METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

INFORMATION SECURITY POLICY

	POLICY NUMBER: ISM 20
SUBJECT: ARTIFICIAL INTELLIGENCE (AI) AND GENERATIVE AI (GENAI) POLICY	DISTRIBUTION DATE: 4/15/2024
	EFFECTIVE DATE: 4/15/2024
ISSUING AUTHORITY: Director of Information Technology Services of the Metropolitan Government of Nashville and Davidson County	EXPIRATION: 8/1/2025

PURPOSE

This purpose of this policy is to inform users of the Metropolitan Government of the acceptable use of Artificial Intelligence (AI), including Generative Artificial Intelligence (GenAI), within Metropolitan Government. This policy is intended to promote the safe and responsible use of Artificial Intelligence and Generative AI, while also protecting Metro, and the privacy and security of our users and residents.

The Metropolitan Government recognizes that the use of AI solutions has the potential to provide significant benefits to Metro users by enabling them to work more effectively and efficiently. In cases where the use of AI can help users to do so, users are allowed to use AI technologies in accordance with the policies and guidelines set forth in this policy. The use of AI should always be subject to careful consideration and evaluation to ensure that it aligns with Metropolitan Government's values, goals, and best practices, including the Metropolitan Government's Artificial Intelligence goals:

- **Accountability**: to ensure AI systems have a human owner responsible for system oversight, accountability and measuring accuracy.
- **Accuracy**: to deploy AI systems that have a high accuracy rate.
- **Equity**: to use AI in alignment with its commitment to equity and reducing racial and socioeconomic disparities.
- **Security**: to ensure security and data privacy is provided in all AI systems.
- **Transparency**: to provide information about the AI systems it uses to the public so that they are informed.
- **Utility**: to adopt AI systems that will have a useful and positive impact on residents and the delivery of services.

This policy applies to any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI. This includes, but is not limited to, AI used in standalone AI solutions, the use of AI APIs, and AI embedded in other software, such as those using machine learning (ML).

DEFINITIONS

Certain capitalized terms used in this policy have specific meanings as defined in the *Glossary* section below.

POLICY

1. In General

1.1. No data classified as Confidential or Restricted shall be provided to GenAI that are not purpose built for Metropolitan Government use in a prompt or as part of the learning data.

1.2. All AI and GenAI use shall encourage and promote inclusive growth, fairness, non-discrimination, human-centered values, transparency, safety and security, and accountability.

1.3. All AI and GenAI use shall comply with relevant data privacy laws and shall not violate any intellectual property use. This requirement includes ensuring that training data is legally obtained, and its use is legal and licensed appropriately.

1.4. Use of AI and GenAI shall comply with all applicable public records laws, including the *Tennessee Public Records Act* . This requirement extends to all data that is deemed to be requestable under that act.

1.5. All content generated by AI and GenAI shall be reviewed by a human reviewer prior to being used for accuracy and bias, also known as “human in the loop (HITL)”.

1.6. Content generated by AI and GenAI that is used communications, decision making, etc. shall be cited and disclosed as such in applicable labels or communications if the contribution is significant or a substantial portion of the content used in the final version comes from the GenAI. For example, in a footer or clearly marked disclosure statement.

1.7. Any use of embedded AI within a vendor managed and hosted solution shall be disclosed to the applicable Metropolitan Government Director or Agency Head and the Metropolitan Government’s Chief Information Officer.

1.8. Any use of GenAI to author official Metropolitan Government documentation, including communications, shall be disclosed to the applicable Metropolitan Government Director or Agency Head.

1.9. Any decisions made by AI or made using AI generated content shall be transparent and their decisions can be explained and understood by residents. Transparency is the clear, understandable disclosure of AI system’s functions, data use and decision-making processes. Explainability is the ability to describe an AI system’s processes and decisions clearly and easily in understandable terms. Any use of AI and GenAI shall have a mechanism for reporting inaccuracies or concerns with outputs.

1.10. Any use of AI shall have defined metrics, when possible, to evaluate accuracy, performance and/or impact of the AI solution.

1.11. Fully automated decisions that do not require any meaningful human oversight by that may substantially impact residents is prohibited.

