Automated Clearing House (ACH)
Electronic Payment Policy

Purpose
This policy outlines the standardized procedures and internal controls for processing vendor payments via Automated Clearing House (ACH) to ensure secure, accurate, and timely disbursements in line with municipal governance and public funds accountability. It aims to minimize payment fraud risk, maintain proper documentation, and enhance operational efficiency.

Scope
This policy applies to all employees responsible for initiating, reviewing, approving, and processing ACH payments to vendors, including but not limited to:

- Accounts Payable staff
- Finance/Accounting personnel
- Departmental managers
- System administrators of accounting and banking platforms

Definitions
The following terms will be used throughout this policy

- **Automated Clearing House (ACH**): An electronic network for financial transactions in the U.S., used for direct deposit and vendor payments.
- **Vendor:** Any external party providing goods or services to the City of Mercer Island under a purchase agreement.
- **ERP**: The City's Enterprise Resource Planning system used for financial and procurement operations.
- **Banking Information**: Includes routing number, account number, account type, and bank name.
- **NACHA**: National Automated Clearing House Association, which manages ACH rules and standards.

Internal Controls and Security
Internal controls over vendor information and electronic payments is a priority. Efforts to prevent or detect potential fraud in electronic payments include:

- Segregation of Duties: No individual should initiate, approve, and transmit a payment. Separate users must initiate and authorize electronic transactions.
- Bank Change Requests: All requests for changes in vendor bank information must be:

- Submitted via a new ACH Authorization Form. Changes to vendor ACH accounts must be processed using the City of Mercer Island ACH Authorization Form, under no circumstances will account changes be authorized by telephone or email.
- Be verified through a phone call to a known contact using on-file information
- Access Control and Security:
- Only authorized personnel may access the ACH payment system.
- Each user initiating or approving bank transactions must have separate bank User IDs.
- The City will use bank security measures to prevent unauthorized individuals from initiating or modifying a transfer, i.e., using positive pay and Direct ACH.
- Adherence to City of Mercer Island computer policies and procedures to protect the computers and computing processes used for EFTs from computer malware
- Audit Trails: Maintain documentation of all ACH activities.

Training

To ensure consistent compliance with procedures, employees tasked with processing, reconciling and record-keeping will train in proper procedures and internal controls prior to conducting these functions.

Vendor ACH Enrollment Procedure

- **ACH Authorization Form**: Vendors selecting ACH payment must submit a completed and signed City of Mercer Island ACH Authorization Form.
- **W-9**: Vendors are required to submit a current W-9 to ensure accurate records.
- **Vendor Verification and Enrollment**:
    - Internal control measures are followed to verify vendor W-9 and ACH Form
    - Accounts Payable enters banking details from ACH form to ERP.
    - Vendor's W-9 information is entered and/or updated if applicable.
    - Entry must be reviewed by a second authorized employee before activation.
    - Vendors are notified via email when ACH enrollment is completed.

ACH Payment Process

1. Departments submit approved invoices to Accounts Payable via the ERP system.
2. AP staff ensure invoices are matched to the purchase order (PO) and any receiving documentation.

3. Payment request is initiated in the ERP system.
   AP staff prepares payment batch in ERP on weekly or as-needed basis.
4. Payment files are reviewed and approved by the Deputy Finance Director or Finance Director.
5. A second person must verify vendor bank info before final submission.
6. ACH file is securely transmitted to KeyBank via encrypted portal.
7. Vendors being paid by ACH credit will be advised of the payment by email.

If it is learned that a vendor does not have a right to a payment or the payment amount is more than the amount due, then the payment is to be cancelled. Actions to take will depend upon where the payment is in the timeline of the transaction.

a) If the ACH file has not been transmitted to KeyBank but the payment process has been finalized, staff will void the batch to remove the incorrect payment.
b) If the ACH file has not been transmitted to KeyBank and the ACH process has begun, staff will remove the incorrect payment prior to finalizing the batch.
c) If the ACH file has already been transmitted to KeyBank, staff would complete a KeyBank ACH Service Request for Item Delete/Reversal and fax to KeyBank.

Returns

If a vendor ACH payment is returned to the City, it will be credited to the settlement bank account at KeyBank from which the funds were originally disbursed.
Returned items are monitored as part of the daily deposit process. Any returned items are forwarded to the appropriate Finance staff member to be researched and either voided or reissued as appropriate.
A second Finance Department employee reviews all such returns and their related disposition.

Record Keeping and Reconciliation

AP documentation is stored physically and/or electronically for 7 years.
Monthly bank reconciliations are performed by Finance. Any discrepancies are to be investigated and resolved.
Transaction records will include:

- Chronological number of the EFT payment.
- Time and date of disbursement.
- Payee - name, address and account number.

- Amount of disbursement.
- Purpose of disbursement.
- BARS or other accounting system expenditure/expense account number.
- Name and number of fund(s).
- Disbursing bank's unique transaction identification number, if available.
- Receiving bank or financial institution's identification number.

Fraud Prevention Measures

- ACH approvals require two-factor authentication (2FA) for banking portal users.
- Staff will receive annual training on phishing, social engineering, and financial fraud prevention.
- Finance will conduct annual audits of vendor records for anomalies.
- Confirmation calls for any vendor bank change requests.
- The Finance Director should notify the disbursing bank that access to files, records and documentation of all EFT transactions involving the Finance Director should be provided to the State Auditor when required for the conduct of the statutory post audit.

Exceptions and Non-Compliance

Any exceptions to this policy must be documented in writing and approved by the Deputy Finance Director or Finance Director.

Policy Review

This policy will be reviewed annually by the Finance Department and updated as necessary based on regulatory changes, audit findings, or operational requirements.