Harris County

ARTIFICIAL INTELLIGENCE RESPONSIBLE USE POLICY

Document Version: 1.0

Information Security Record Classification

[https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage]

☐ **Red** ☐ **Amber+Strict** ☐ **Amber** ☐ **Green** ☒ Clear

Version History

DATE	VERSION	AUTHOR	CHANGES MADE
11/12/2024	1	Harris County Universal Services	First version

Table of Contents

1. Introduction

1.1. Harris County Universal Services (HCUS) is the centralized solutions center for Harris County (the County). HCUS provides enterprise-wide Information Technology, Public Safety and Justice Technologies, 311 Constituent Engagement Services, Fleet Services, and Records and Information Governance Services to the County.

1.2. Harris County's Generative Artificial Intelligence (AI) Responsible Use Policy, or AI Policy, is being established to foster effective collaboration between County Departments in the ever-evolving world of artificial intelligence, and its increased usage potential in County work. The policy outlines the necessary safeguards and key elements to ensure that AI's usage aligns with County objectives and standard practices and reduces pertinent security risks by applying the safest potential AI practices.

2. Purpose

The purpose of this policy is to establish best practices for the responsible and secure use of AI. The County is committed to utilizing AI technologies responsibly and ethically to improve processes, enhance services to County residents, and support employees to do their best work. This AI Appropriate Use Policy provides simple, user-centric guidance for all employees, regardless of technical expertise.

3. Scope

3.1. The policy applies to:

3.1.1. All AI systems deployed by the County, used on the county networks, or procured from a vendor, and

3.1.2. This policy applies to all GenAI used by Elected and Appointed officials, County employees, (full-time, part-time, temporary), contractors, vendors, volunteers, temporary agency staff or others while performing a role for the County (collectively "users").

4. Guiding Principles for Responsible AI Systems

4.1. These principles describe the County's values with regards to how AI systems are purchased, configured, developed, operated, or maintained. Characteristics of

trustworthy AI systems include: valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair with harmful bias managed.

4.1.1. Human-Centered Design: AI systems are developed and deployed with a human-centered approach, putting humans in the loop to evaluate and have the final say in AI powered outputs that impact decision making and services of the County.

4.1.2. Security & Safety: AI systems maintain confidentiality, integrity, and availability through safeguards that prevent unauthorized access and use. Implementation of AI systems is reliable and safe, and minimizes risks to individuals, society, and the environment. AI Systems are vetted through County's Information Security Governance Process and approved for usage.

4.1.3. Data Privacy and Security: Comply with all data privacy and security standards such as Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Systems (CJIS), Internal Revenue Service (IRS) to protect Personally Identifiable Information (PII), Protected Health Information (PHI), or any sensitive data in generative AI prompts. Treat AI prompts as if they were publicly visible online to anyone. All AI prompts, data inputs, and outputs are subject to the Texas Public Information Act.

4.1.4. Transparency: The purpose and use of AI systems is proactively communicated and disclosed to the public. An AI system, its data sources, operational model, and policies that govern its use are understandable and documented. All AI outputs will have an explicit "AI augmented" tag.

4.1.5. Equity: AI systems will support equitable outcomes for everyone. Bias in AI systems is effectively managed with the intention of reducing harm for anyone impacted by its use.

4.1.6. Accountability: Roles and responsibilities govern the deployment and maintenance of AI systems, and human oversight ensures adherence to relevant laws and regulations.

4.1.7. Effectiveness: AI systems are reliable, meet their objectives, and deliver precise and dependable outcomes for the utility and contexts in which they are deployed.

4.1.8. Workforce Empowerment: Staff are empowered to use AI in their roles through education, training, and collaborations that promote participation and opportunity.

4.1.9. Informed Consent: Members of the public, county officials and employees should be informed when they are interacting with an AI tool and have an "opt out" alternative to using AI tools available. Based on the individual system.

5. Roles and Responsibilities

5.1. Several roles are responsible for enforcing this policy, as outlined below.

5.1.2. Chief Information Officer

5.1.2.1. The Chief Information Officer (CIO) is responsible ensuring AI systems are used in accordance with the County Information Security Policy.

5.1.2.2. The CIO is responsible for overseeing the enterprise security infrastructure, cybersecurity operations, updating security policies, procedures, standards, guidelines, and monitoring policy compliance.

5.1.2.3. The CIO or designee shall notify County departments when an update to this policy is released.

5.1.3. County Departments

5.1.3.1. County departments are responsible for following this policy and following updates to this policy and shall check compliance with these documents at least annually.

5.1.3.2. County Department Directors are responsible to ensure that the product has been vetted through the County's Cybersecurity Governance process and follows all the confidentiality, integrity, and availability requirements based on the data privacy requirements.

6. Policy

6.1. Purchasing, Configuring, Developing, Operating, or Maintaining AI Systems

6.1.1. When purchasing, configuring, developing, operating, or maintaining AI systems, the County will:

6.1.1.1. Uphold the Guiding Principles for Responsible AI Systems,

6.1.1.2. Conduct an AI Review to assess the potential risk of AI systems. The CIO is responsible for coordinating review of AI systems used by the County,

6.1.1.3. Obtain technical documentation about AI systems by creating documentation if internally developing the AI system.

