FIN-045 Electronic Funds Transfers

Effective Date Thursday, June 27, 2013

Status Final

Last Revised Tuesday, July 20, 2021

Policy Type University

Contact Office
Treasury Management

Oversight Executive
Vice President and Chief Financial Officer Executive Vice President and Chief Operating Officer

Applies To
Academic Division The Medical Center The College at Wise

Table of Contents

Reason for Policy

Requirements for making outgoing electronic funds transfers (EFTs) for the University have been established in order to protect against cyber fraud and to reduce the risk of loss. This policy is intended for employees who enter EFT transactions into a banking system but excludes batch ACH files transmitted to the bank using a system-to-system direct interface and EFTs initiated by an external party.

Definition of Terms

Automated Clearing House (ACH)

An electronic network for financial transactions in the United States. ACH processes large volumes of credit and debit transactions in batches. ACH credit transfers include direct deposit payroll and vendor payments.

Electronic Funds Transfer (EFT)

The electronic exchange or transfer of money from one account to another, either within a single financial institution or across multiple institutions, through computer-based systems. Both Automated Clearing House and Wire Transfers are considered EFTs.

Security Administrator

Employee with the responsibility of granting electronic funds transfer entitlements within a banking system to users of that system.

University Units

Schools and departments within the University.

Wire Transfer

The direct, electronic transfer of funds from one bank account to another, using the Federal Reserve Bank's FedWire System as an intermediary.

Policy Statement

Electronic Funds Transfer (EFT) offers an efficient way to move funds but possesses inherent risks. The policy is intended to establish effective controls and mitigate risks surrounding EFT processing requirements.

1. **Risk Management of Electronic Funds Transfers:**
   As EFTs present a significant fraud risk, the following security practices must be adhered to; exceptions to the security practices in this section may be granted by Treasury Management where deemed appropriate:
   a. The **Security Administrator** must ensure that:
      - Each employee who enters EFT transactions into a banking system be assigned a unique log-in and password.
      - User IDs are deleted as part of the exit procedure when an employee leaves the University.
      - User IDs and passwords for employees on extended leave of 90 days or more are disabled.

   b. The **User Department Head** must:
      - Review the list of department employees with EFT functions annually to determine if each employee's access is still necessary.
      - Revoke access for a department employee with EFT functions when it is no longer needed.
      - Review audit logs periodically to confirm that employees have access only to the functions needed to perform their jobs.

   c. Those **employees authorized to enter EFTs** must:
      - Not share or disclose passwords and account or log-in credentials with anyone.
      - Not have the same User IDs or Passwords used for banking systems as those used to access public sites (such as Gmail, Google, Facebook, Yahoo).
      - Transact EFTs via a system of dual control (two or more employees to transact).
      - Use a dedicated secure line when internet access from the EFT PC occurs outside of the University's secure network.
      - Not use public or unsecured networks.
      - Use bank accounts that are subscribed to the following bank-offered fraud protection services:
        - Automated Clearing House (ACH) debit blocks and filters.
        - Check-clearing blocks for non-checking accounts.
        - Payee Name Positive Pay or Reverse Positive Pay.
        - If available, the use of a maximum dollar amount allowable per transfer (or user defined time interval) to limit exposure if system is compromised.
      - Use multi-factor authentication tools offered by banks (such as tokens, digital certificates, smart cards, etc.).
      - Not share University banking information until discussed with and approved by either Treasury Management or the department handling banking and EFT responsibilities.

- Use a computer that has been set up solely for web-initiated EFTs and appropriately secured, preferably by an Information Technology Specialist or Local Support Partner ("LSP"). Computer security includes, but may not be limited to:
    - Restricting Internet access only to EFT-related websites.
    - Removing all computer programs, including those used for email and text messaging, and turn off all computer functions not essential for EFTs.
    - Encrypting the computer's hard drive.
    - Storing the computer in a physically secure location when not in use.
    - Not leaving the EFT computer unattended when logged-in to a banking system.
    - Clearing the EFT computer's cache and cookies after each web session.

2. **Compliance with Policy:**
   Failure to comply with the requirements of this policy may result in disciplinary action up to and including termination or expulsion in accordance with relevant University policies.

   Questions about this policy should be directed to Treasury Management.

Procedures

1. **EFT Processing for the Academic Division:**
   Information for processing EFTs for the Academic Division can be found at Wire Transfers.

2. **EFT Processing for the Medical Center and the College at Wise:**
   Information for processing EFTs for the Medical Center and the College at Wise can be found in each division's procedures manual, respectively.

Related Information

Institutional Data Protection Standards
IRM-003: Data Protection of University Information
IRM-017: Records Management

Major Category Finance and Business Operations

Next Scheduled Review Monday, June 27, 2016

Revision History

Added Compliance section 7/20/21.

Applies To Text

Academic Division, Medical Center, and the College at Wise.

Last modified April 22, 2024 - 11:48am

Approved By Executive Vice President and Chief Operating Officer

Approved Date June 27, 2013 - 12:00pm