1.12. AI shall not be used to generate or alter human likenesses and voices in a manner that appears realistic, i.e., deepfakes, for the purpose of deception, spreading misinformation, or other malicious or unlawful purposes.

2. Training and Awareness

Metropolitan Government shall provide training to applicable staff on the responsible use of AI and GenAI technologies, emphasizing security, ethics, respect for intellectual property rights and privacy considerations.

3. Evaluation and Procurement

   Metropolitan Government shall conduct a thorough evaluation using established processes and procedures before acquiring any AI or GenAI solution. Evaluation criteria shall include:
   - Assessing the vendor's reputation for security, reliability and respecting intellectual property rights.
   - Evaluating the solution's compatibility with existing systems.
   - Ensuring compliance with relevant data privacy laws. Reviewing the vendor's commitment to responsible AI.

   Procurement decisions shall prioritize vendors that prioritize security, privacy, respect for intellectual property rights and transparency in their AI solutions. Appropriate language shall be added to contracts to address vendor's obligations.

4. Generative AI Acceptable Use

   Generative AI shall be used for:
   - research purposes, such as generating new ideas or prototypes,
   - artistic or creative purposes, such as drafting original content for marketing campaigns or advertising, and
   - training and development purposes, such as creating simulated scenarios for employee training.
   - consultation in decision-making processes such as determining response configurations, verifying information, recommended staffing levels, etc., provided outputs are reviewed by a human reviewer.

5. Generative AI Unacceptable Use

   Generative AI shall not be used:
   - as the sole basis for decision-making processes, such as determining eligibility for employment, housing, personnel decisions, or financial services,
   - for any information, images, or data being shared with the public without first being reviewed, transformed, and edited by humans for public consumption or cited as being generated by AI,
   - to generate content that violates Metropolitan Government code of conduct, policies, or any applicable laws, and
   - for the generation of computer code to be utilized in Metro's production environments as written. It may only be used for proof of concepts and idea generation but shall undergo a detailed review prior to any use.

GLOSSARY

- *Artificial Intelligence (AI)* - Interdisciplinary field, usually regarded as a branch of computer science, dealing with models and systems for the performance of functions generally associated with human intelligence, such as reasoning and learning. (SOURCE: NIST)
- *Artificial General Intelligence* – strong artificial intelligence, theoretical form of AI where machine would have intelligence equal to humans and exhibit a self-aware consciousness that has the ability to solve problems, learn, and plan for the future. (SOURCE: IBM).
- *Deepfake* - the creation and manipulation of audiovisual media using advanced artificial intelligence and machine learning technologies, particularly deep learning, to generate or alter human likenesses and voices in a manner that appears realistic. This includes, but is not limited

to, the synthesis of human facial and vocal characteristics to create entirely new, false representations or the alteration of existing media to create misleading or untruthful portrayals. The term encompasses both the technology used for such purposes and the resultant media. (SOURCE: IBM).

- *Generative Artificial Intelligence (GenAI)* - [a kind of artificial intelligence] capable of generating new content such as code, images, music, text, simulations, 3D objects, videos, and so on. Examples of generative AI technologies are Bard, ChatGPT, and AutoGPT. (SOURCE: IBM)
- *Machine Learning (ML)* – a subset of AI, the study or the application of computer algorithms that improve automatically through experience. Machine learning algorithms build a model based on training data to perform a specific task, like aiding in prediction or decision-making processes, without necessarily being explicitly programmed to do so. (SOURCE: NIST)

CONTACT

Questions should be directed to (615) 862-6222 or by email at ciso@nashville.gov

SIGNATURE

Keith Durbin
Chief Information Officer/Director of ITS
Metropolitan Government of Nashville and Davidson County

REFERENCES

- AI Principles from Microsoft
- AI Principles from Google
- NIST AI Risk Framework
- Gartner: Generative AI Policy Template
- AI Policy Template from City of San Jose Government AI Coalition
- City of Boston Interim Guidelines for Using Generative AI
- City of San Jose INFORMATION TECHNOLOGY DEPARTMENT GENERATIVE AI GUIDELINES

REVISION HISTORY

REVISION	DATE	CHANGES
0.1	8/2/2023	DRAFT
1.0	4/15/2024	Initial Release