
Approved By
City Council

History

Adopted: June 12, 2023

Purpose

The purpose of this policy is to establish procedures to prevent fraudulent payments or transfers to employees, vendors, and contractors.

Scope

This policy applies to all city departments and employees that have control over city disbursement transactions and governs the actions of all city employees.

Processes to prevent fraud

Employee portals and city intranets will utilize multiple authentications when available.

The following are required processes to prevent the fraudulent disbursement of public funds:

Accounts payable

1. Vendor payment approvals:
 - a. Must have at least two approvals within the city for all disbursements of funds.
 - b. City manager or designee approval is required on large payments exceeding amounts set in city policy.
2. Update and review vendor files annually
 - a. Accounts Payable will review and correct duplicate vendors in the system with minor differences (i.e., LLC or Inc.).
 - b. Accounts Payable will annually review the list of vendors and close or inactivate vendors not currently used by the city.
 - c. Accounts Payable will review for unusual activity such as fluctuation in payment amounts, activity for closed vendors, etc.
 - d. Accounts Payable will develop a vendor change form for critical information such as electronic banking information, addresses, or billing practices. These forms will not be provided online but requested from accounts payable and mailed or e-mailed to trusted information on file.

- e. Accounts Payable will verify change forms received from vendors by obtaining verbal confirmation using trusted information on file before making changes to any critical information.
3. Payment terms contained within contracts posted with council will be hidden or redacted.
4. Vendor invoices will not be included in council packets or posted on the internet. Detailed claims listings will not be included with the council packets. Claims lists will be emailed directly to the city council for their review.
5. A signed Form W-9 from every new payee will be required in advance of making any payments or changes to a mailing address. Changes must be confirmed online or directly with the IRS.

Payroll

1. Payroll will request and must receive both written and verbal confirmation from employees prior to making requested changes to direct deposit banking information.
2. Employees must use official payroll change forms to make changes to their banking information. Emails from employees will not be accepted as direction for change unless the email has an attached payroll change form and verbal confirmation is received.
3. Payroll change forms for critical information such as direct deposit banking information will not be provided online but requested from finance/human resources or kept on a secure employee intranet. Finance/Human Resources may email a payroll change form to an employee's West St. Paul email address at the employee's request. All payroll and records containing data covered by the Minnesota Government Data Practices Act must be stored and transmitted securely.
4. Employees not personally known to a finance or human resources staff person to make payroll changes must provide their employee badge or other acceptable form of identification. Employees making payroll changes remotely must provide proof of identification to finance or human resources staff such as a scan of an employee badge or identification card.