City of WHITEWATER		AI & LLM Acceptable Use Policy			
Owner:	IT Director	Approving Position:	Common Council	Pages:	
Issue Date:		Revision Date:		Review Date:	
Special Instructions:					

I. PURPOSE

The purpose of the City's AI & LLM Acceptable Use Policy is to establish the acceptable use of AI (artificial intelligence) and LLM (large language models) technologies within the operations of the City. Through the use of AI & LLM, the City can drive innovation, increase operational efficiencies, and better serve the community while protecting privacy, managing risk, and promoting accountability, safety, and equity.

II. GUIDELINES

The City may use AI systems to further its mission and meet critical business needs. The use of AI, even if not subject to this policy, must be in compliance with applicable State and federal law. Additionally, employees must maintain awareness of how the AI system uses personally identifiable, confidential, or sensitive information to ensure such use complies with applicable laws, rules, regulations, notices, and policies. Employees are required to have IT Director approval prior to adopting new AI systems.

AI systems aid and enhance human decision making that may impact the public. Employees must ensure that decisions that impact the public are not made without oversight by appropriate staff, who make the final decisions. Automated final decision systems are not permitted. Employees shall take steps to ensure that where AI systems are used to aid in decision making that impacts the public, the outcomes, decisions, and supporting methodologies of such AI systems are documented appropriately. The Department Head, with assistance from the IT Department if necessary, is responsible for periodically assessing the outputs of their in-production AI systems to validate continuing reliability, safety, and fairness. Systemic, computational, and human biases should be identified and remediated. All AI systems should be explainable to the maximum extent practicable.

III. PROCEDURE

a. Treat all information as highly confidential. Do not disclose or share any sensitive customer, employee, voter, CJIS (Criminal Justice Information Services), etc. data during interactions with AI or LLM platforms.
b. All use of AI systems involving personally identifiable information (PII) must comply with Wisconsin privacy laws, including the Wisconsin Data Breach Notification Law (Wis. Stat. § 134.98). Employees must report any suspected data breaches immediately to the IT Department and Data Privacy Officer.
c. All interactions with CJIS data must comply with the CJIS Security Policy, including encryption, access controls, and vetting requirements.
d. Monitoring of employee interactions with AI and LLM systems must comply with the Wisconsin Electronic Surveillance Control Law to ensure that employee privacy rights are not violated.
e. Ensure that AI and LLM platform interactions occur over secure channels and on systems with appropriate security measures to protect information from unauthorized access or disclosure.

f. Usage must adhere to all relevant laws, regulations, and industry standards, such as data protection and privacy regulations and financial industry guidelines.
g. AI and LLM platform usage and/or integration into existing tools will require review and approval by the IT Department.
h. Exercise caution when relying on AI and LLM responses for critical decisions or actions. Use these models as a support tool rather than a sole source of information.
i. Conduct periodic audits and assessments of AI and LLM usage, including access controls, data handling practices, and compliance with policies and regulations.
j. Implement monitoring mechanisms to track and record interactions with AI and LLM platforms for security, compliance, and quality assurance purposes.
k. Educate employees on the appropriate usage of AI and LLM platforms, including data privacy, security best practices, and the importance of adhering to the established policies.
l. Regularly review and update the policy as needed to address emerging risks, changes in regulations, or advancements in technology.

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties. Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.