RTC Management Policy P-XX
Date Approved: TBD

MANAGEMENT POLICY

SUBJECT: ARTIFICIAL INTELLIGENCE (AI) TECHNOLOGIES

I. PURPOSE

The purpose of this policy is to guide the responsible use of Artificial Intelligence (AI) technologies within the Regional Transportation Commission (RTC). AI technologies can be used to enhance work and work product, but must be used in a way that ensures data security and is transparent and ethical.

II. SCOPE

Public
Board Members
RTC Officers
X RTC Employees
Other: _____

III. DEFINITIONS

A. Artificial Intelligence (AI) – Technology that leverages large volumes of data and machine learning techniques to produce content based on user inputs.

B. Generative AI – AI that can be used to create (or generate) new content such as text, images, music, audio, and video.

C. Large Language Model (LLM) – A type of AI that uses machine learning to understand and generate human-like text based on large datasets.

D. Open LLM – An AI model available for public use, which can be utilized for various purposes but with higher risks related to data security.

E. Closed LLM – An AI model specifically designed and restricted for use within RTC, ensuring data security and tailored to RTC's needs.

F. Meeting AI Tools – AI tools that transcribe and analyze recordings of meetings for various purposes, including note-taking, action item tracking, and preparing meeting minutes.

G. Personally Identifiable Information[1] – Data or information that, alone or in combination with other information, could be used to identify a person or an electronic device used by the person, such as the name, address, telephone number, date of birth, and directory information of a person. The disclosure of personally identifiable information can potentially create negative consequences for the person, such as financial loss, stigmatization, harm to reputation, anxiety, embarrassment, fear or other physical or emotional harm. RTC is required to maintain a list of the records and portions of records determined to be confidential because they contain personally identifiable information. NRS 239.014(2).

IV. POLICY

A. General

1. The RTC is committed to harnessing AI technologies responsibly and ethically to enhance public services, foster innovation, and benefit our community.

2. AI tools must be used in a manner that protects the privacy of individuals and complies with applicable federal and state laws regarding data protection. An example of a federal law would be the Health Insurance Portability and Accountability Act (HIPPA). An example of a state law would be a statute that declares records or portions of records to be confidential,[2] or a statute or other legal authority pursuant to which RTC has determined that a record or a portion of a record to be confidential.[3]

3. Data Protection

   a. Data and other information entered into a Generative AI tool, and content generated by a Generative AI tool, could be public records and may be subject to a records request under NRS Chapter 239.

   b. Data and other information entered into a Generative AI tool may be viewable and usable by the company that provides the AI tool, and could be leaked unencrypted in a data breach.

[1] This term was developed based on the definition of "personally identifiable information" in NRS 239.014(5), and the extent to which RTC may determine that records or portions of records containing personally identifiable are confidential under Nevada law.
[2] For example, NRS 332.061 declares that "proprietary information" is confidential.
[3] For example, RTC may determine that a record or a portion of a record is confidential if a common-law balancing of interests test shows that the public interest in disclosure is outweighed by other public policy interests, such as privacy, the ability of the agency to perform its function, or other public policy concerns. *Donrey of Nevada, Inc. v. Bradshaw,* 106 Nev. 630 (1990).

c. Users must not enter any data or information into a Generative AI tool that should not be available to the general public, such as personally identifiable information and other potentially confidential information.

d. Users must consult with legal counsel if they have any question about whether data or information should be available to the general public.

4. Users must review, revise, and independently fact-check (via multiple sources) any content generated by a Generative AI. Users cannot rely on the accuracy or quality of content generated by a Generative AI tool. Users are responsible for the work and work product they produce with the support of Generative AI tools.

B. Open LLM

1. Use Guidelines: Open LLMs can be used for drafting documents, generating ideas, and summarizing text. However, users must:

a. Avoid including any sensitive, confidential, or personally identifiable information in prompts.

b. Verify the accuracy of content generated by AI tools before using it in official documents.

c. Ensure compliance with applicable law.

2. Security Measures: Users must follow RTC Management Policy P-40 – Information Technology Acceptable Use, ensuring no unauthorized software is downloaded and that the AI tool complies with RTC's data security standards.

C. Closed LLM

1. Implementation: RTC may implement Closed LLMs to handle specific use cases within RTC, such as content related to historical board meeting materials, internal policies and procedures, and projects.

2. Data Security: The data and information processed by closed LLMs will be securely stored and managed according to RTC Management Policy P-40 – Information Technology Acceptable Use and RTC’s data security standards.

3. Users must verify the accuracy of content generated by Closed LLMs before using it in official documents.

D. Meeting AI Tools

1. Recording Use: Meeting AI Tools may be used to transcribe and analyze participation at meetings to improve note-taking, track action items, and prepare meeting minutes.

2. Usage Conditions:

   a. Users may only use Meeting AI Tools that allow the user to have sole access to the content generated. Users may not use Meeting AI Tools that send the content to participants or others, or that allow participants or others to access the content. The user can then decide how to use the content, and who to share the content with.

   b. Users must receive approval from both the Executive Director and legal counsel prior to using Meeting AT Tools.

3. Notice to Participants: Meeting participants must be informed in advance of the meeting that Meeting AI Tools will be used, and must be informed at the beginning of the meeting that Meeting AI Tools are being used.

4. Employee Concerns: If an employee has concerns about participating in a meeting where Meeting AI Tools will be used or have been used, the employee should share those concerns with their supervisor, department director, or the Administrative Services Director.

5. Users must verify the accuracy of content generated by Meeting AI Tools before using it in official documents.

- END -