

County of Monterey Board Policy Manual

Policy Name Generative Artificial Intelligence	Policy Number O-10	Page 1 of 4
Policy Category Operations and Maintenance		

I. Purpose

The purpose of this policy is to establish the requirements for the responsible, ethical, and secure use of approved Generative Artificial Intelligence (GenAI) tools and services within the County of Monterey (County). It aims to ensure compliance with applicable laws, regulations, and County standards, while maximizing the benefits of Artificial Intelligence (AI) innovation. Through this Policy, the County seeks to promote innovation in the delivery of public services while mitigating potential risks associated with the use of GenAI tools and services.

II. Applicability

The scope of this Policy extends to all information assets owned or operated by the County or its departments, all personnel authorized to use these assets, including, but is not limited to, AI-driven capabilities such as text generation, image creation, code suggestions, and other forms of content generation.

Exceptions to this Policy must be formally documented and will be evaluated on a case-by-case basis. To request a security exception, personnel are required to submit a formal request through a service ticket to the Information Technology Department. Exceptions may be granted for the following reasons:

- a. Compliance with this Policy is not administratively or technically feasible.
- b. Temporary deviation from this Policy is necessary to support a mission critical business function.

III. Definitions

County of Monterey has adopted the information security and privacy definitions published by the National Institute of Standards and Technology in implementing information security and privacy policy. The glossary is available here: <https://csrc.nist.gov/glossary>

- a. **Artificial Intelligence:** A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.
- b. **Approved Generative Artificial Intelligence:** Refers to any Generative AI system, tool, or application that has been formally approved for use by County Information Technology Division. Such systems

must comply with applicable laws, regulations, and County policies, including but not limited to data security, privacy, bias mitigation, and intellectual property protections.

- c. Automated Decision System: A computational process that screens, evaluates, categorizes, recommends, or otherwise makes a decision or facilitates human decision-making that impacts applicants or employees.
- d. Confidential Information: Information maintained by state agencies that are exempt from disclosure under the provisions of the California Public Records Act (Government Code sections 7920.000-7931.000) or has restrictions on disclosure in accordance with other applicable state or federal laws.
- e. Generative Artificial Intelligence: 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.
- f. Personal Information: Any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, the individual's name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.
- g. Personnel: Includes employees, volunteers, contractors, sub-contractors commissioned, employed by or otherwise engaged in the performance of work associated with administration of a state entity program.
- h. Public Information: Public information refers to any information, regardless of form or format, that an organization intentionally makes available to the public. This information is typically unclassified and has no restrictions on access, allowing it to be freely shared, distributed, and used by the general public.
- i. Sensitive Information: Information maintained by state agencies that requires special precautions to protect it from unauthorized modification, or deletion. Sensitive information may be either public or confidential (as defined above).

IV. Policy Requirements and Procedure

This Policy establishes requirements for the use of approved generative artificial intelligence (GenAI) tools and services to ensure responsible, ethical, and secure use, while balancing the benefits and risks of GenAI. This includes but is not limited to text generation, image creation, code suggestions, and any other GenAI driven content generation.

County personnel shall:

- a. Use GenAI to enhance public services and fulfill official duties in support of the County's mission, values, and goals. Use of GenAI is permitted while performing official duties for the County, including but not limited to the following general uses:
- b. For general knowledge questions intended to enhance your understanding of a work-related topic.
- c. To generate ideas related to projects you are working on.
- d. To develop formulas for spreadsheets or similar software.
- e. To develop or debug code, to be verified before deployment
- f. To draft emails or preliminary letters for human review prior to distribution.

- g. Ensure that no information that is classified as confidential, personal or sensitive be entered, inputted, or ingested into approved GenAI software.
- h. Ensure that all GenAI output, content, and final work product undergoes thorough levels of human review and validation. GenAI content must not be trusted without reasonable and appropriate levels of human review.
- i. Ensure that GenAI-generated content does not perpetuate or promote discrimination, bias, misinformation, or manipulation of public opinion.
- j. Acknowledge and agree to NOT use approved GenAI for creating or promoting deceptive content, including but not limited to deepfakes, or in any way that could mislead the public.
- k. Ensure GenAI uses do not infringe on copyright, trademarks, or other protected works without appropriate licensing.
- l. Refrain from using GenAI in automated decision making in areas such as public health and safety, administration of public benefits or employment matters.
- m. Ensure Gen-AI generated content in areas such as official County communications, policy documents, human resources, and legal matters, are reviewed by designated subject matter experts (SMEs) and key stakeholders before it is accepted, relied upon, implemented, used or distributed. All legal matters or legal language must be reviewed by the County Counsel's Office.
- n. Understand that misuse of GenAI tools, including use of unauthorized GenAI violation of this policy, may result in disciplinary action.
- o. Stay well informed of the impact of violating this policy including the potential for legal action in the event of violations involving intellectual property infringement, security incidents, or other unlawful activities.

V. Roles and Responsibilities

County Personnel

- a. Use only approved GenAI tools in alignment with this Policy.
- b. Actively protect County resources from unauthorized GenAI access, use, disclosure, storage or transmission of confidential and/or sensitive data.
- c. Immediately reporting actual or suspected GenAI-related security incidents to their Departmental Information Security Officers (DISOs) and County Chief Security Officer (CSO).
- d. Report violations of this Policy to the DISO and CSO.
- e. Personnel are required to complete annual information security awareness training.

Departmental Information Security Officers (DISOs)

- a. Act as the initial security point of contact for their department's employees concerning GenAI-related issues.
- b. Coordinating with the County's Security Incident Response Team and the CSO to investigate and address any reported security incidents involving GenAI tools.
- c. Collaborate with appropriate teams to implement corrective actions within their departments.

Chief Security Officer

- a. Oversee, maintain and update the County's GenAI policy.
- b. Properly review GenAI software and use cases.

- c. Investigate reported GenAI policy violations.
- d. Report actual data breaches to control agencies.
- e. Update awareness training content to include safe use of GenAI technologies.

Department Managers and Supervisors

- a. Ensure employees under their supervision comply with County Information Technology Department policies.
- b. Ensure only approved GenAI is used.
- c. Reviewing work product for compliance with this Policy.

VI. Compliance

Violations of this Policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of services and/or legal penalties, both criminal and civil. All County entities shall ensure compliance with applicable security and privacy laws, regulations, rules, and standards specific to and governing the administration of their programs.

VII. Auditing and Reporting

- a. The County reserves the right to audit any activities related to the use of County information assets, systems and/or networks.
- b. Violations of this Policy must be reported to respective County Department Information Officer and the Chief Security Officer.

VIII. Authority/References

[Federal Information Security Management Act of 2002, 44 U.S.C. §§ 3541–3549 \(2002\)](#)

[Federal Executive Order on the Safe, Secure, and Trustworthy Development of AI \(EO 13960\)](#)

[National Institute of Standards and Technology Artificial Intelligence Risk Management Framework \(AI 100\)](#)

[National Institute of Standards and Technology Artificial Intelligence Risk Management Framework Generative Artificial Intelligence Profile \(AI-600\)](#)

[California Executive Order N-12-23](#)

[California Department of Civil Rights Department Regulation Regarding Automated Decision Systems](#)

[County of Monterey Appropriate Use Policy](#)

[County of Monterey Data Privacy Policy](#)

IX. Review Date

- a. This Policy will be reviewed for continuance by March 17, 2030.

X. Board Action

- a. Legistar File Number: 25-190, March 18, 2025.