City of WHITEWATER		Vendor Remote Access Policy			
Owner:	Chief Information Officer	Approving Position:	Common Council	Pages:	
Issue Date:		Revision Date:		Review Date:	
Special Instructions:					

I. PURPOSE

The purpose of the City's Vendor Remote Access Policy is to establish requirements governing remote access by vendors, contractors, and third parties to City of Whitewater information systems. This policy is intended to protect City systems, data, and critical infrastructure while enabling necessary vendor support for operational, maintenance, and emergency activities.

II. GUIDELINES

a. Vendor remote access may be permitted when required to support City business or critical operations. All vendor access must comply with applicable State and federal laws, City policies, contractual obligations, and security requirements.
b. Vendor access shall be granted only with IT approval and only when a documented business need exists. Access must be limited to the minimum systems and privileges necessary to perform approved work.
c. Each vendor user must be assigned unique, individual credentials. Shared or generic vendor accounts are not permitted. Vendor access must be attributable, authenticated, monitored, and revocable.
d. Vendor remote access must use City-approved secure access methods that centralize and control vendor entry into City systems. Direct exposure of City systems to the public internet or use of unapproved third-party remote access tools is prohibited unless explicitly approved as an exception.
e. Multi-factor authentication (MFA) is required for all vendor remote access.
f. Access to high-risk or critical systems, including utility and SCADA environments, is subject to enhanced controls and explicit CIO approval.

III. PROCEDURE

a. Vendor remote access must be implemented in accordance with the City's Vendor Remote Access SOP and related security procedures.
b. All vendor activity is subject to logging, monitoring, and review. Session activity may be recorded for security, audit, and compliance purposes. Vendors have no expectation of privacy while connected to City systems.
c. Vendor access must be revoked immediately when it is no longer required, upon completion of work, or upon contract or project termination.
d. Any deviation from this policy requires documented CIO approval and must include compensating security controls.
e. The policy and supporting procedures shall be reviewed and updated periodically to address evolving risks, operational needs, and changes 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.