



METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY INFORMATION SECURITY POLICY

POLICY NUMBER: ISM 20

SUBJECT: ARTIFICIAL INTELLIGENCE (AI) AND Generative AI (GENAI) POLICY

ISSUING AUTHORITY: Freddie O'Connell Executive Order No. 37

DISTRIBUTION DATE: 4/15/2024

EFFECTIVE DATE: 4/15/2024

EXPIRATION: UNTIL RESCINDED

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 all Metropolitan Government employees, elected officials' staff, contractors, consultants, temporary workers, vendors, service providers, cloud providers, and other third parties who use, access, develop, procure, integrate, or manage AI solutions on behalf of Metropolitan Government.

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, AI embedded in other software, such as those using machine learning (ML), open-source AI solutions, internally developed AI solutions, third-party AI solutions, embedded AI functionality, AI

agents, large language models, large action models, machine learning models, and future technologies that mimic human reasoning, content generation, decision support, or operational task execution.

DEFINITIONS

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

POLICY

1. In General

- 1.1. The Metropolitan Government shall maintain an AI governance process responsible for reviewing AI solutions, approving permitted uses, maintaining an approved AI solutions list, reviewing exceptions, and issuing supporting standards, procedures, and guidance.
- 1.2. Users shall not create accounts, authenticate, connect, or integrate AI solutions using Metropolitan Government credentials, email addresses, single sign-on, data, systems, or devices unless the AI solution has been approved through the AI risk assessment process.
- 1.3. 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.
- 1.4. All AI and GenAI use shall encourage and promote inclusive growth, fairness, non-discrimination, human-centered values, transparency, safety and security, and accountability.
- 1.5. 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.
- 1.6. 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)”.
- 1.7. 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.



- 1.13. Users shall remain responsible for all prompts submitted, outputs used, and work products created with GenAI assistance. Gen AI shall not replace professional judgment, required review, supervisory approval, or accountability for official work.
- 1.14. AI-based transcription, recording, summarization, meeting assistant, or notetaking tools shall comply with applicable Metropolitan Government standards for recording, transcription, participant notice, consent, accuracy review, retention, vendor restrictions, deletion, and incident reporting.
- 1.15. Embedded AI functionality in vendor-managed or hosted solutions shall be disclosed and reviewed when required by Metropolitan Government policy, procurement procedure, security review, or AI governance process.
- 1.16. AI-enabled systems that support critical business functions, public-facing services, public safety, cybersecurity, financial operations, human resources, infrastructure, or legally mandated services shall be evaluated for business continuity, disaster recovery, availability, resilience, vendor dependency, data portability, and manual fallback procedures.
- 1.17. AI shall not be used for fully automated decisions that do not include meaningful human oversight and that may substantially impact residents, employees, applicants, vendors, benefits, enforcement actions, access to services, eligibility, employment, housing, public safety, financial interests, or legal rights are prohibited.
- 1.18. AI integrations, agents, plugins, and connected applications shall use least privilege, need-to-know access, separation of duties, approved authentication methods, logging, monitoring, and periodic access review. AI tools shall not be granted broad access to email, calendars, file repositories, source code, service desks, databases, or collaboration platforms unless specifically approved for the use case and data classification.

2. Risks of AI Usage

AI use may create risks including inaccurate or fabricated outputs, biased or discriminatory results, exposure of confidential or restricted data, intellectual property or licensing violations, harmful or misleading content, overreliance on automated recommendations, public-records and retention issues, vendor lock-in, and reduced public trust. Users and departments shall identify and mitigate these risks before relying on AI for official business.

3. Request, Review, and Approval

- 3.1. Users shall complete the applicable request, review, and approval process before using any AI solution for Metropolitan Government business when required by this policy, Metropolitan Government procedure, procurement requirements, data classification, or risk level. This requirement includes connecting GenAI tools to Metropolitan Government email, calendar, file repositories, collaboration tools, source code repositories, service desks, databases, or other systems unless the integration has been reviewed and approved by Metropolitan Government Information Technology Services (ITS) and any required data protection terms are in place.
- 3.2. Approved use shall be limited to the specific solution, platform, account type, business purpose, data classification, output type, integration, and risk conditions identified in the approved request.
- 3.3. Directors, Agency Heads, Elected Officials or their designees shall ensure approved use is necessary for official business, aligns with Metropolitan Government guidance, includes appropriate human review, and is discontinued or re-reviewed when the business need, tool, data type, or risk profile changes.



- 3.4. An AI risk assessment shall be completed when required, including new solutions, sensitive use cases, public-facing services, decision support, integrations with Metropolitan Government systems, use with non-public information, or other higher-risk use.

