District of Columbia Government – Office of the Chief Technology Officer

AI/ML Governance Policy

Policy Number:	**Approval Date:**	**Effective Date:**
Approved by _______________________________ _ **Chief Technology Officer**	**Review by Legal Counsel:** ______________________________ _ **General Counsel**	**TBD**

1. **Purpose**
This Policy aims to establish guidelines for the responsible and secure usage of Artificial Intelligence (hereafter referred as AI) and Machine Learning (hereafter referred as ML) technologies within the District of Columbia Government (hereafter known as District) and protect the District's assets, workforce, residents, businesses and visitors from risks that may result from the inappropriate use or bias. The policy covers users, developers, and administrators and focuses on privacy, cybersecurity, and data protection, particularly concerning the usage of non-enterprise or free AI and ML platforms.

2. **Authority**
DC Official Code § 1-1401 et seq., provides the Office of the Chief Technology Officer ("OCTO") with the authority to provide information technology (IT) services, write and enforce IT policies, and secure the network and IT systems for the District. This document can be found at*: https://code.dccouncil.us/dc/council/code/sections/1-1402.html*.

3. **Applicability**
This policy applies to all District workforce members responsible for application identity and role definition on behalf of the District, and/or any District agency/District/entity who receives enterprise services from OCTO. In addition, this policy applies to any provider and third-party entity with access to District information, systems, networks, and applications.
This Policy also applies to any provider and third-party entity with access to the District's information, networks, and applications.

4. **Policy**

4.1. General Guidelines

4.1.1. Follow AI/ML Adoption and Usage Guidelines published by OCTO at: https://octo.dc.gov/page/aiml-adoption-andor-usage-guidelines

4.1.2. Users, developers, and administrators should only use AI and ML technologies and/or platforms approved by OCTO or Agency Information technology division to ensure security, data protection, and regulatory compliance.

4.1.3. Written approval of the Agency Director or their designee must be obtained prior to utilizing Agency data with any AI and/or ML technologies or platforms.

4.1.4. Define roles and responsibilities of individuals and teams involved in AI/ML development, deployment, and monitoring.

4.1.5. Establish a governance board or committee responsible for overseeing AI/ML risk management.

4.1.6. Adequate auditing and logging mechanisms should be implemented to monitor the usage of AI and ML technologies.

4.1.7. Prior to using any AI and ML platforms, a cyber and business risk assessment must be performed to evaluate the potential risks associated with data protection, and compliance with relevant regulations.
4.1.8. Implement measures to detect and mitigate biases in data, algorithms, and decision-making processes.
4.1.9. Regularly monitor and evaluate AI/ML systems for fairness across different user groups.
4.1.10. Agencies should provide education and training programs to their employees involved in AI/ML initiatives.
4.1.11. Any known or suspected policy violations or security incidents related to AI and ML technologies must be immediately reported to SOC (soc@dc.gov) and Agency CIO.

4.2. Data Privacy and Protection
4.2.1. All AI and ML activities must comply with applicable privacy laws and regulations, including the organization's data protection policies.
4.2.2. Open Data must be utilized when experimenting with AI and ML technology.
4.2.3. Agency's exploring AI/ML tools or platforms should not use data classified higher than "Level 0" as defined in the DC Data Policy.
4.2.4. Anonymized or de-identified data should be used for AI and ML purposes if utilizing production data on commercial platforms or vendor proof of concepts.
4.2.5. Define guidelines for data collection, storage, and usage to ensure compliance with privacy regulations, data protection, and data quality standards.
4.2.6. Rigorously validate and test your AI/ML models before deploying them.
4.2.7. Implement robust evaluation methods to assess performance, fairness, and potential risks associated with the models.
4.2.8. Ensure proper data governance practices are in place, including data quality control, data privacy, and security measures.
4.2.9. Be aware of biases and potential discrimination in the data used for training ML models.

