



RESOLUTION 2024-03-27 (1)

Date: March 27, 2024

To: THA Board of Commissioners

From: April Black
Executive Director

Re: Adoption of THA Policy F-25 Electronic Fund Transfers

This resolution would authorize the adoption of the Electronic Fund Transfer Policy to establish procedures, which improve efficiency in the vendor payment process and provide appropriate controls over the expenditure of public funds.

BACKGROUND

The Washington State Auditor's Office recommends agencies establish policies to safeguard Electronic Fund Transfer transactions from internal and external threats.

RECOMMENDATION

Approve Resolution No. 2024-03-27 (1) adopting THA Policy F-25 Electronic Fund Transfers in substantially the form set out in the attached draft. Staff may further amend the policy without Board review for purposes of minor clarification, formatting changes and the addition or modification of flow charts and other visualization, and forms.



RESOLUTION 2024-03-27 (1)

(Adoption of THA Policy F-25 Electronic Fund Transfers)

A **RESOLUTION** of the Board of Commissioners of the Housing Authority of the City of Tacoma

WHEREAS, the Housing Authority of the City of Tacoma (the "Authority") receives and disburses funds by means of wire and other electronic communication; and

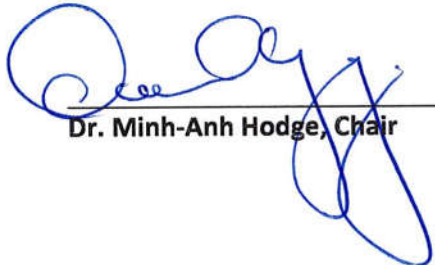
WHEREAS, state law (RCW 39.58.750) requires that the transfer of funds by wire or other electronic communication shall follow the standards set forth by the State Auditor; and

WHEREAS, the State Auditor's Budgeting, Accounting and Reporting System (BARS) Manual 3.8.11.10 recommends adopting policies for electronic funds transfer transactions; now, therefore, be it

Resolved by the Board of Commissioners of the Housing Authority of the City of Tacoma, Washington as follows:

Authorizes THA's Executive Director to adopt and implement THA's Policy F-25 Electronic Fund Transfers.

Approved: March 27, 2024



Dr. Minh-Anh Hodge, Chair



TACOMA HOUSING AUTHORITY

Policy No.	F-25
Policy	Electronic Fund Transfers
Date	December 1, 2023

1. Purpose

The purpose of this policy is to establish responsibilities for implementing Electronic Fund Transfer (EFT) procedures, which improve efficiency in the vendor payment process and provide appropriate controls over the expenditure of public funds.

2. Sources for Policy

- ▶ RCW 39.58.750 Receipt, disbursement, or transfer of public funds by wire or other electronic communication means authorized
- ▶ THA Policy PCI-01 Procurement

3. Scope of Policy

This policy applies to all THA directors, managers, and employees initiating, processing, approving, or overseeing EFT transactions.

4. Who is Responsible for Implementing Policy

Who	Responsibilities
<i>Finance Director</i>	Implement and maintain a system of effective internal controls to ensure EFT payments are properly authorized and executed and are protected from internal and external threats.
<i>Comptroller/Assistant Comptroller</i>	Monitor and approve new setups and modifications of vendor EFT payments. Establish, implement, and oversee procedures for the timely and secure EFT payment of vendor bills. Approve new wire templates. Approve EFT payments.
<i>Department Directors/Managers/ Employees</i>	Ensure new and modifications of vendor/employee EFT payment setup are documented by vendors/employees using approved THA Forms or electronic forms (e.g., Airtable, Yardi Vendor Portal).
<i>Senior/Payroll Accountants and Accounting Specialists</i>	Authenticate new and modifications of vendor/employee EFT payment setup. Update vendor/employee records with authenticated EFT banking information. Initiate EFT payments. Create and upload EFT payment files to the bank.