4. Data Classification and Prohibited Inputs

- 4.1. Users shall understand the classification of information before entering, uploading, pasting, summarizing, transcribing, analyzing, or otherwise providing information to an AI or GenAI solution.
- 4.2. Users shall not enter, upload, paste, summarize, transcribe, or otherwise disclose Restricted, Confidential, sensitive, private, legally privileged, protected health information, criminal justice information, procurement-sensitive information, credentials, passwords, API keys, tokens, security architecture details, nonpublic vendor information, or other nonpublic Metropolitan Government information unless the solution has been formally approved for that data classification and use case.
- 4.3. Users shall not upload source code, configuration files, credentials, keys, tokens, vulnerability information, network diagrams, incident details, or security-sensitive information to an AI or GenAI solution unless the solution has been approved for that exact use and data classification

5. Public Records, Retention, and Archiving

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.

- 5.1. Prompts, outputs, uploaded files, generated images, audio, video, transcripts, AI interaction history, metadata, and related work products may constitute public records when created, received, retained, or controlled in connection with official Metropolitan Government business.
- 5.2. Users shall comply with applicable records retention, legal hold, e-discovery, public records, and department procedures for GenAI prompts, outputs, and related records.
- 5.3. Prompts and outputs shall be archived when required by Metropolitan Government, the Department of Law, a records request, a legal hold, department procedure, or the approved use case.
- 5.4. Users are responsible for reviewing and redacting any records that are requestable under the Tennessee Public Records Act.
- 5.5. Records shall not be retained longer than 10 days unless retention is required by law, policy, litigation hold, public records request, records schedule, or other applicable records guidance.

6. 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.



7. Evaluation and Procurement

- 7.1. Users and departments shall review and understand applicable terms of use, privacy terms, data retention terms, ownership terms, licensing terms, and vendor data practices before using an AI solution.
- 7.2. Users shall opt out of model training, chat history retention, or vendor data collection when the platform provides that option, unless retention is required by an approved enterprise configuration, contract, legal requirement, or records requirement.
- 7.3. Metropolitan Government data shall not be used by a vendor to train AI models unless specifically authorized by contract and approved by Metropolitan Government Information Technology Services and the Metropolitan Government Department of Law.
- 7.4. AI solutions shall not be used if the applicable terms, privacy practices, security controls, or licensing conditions are inconsistent with Metropolitan Government requirements or the approved business purpose.
- 7.5. 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.
- 7.6. Procurement decisions shall prioritize vendors that prioritize security, privacy, respect for intellectual property rights and transparency in their AI solutions.
- 7.7. Metropolitan Government shall develop a process to add appropriate language to contracts to address vendor's obligations.

8. Accuracy, Human Review, and Disclosure

- 8.1. AI-generated content shall be fact-checked and independently verified before use in official materials, public communications, analysis, recommendations, decision support, or other Metropolitan Government work products.
- 8.2. AI-generated facts, citations, links, legal interpretations, statistics, calculations, summaries, translations, and code shall not be assumed to be accurate.
- 8.3. AI-generated content shall be reviewed for bias, inappropriate language, accessibility concerns, branding concerns, and potential harm before use, distribution, publication, or reliance.
- 8.4. Use of GenAI shall be cited or disclosed when AI made a substantial contribution, had a distinctive impact on the work, was copied verbatim, was used to generate images, video, or audio, was used for data analysis, or otherwise materially shaped official content.



- 8.5. Facts and figures in official materials shall cite credible primary or supporting sources rather than the AI tool itself.
- 8.6. A mechanism shall exist, when practical, for reporting inaccuracies, concerns, or harmful outputs associated with AI-assisted content used in official Metropolitan Government business

9. GenAI Acceptable Use

GenAI 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.

10. GenAI Unacceptable Use

GenAI 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 can 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 GenAI 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



John Griffey
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: GenAI Policy Template
- [AI Policy Template from City of San Jose Government AI Coalition](#)
- [City of Boston Interim Guidelines for Using GenAI](#)
- [City of San Jose INFORMATION TECHNOLOGY DEPARTMENT GENAI GUIDELINES](#)
- NIST Artificial Intelligence Risk Management Framework
- NIST Cybersecurity Framework 2.0
- NIST Special Publication 800-53 Rev. 5
- NIST Special Publication 800-171 Rev. 3
- 200-POL-007 *Enterprise Artificial Intelligence Policy* – State of TN AI policy

REVISION HISTORY

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



1/1	7/3/2026	Addition of the following sections: 1.1, 1.2, 1.13-1.18 <i>2.0 Risks of AI Usage</i> <i>3.0 Request, Review, and Approval</i> <i>4.0 Data Classification and Prohibited Inputs</i> <i>5.0 Public Records, Retention, and Archiving</i> <i>7.0 Evaluation and Procurement</i> <i>8.0 Accuracy, Human Review, and Disclosure</i>
-----	----------	---