6.1.1.4. In the event of an incident involving the use of the AI system, the County will follow an Incident Response Plan as detailed in the County's Cybersecurity Response Policy. The CIO or designee is responsible for overseeing the security practices of AI systems used by or on behalf of County departments.

6.2. AI Notetaking Guidelines

6.2.1. **Transparency:** Transparency regarding the use of AI note-takers instills trust. Clearly state the purpose of note-taking and specify the AI tool being used.

6.2.2. **Meeting host responsibilities:**

6.2.2.1. The meeting organizer determines the use of AI note-taking

6.2.2.2. Informing participants of a meeting that AI note-takers will be used is essential. Participants should be clearly notified about the process and purpose of using the technology.

6.2.2.3. The notes taken with Generative AI tool should be shared with all the participants and accuracy is verified before it is released.

6.2.2.4. Any objection to the usage of Generative AI tool for notetaking should be carefully considered and vetted with the attendees before the tool is used.

6.2.2.5. If an objection exist, alternative note-taking methods should be explored and considered.

6.2.3. **Information security:** Sensitive data must be handled securely. Adhere to Federal law, State law, and *when applicable but not limited to,* Harris County policies regarding storage, access, and retention periods.

6.2.4. **Accuracy:** AI notes may contain errors and should be reviewed for accuracy before wide-spread distribution.

6.3. Verification is crucial, particularly for high-stakes decisions.

6.3.1.1. If meeting notes are kept for the purpose of documenting the meeting (as opposed to personal notes), they should be reviewed by the host, verified by participants, and formally approved by the represented group.

6.3.1.2. Be aware of potential biases in AI algorithms and take steps to mitigate them. Ensure summaries are fair and representative of all participants.

6.3.1.3. AI notes should summarize the meeting content objectively

6.3.1.4. Private conversations or irrelevant details should be removed.

6.4. **Accessibility:** Ensure accessibility to AI notes for all participants, considering potential disabilities or preferences for non-digital formats.

6.5. Prohibited Uses

6.5.1. The use of certain AI systems is prohibited due to the sensitive nature of the information processed and severe potential risk. This includes, but not limited to, the following prohibited purposes:

6.5.1.1. Real-time and covert biometric identification,

6.5.1.2. The use of computer vision techniques to classify human facial and body movements into certain emotions or sentiment (e.g., positive, negative, neutral, happy, angry, nervous),

6.5.1.3. Fully automated decisions that do not require any meaningful human oversight but substantially impact individuals,

6.5.1.4. Social scoring, or the use of AI systems to track and classify individuals based on their behaviors, socioeconomic status, or personal characteristics,

6.5.1.5. Cognitive behavioral manipulation of people or specific vulnerable groups,

6.5.1.6. Autonomous weapons systems.

6.5.2. When using AI systems, all users must also abide by the Harris County Personnel and Policies & Procedures Manual, Section 7: County Property and Electronic Services Policy approved by Commissioners Court.

6.5.3. If County staff become aware of an instance where an AI system has caused harm, staff must report the instance to their supervisor and the Harris County Universal Services at 713-755-6624 or helpdesk@us.hctx.net.

6.6. Public Records

6.6.1. The County is subject to the Texas Public Information Act and must follow all current procedures for records retention and disclosure.

6.7. Policy Enforcement

6.7.1. This policy applies to all GenAI used by Elected and Appointed officials, County employees, (full-time, part-time, temporary), contractors, vendors, volunteers, temporary agency staff or others while performing a role for the County (collectively "users"). It is noted that judicial records are governed by the State of Texas Judicial Administration Rule 12. [https://www.txcourts.gov/media/524153/rjac-rule-12.pdf]

6.7.2. All users must follow this policy. Failure to comply with the policy can result in a loss of access to the County network. Disciplinary action, up to and including termination of employment, contracts and/or other relationships will be handled by the user's department head or elected official. Additionally, legal action may be taken in response to violations of applicable regulations and laws.

6.7.3. If HCUS determines that a department is in violation of the policy and the violation poses a high risk to the County network, the department may be temporarily disconnected from the County network until the risk is mitigated.

7. Violations of the AI Policy

7.1. Violations of any section of the AI Policy may be subject to disciplinary action, up to and including termination. Violations made by a third party while operating an AI system on behalf of the County may result in a breach of contract and/or pursuit of damages. Infractions that violate local, state, federal, or international law may be remanded to the proper authorities.

8. Terms and Definitions

8.1. Algorithm: A series of logical steps through which an agent (typically a computer or software program) turns particular inputs into particular outputs.

8.2. Artificial Intelligence or "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.

8.3. AI system: Any system, software, sensor, or process that automatically generates outputs including, but not limited to, predictions, recommendations, or decisions that augment or replace human decision-making. This extends to software, hardware, algorithms, robotic applications, tools, and utilities that operate in whole or in part using AI and data generated by these systems. AI is often used to automate large-scale processes or analyze large data sets.

8.4. Generative Artificial Intelligence or "GenAI": Artificial intelligence models that can create new content such as text, images, music, or code, based on patterns learned from existing data. It uses techniques like deep learning and neural networks to generate human-like responses.