GRAND RAPIDS PUBLIC UTILITIES *Service is Our Nature*	**COMMISSION POLICY** **Fraud Prevention**

Category:	Subcategory:	Policy Number:
Business Services		

1.0 – Purpose

The purpose of this policy is to establish procedures to prevent fraudulent payments or transfers to employees, vendors, and contractors. Protecting public funds is a high priority for Grand Rapids Public Utilities Commission (GRPUC).

2.0 – Scope

This policy applies to all Grand Rapids Public Utilities (GRPU) departments and employees that have control over GRPU disbursement transactions and govern the actions of all GRPU employees.

3.0 – Background

Governments are becoming more transparent with information on the internet and electronic banking is becoming widely accepted. Effective internal control policies and procedures need to be adopted to protect municipal utility funds from fraudulently being disbursed.

Advances in technology have reduced the effectiveness of traditional fraud prevention techniques and have even enabled new forms of fraud. Fraudsters are using techniques like social engineering tactics, such as impersonation and manipulation, to deceive employees with legitimate-looking correspondence or phone calls to obtain personal information such as bank accounts or address changes that will re-direct payments intended for an employee or vendor. Often a fraudster will follow government news to learn of newly contracted vendors and use the information and proper timing to contact the municipal utility as the vendor impostor and request the first down payment. Commonly used software allows fraudsters to copy or create legitimate-looking vendor invoices that include slight changes to the name and address.

4.0 – Policy

Processes to prevent fraud

Employee portals and municipal utility intranets should utilize multiple authentications when available. Following are processes to prevent the fraudulent disbursement of public funds:

Accounts payable

1. Vendor payment approvals
   a. Require at least two approvals within the GRPU for all disbursements of funds.

   b. Require municipal utility general manager or designee approval on large payments exceeding amounts set in GRPU policy.

2. Update and review vendor files annually
   a. Review and correct duplicate vendors in system with minor differences, i.e., LLC or Inc.

   b. Annually review list of vendors and close or inactivate vendors not currently used by GRPU.

   c. Review for unusual activities such as fluctuation in payment amounts, activity for closed vendors, etc.

   d. Compare vendor information such as phone numbers, address, and bank account information to employee records for other than employee expense reimbursements.

   e. Develop vendor change form for critical information such as electronic banking information, addresses, or billing practices. These forms should not be provided online but requested from GRPU accounts payable.

   f. Receive verbal communication using trusted information on files regarding all vendor changes on critical information.

3. Do not provide copies of vendor invoices within commission packets that are posted on the utility website.

4. Always require a signed Form W-9 from every new payee in advance of making any payments or change in a mailing address. This can be confirmed online or directly with the IRS.

5. GRPU is required to use ACH blocks and filters as a fraud prevention tool. This requires wire transfers process to have two tier approval process. Above the first-tier specific dollar amount for a single approval, electronic or verbal authentication, with the banking institution and a higher second-tier specific dollar amount with dual approval, and verbal authentication with banking institution. For example, first-tier $250,000 and second-tier $500,000.

6. Required first-tier and second-tier specific dollar amount wire transfers to have a verification of the vendor payment with a representative of the vendor directly independent of email.

7. GRPU is required to use positive pay as a fraud prevention tool.

Payroll

1. Receive both written and verbal communication from the employee, confirming any requested changes to direct deposit banking information.

2. Develop employee change forms for critical information such as direct deposit banking information. These forms should not be provided online but requested from finance/human resources or kept on a secure employee intranet. All payroll and records containing data covered by Minnesota Government Data Practices Act must be stored and transmitted securely.

Review and Maintenance of Policy
The GRPU finance department is responsible for maintaining and reviewing this Fraud Prevention Policy.

GRPU Commissioner

GRPU Commissioner

POLICY HISTORY:

Adopted:

Revised: