WASHINGTON COUNTY
Community Development Agency

7645 Currell Boulevard, Woodbury, MN 55125
office: 651-458-0936 fax: 651-458-1696

Artificial Intelligence (AI) Acceptable Use Policy

Purpose

The purpose of this policy is to establish clear standards for the acceptable and responsible use of Artificial Intelligence (AI) applications for CDA business. This policy ensures that AI tools and services are used in a manner that advances CDA objectives, strengthens operational efficiency, enhances service delivery, and complies with all relevant policies, laws, and security requirements. With the quick advancement of AI technologies, the application of this policy will require constant review and interpretation.

Scope

This policy applies to:

- All employees who access or use AI systems on behalf of the organization.
- All CDA devices, networks, accounts, systems, programs, and software where AI is available.
- Both internal and external AI tools, including generative AI platforms, machine learning applications, and automation systems.

Definitions

- Artificial Intelligence (AI): Technologies and systems that perform tasks normally requiring human intelligence, such as natural language processing, predictive analytics, or machine learning.
- Generative AI: AI applications that produce content such as text, images, video, or code.
- Sensitive Data: This includes any information that is considered private, confidential, nonpublic, or private nonpublic data, such as data regulated by MN Data Practices, HIPAA, GDPR, or PCI standards. Sensitive Data includes, but is not limited to, information that could be used to identify an individual customer or vendor.
- AI Systems: Any software or service that uses AI to analyze information and generate outputs such as text, images, summaries, predictions, or recommendations.

- Web-Based AI Applications: External AI tools that are not licensed or managed by CDA.
- Licensed AI Applications: Internal AI tools that integrate with CDA systems, authenticate using CDA credentials, and are capable of processing internal data.

Terms of Use

Data Protection

To protect CDA data and ensure compliance with privacy requirements, employees must follow these safeguards when using AI systems:

- Employees must never enter or input Sensitive Data into AI systems.
- AI use must comply with the CDA's General Standards of Conduct; please refer to Section 5 of the Employee Handbook for further guidance and information.
- When in doubt, treat information as Sensitive Data, do not enter it into AI systems, and consult the IT Manager or Administration Director.

Compliance with Laws and Regulations

To ensure all AI activities meet legal and contractual requirements, employees must follow the guidelines below:

- All use of AI must adhere to applicable laws, regulations, licensing agreements, and intellectual property rights.
- Plagiarism, misrepresentation, or uncredited use of AI-generated content is prohibited.

Ethical and Responsible Use

To uphold the CDA's standards of professionalism and to prevent harm, all AI use must follow these ethical and responsible use expectations:

- AI must not be used to generate misleading, discriminatory, offensive, fraudulent, or harmful content.
- AI must not be used to create or spread misinformation.
- AI must not be used to interpret regulatory or statutory language. Such interpretation requests should be made to a supervisor or CDA legal counsel, as applicable.

Accuracy and Oversight

To maintain the quality and integrity of CDA deliverables, employees must carefully review and validate all AI-generated outputs before using or sharing them:

- Employees must carefully examine and verify any content produced by AI systems before relying on it in any way. This means confirming that the information is factually accurate based on verification of primary source documentation, complete, aligned with CDA policies, and appropriate for the intended audience.
- Employees are responsible for ensuring the quality, accuracy, and appropriateness of any work produced with the assistance of AI.
- AI-generated outputs must follow the same approval process as outputs not generated by AI before being distributed to internal or external audiences.

Approval of New AI Applications

To maintain security, compatibility, and compliance, licensed AI applications must go through the established review and approval process before use:

Submitting the Request

- The employee identifies the need for an AI application and submits a request to their supervisor for consideration.

Supervisory Review

- The supervisor reviews the request to determine whether the proposed application is appropriate and aligns with the department's operational needs, CDA's strategic objectives, and meets budget requirements. The supervisor may request additional information or clarification, if necessary, before determining whether the request should proceed.

CDA Evaluation

- If the supervisor approves the request, it is forwarded to the IT Manager for a comprehensive assessment to verify the proposed application meets all CDA requirements related to:
  - Security and data protection
  - Regulatory and legal compliance
  - Technical compatibility and integration feasibility
  - Overall suitability for organizational use

Approval from the IT Manager is required before any AI application is licensed.

Roles and Responsibilities

- Employees: Responsible for following this policy and exercising judgment in the use of AI applications.
- Supervisors/Managers: Ensure their teams understand and comply with this policy.
- The Administration Department is responsible for implementing security protocols and overseeing adherence to regulations.

Reporting and Enforcement

- Any misuse, security incident, or concern related to AI must be reported immediately to the IT Manager or Administration Director.
- Violations of this policy may result in disciplinary action, up to and including termination of employment or contract.
- The CDA reserves the right to revoke access to AI systems at any time for noncompliance.