GenAI.

CUSTOMIZATION GUIDELINES

Please review the following section carefully and customize accordingly to meet your agency's practice:

- **USE OF GENERATIVE AI** (If your agency does not authorize any usage of GenAI for work-related purposes, delete the section or indicate that the usage is prohibited.)

We recommend that there are no changes to the following sections because they are based on best practice guidelines:

- **AI COORDINATOR** (There should be no change to the responsibilities listed in this subsection without thoughtful review and consultation with appropriate legal counsel and the agency's information technology services provider.)
- **PROHIBITED USE** (There should be no change to this section unless your agency wants to expand on the list of prohibitions.)