A G E N D A

TECHNOLOGY AND SECURITY
TECHNICAL ADVISORY COMMITTEE

MEETING

APRIL 22, 2026 AT 9:00 A.M.

MEETING WILL BE HELD VIRTUALLY
Video call link: https://meet.google.com/thg-igrn-eom

1. Call to order.
2. Public comment period.
3. Information Technology Security Policy Update
4. AI Policy Subcommittee Report
5. Security update:
    a. Two-Factor Authentication (TFA) rollout
    b. Incident reports
    c. Infrastructure upgrades - CalOES grant application
6. Adjournment

DRAFT

Generative AI (GenAI) Guidelines for County Government Employees

Introduction

This document establishes guidelines for the responsible, ethical, and secure use of Generative Artificial Intelligence (GenAI) tools and platforms by all County government employees, contractors, and affiliates. These guidelines are designed to maximize the benefits of GenAI for enhancing productivity and public service delivery while mitigating risks related to data security, privacy, accuracy, and public trust.

Core Principles for GenAI Use

All County employees must adhere to the following principles when using GenAI in their work:

1. Transparency and Disclosure

- **Trusted Data Sources:** Use reputable and verified data sources both internal and those provided by third parties, ensuring accuracy and reliability of the data used.
- **Fact-Checking:** Establish mechanisms to verify the accuracy of information provided by AI, particularly when it involves critical decisions or public announcements.
- **Identify AI-Generated Content:** Employees must clearly disclose when work products (e.g., reports, summaries, drafts, communications) have been substantially generated or altered by GenAI.
- **Source Citation:** While GenAI output itself is not a primary source, any factual information generated must be independently verified and properly attributed to its original source if included in final public-facing documents.

2. Data Security and Privacy

- **Data Privacy:** Ensure AI complies with relevant data protection laws and regulations, such as those related to personally identifiable information and protected health information, and respect residents' rights to privacy.

- **Secure Data Storage:** Store sensitive data securely, utilizing encryption and access controls to prevent unauthorized access.
- **No Confidential Data Input:** Employees are strictly prohibited from entering any sensitive, confidential, proprietary, or personally identifiable information (PII) into public GenAI tools (e.g., ChatGPT, Bard, Claude) or any non-approved GenAI platform. This includes, but is not limited to:
    - Protected Health Information (PHI)
    - Law enforcement sensitive data
    - Internal County strategy documents
    - Employee or constituent PII
- **Use Approved Tools Only:** Employees must use only GenAI tools that have been explicitly approved by the County's IT department for official use, which include appropriate security and data usage agreements.

3. Accuracy and Verification

- **Human Review is Mandatory:** GenAI output is not guaranteed to be accurate, unbiased, or relevant. All output must be thoroughly reviewed, verified, and edited by a human expert before use, especially for public dissemination or decision-making.
- **Guard Against Hallucinations:** Employees must be aware that GenAI models can "hallucinate" (generate false or nonsensical information presented as fact). Unverified GenAI output must never be used as the basis for official County actions or communications.

4. Ethics and Equity

- **Avoid Bias:** Employees must be vigilant in reviewing GenAI output for potential bias, discrimination, or inequitable outcomes. GenAI must not be used to justify or automate biased decision-making.
- **Uphold County Values:** The use of GenAI must always align with the County's commitment to fairness, accessibility, and public service integrity. GenAI should not be used for malicious purposes, harassment, or to generate content that violates County policies or legal statutes.

Permitted and Prohibited Uses

Permitted Uses (Subject to Verification and Security Rules)

Use Case	Description	Caveats/Requirements
Drafting & Summarization	Generating initial drafts of non-confidential emails, reports, meeting agendas, and summarizing long documents.	Must be fact-checked and reviewed for accuracy and tone. Do not input confidential details.
Code Generation/Debugging	Generating non-critical code snippets or identifying errors in existing, non-sensitive code.	Code must be reviewed by IT/developers for security vulnerabilities before deployment.
Brainstorming & Ideation	Generating ideas for public outreach, process improvements, or policy language exploration.	Output is for internal consideration only; final decision-making must be human-led.
Simple Data Transformation	Reformatting non-confidential data or translating simple text between languages (use caution).	Verify translations for accuracy, especially for official documents.

Prohibited Uses

- **Inputting Sensitive Data:** Entering PII, PHI, financial data, or any legally protected information into public GenAI tools.
- **Automated Decision-Making:** Relying solely on GenAI output for final decisions regarding constituent services, legal interpretations, procurement, or policy enforcement.
- **Plagiarism/Misrepresentation:** Submitting GenAI output as one's own original, unedited work without proper review or failing to disclose its role in creation.
- **Creating Harmful Content:** Generating libelous, discriminatory, defamatory, or misleading content.

Implementation and Training

Employee Responsibilities

- All employees must complete mandatory training on these GenAI guidelines.
- Employees are responsible for staying informed about updates to County technology policies regarding GenAI.
- Any potential misuse or security concern related to GenAI must be immediately reported to the IT Department.

IT Department Responsibilities

- The IT Department will maintain a list of County-approved GenAI tools and platforms.
- IT will monitor the landscape of GenAI technology and periodically review these guidelines.
- IT will provide ongoing training and support for employees on the secure and effective use of approved GenAI tools.

Failure to adhere to these guidelines may result in disciplinary action, up to and including termination of employment.