5. Definitions

<i>Electronic Funds Transfer (EFT)</i>	EFTs are transactions that move money electronically between accounts, individuals, or financial institutions.
--	--

*Automated Clearing House
(ACH)*

Wire Transfer

They are also known as electronic bank transfers, e-checks, or electronic payments. Wire transfers and ACH payments are examples of EFTs.

A nationwide payment and collection system that provides for the electronic distribution and settlement of funds, including direct deposits, within the United States.

An electronic transfer of funds from one bank account to another is initiated directly with the payer's bank. This type of transfer utilizes a system operated by the Federal Reserve Banks (FedWire).

6. Forms Associated with this Policy

7. Policy

7.1 General

THA uses EFTs to receive intergovernmental payments, grant payments, and other revenues where practical. THA also uses EFTs to transmit payments for payroll, withholdings, taxes, debt service, credit cards, banking fees, real estate transactions, housing assistance payments, and other disbursements where practical or required.

All EFT payments will be coordinated and submitted through the Finance Department. The Finance Director, Comptroller, or their designee will approve all new requests and any changes to EFT requests, ensuring that the payment is necessary, all required documentation is provided and appropriately approved, and that the request and bank account information is accurate and valid, and that the transaction is accurately recorded in the general ledger system.

All EFT payments are subject to the applicable purchasing policy - THA Policy PCI-01 Procurement – and all other THA policies and procedures governing the purchase of goods or services.

7.2 Initiating EFT Transactions

Authentication of requests for new and changes to existing EFT setups is required before the new EFT information is entered into vendor/employee or banking records. Authentication of these requests includes the following steps:

- (a) Validating all new electronic payment instruction requests, even those received internally.
- (b) Contacting the vendor/employee directly by phone to confirm any request for electronic payment or payment instruction changes. Such contacting should not be done using the contact information provided in the request but using existing contact information

known to be genuine, such as that in the vendor/employee master file or the original contract.

- (c) Confirming the bank name, account number, and routing information with the contact person.
- (d) Documenting the verification of the EFT information.
- (e) Verifying the accuracy of ACH banking information by creating an ACH Prenote (zero-dollar test transaction).
- (f) Approving the ACH Prenote by the Finance Director, the Comptroller, or their designee after a review of the EFT request and the documented verification of the EFT information.

Once EFT information is authenticated, ACH banking information may be entered and enabled in the vendor/employee record by employees authorized to perform vendor/employee maintenance, and wire banking information may be entered into bank wire templates used to generate wire transactions by employees permitted to create wire templates.

Except for recurring debit ACH transactions approved by the Finance Director or the Comptroller, no debit ACH transactions will be permitted. Heritage Bank has set up ACH Positive Pay on all operating accounts and ACH blocks on all other accounts to reduce the risk of fraud.

7.3 Processing and Approving EFT Transactions

All invoices to be paid with EFT transactions will be approved as required by THA's procurement policy and processed by the authorized Finance Department staff. Generation of ACH files and transmission of the ACH file to the bank will occur through token-secure single-user account login by designated Finance Department staff.

The Comptroller or their designee will approve ACH files after comparison to the matching records in the financial accounting system. Bank balances and transactions will be monitored daily by designated Finance Department staff for unusual or unexpected transactions, and any unexpected transactions will be reported to Heritage Bank immediately.

Heritage Bank user profile permissions will be set up to disallow a person generating an ACH transaction to approve that transaction to ensure adequate separation of duties exists. Heritage Banks' existing controls prevent the same online user from generating and approving a wire transfer.

7.4 Training, Security, and Fraud Prevention

All THA employees must complete cybersecurity training annually, including social engineering training. Finance Department staff will also be trained on ACH fraud schemes upon hiring and at least annually after that.

THA computers will be protected from malware with anti-malware applications and secured appropriately to lower the risk of fraudulent modifications or access to confidential banking information. Multi-factor authentication will be used in THA's systems and is also required for single-user account login for online banking.