4.3. Unauthorized Uses and Specific Prohibitions
4.3.1. The usage of non-enterprise or free AI and ML platforms is discouraged, as they may pose potential risks to data security and privacy.
4.3.2. Unauthorized creation, transmission, or usage of AI and ML generated content.
4.3.3. Unauthorized sharing or uploading of DC Agency data to third-party platforms.
4.3.4. Sharing Personal or sensitive data without appropriate consent.
4.3.5. Utilizing AI and ML tools to bypass security and/or regulatory controls.
4.3.6. Integrating public facing or internal application with AI platforms without proper disclosure.
4.3.7. Create or re-create content that violates copyright and/or violates the District Government ethical standards.
4.3.8. Create materials related to illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited, etc.

4.4. Cyber Security and Continuous Monitoring
4.4.1. Implement mechanisms for continuous monitoring and evaluation of AI/ML systems to identify and address emerging risks.
4.4.2. Establish processes for auditing, reporting, and addressing non-compliance.
4.4.3. Regularly review and update the risk management framework to adapt to changing technological, regulatory, and organizational requirements.
4.4.4. Implement robust security measures to protect AI/ML systems from adversarial attacks, data breaches, and unauthorized access.
4.4.5. Regularly assess vulnerabilities and apply appropriate security patches and updates.

5. **Exemption**s

Exceptions to this policy shall be requested in writing to the Agency CIO and the request will be escalated to the OCTO Chief Information Security Officer ("CISO").

6. Definitions

The definition of the terms used in this document can be found in the Glossary section of the OCTO Policy Website and appendix 1 below.

7. Sanctions

To safeguard District Government technology and other resources, violators of this policy may be denied access to District Government computing and network resources and may be subject to other disciplinary action within District Government. Violators of this policy will be handled in accordance with the District Government's established disciplinary procedures and/or applicable Collective Bargaining Agreement. OCTO may suspend, block, or restrict access to computing resources and accounts, independent of such procedures, when it reasonably appears necessary to do so to protect the integrity, confidentiality, or availability of District Government computing and network resources, or to protect the District Government from liability.

7.1. If violations of this Policy are discovered that are illegal activities, the District Government may notify appropriate authorities.

7.2. The District Government reserves the right to pursue appropriate legal actions to recover any financial losses suffered because of the violations of this policy.

8. References

9.1. NIST Special Publication (SP) 800-53 Revision 4 – Security and Privacy Controls for Federal Information Systems and Districts (April 2013).

9.2. NIST Special Publication (AI) 100-1

9. Revision History.

Date	Reviewed by	Action	Effective Date	Next Review Date

10. Contact Information

Questions concerning this policy may be directed to the Office of the Chief Technology Officer at the 202-727-2277 or infosecpolicy@dc.gov.

APPENDIX

Appendix 1 – Terms and Definitions:

Term	Definition
District Government Information Systems	Technology systems owned or paid for by District Government funds, including, but not limited to Internet/Intranet/Extranet-related systems, computer and other digital equipment, software, operating systems, storage media, network accounts providing electronic mail and other messaging, and systems that enable web browsing, and file transfer. Source: OCTO
District Government Workforce	Individuals who perform District Government functions and who are classified as employees, volunteers, contractors, and interns. Source: OCTO
District Government Technology Resources	Technology resources owned or paid for by District Government funds, including, but not limited to: Internet/Intranet/Extranet-related systems, computer and other digital equipment, software, operating systems, storage media, network accounts providing electronic mail and other messaging, and systems that enable web browsing, and file transfer. Source: OCTO
AI	Artificial Intelligence (AI) refers to the capability of a device to perform functions that are normally associated with human intelligence such as reasoning, learning, and self-improvement. Source: NIST
ML	Machine Learning (ML) refers to the ability of systems to learn and improve from available data without explicit programming. Source: OCTO
Enterprise AI and ML Platform	The enterprise AI and ML platform refers to the authorized, licensed, or internally developed AI and ML technologies approved for use within the organization.
Non-Enterprise or Free AI and ML Platforms	Non-enterprise or free AI and ML platforms refer to external platforms or tools not officially sanctioned or approved by OCTO or your Agency for AI and ML purposes.