Mercantile Bank®

Treasury Services Self-Assessment

Treasury Services operating rules impose specific data security requirements for all transactions that involve the exchange or transmission of banking data. Customers using these services must ensure appropriate security controls are in place to meet these requirements. Compliance applies to users, computers, processes, media, and controls used by the Customer to manage and maintain use of Treasury Services.

The policies, procedures, systems, and controls must:

- Protect the confidentiality, integrity, and availability of Protected Information (Protected Information is defined as non-public personal information, including financial information, of a natural person).
- Protect against anticipated threats or hazards to the security and integrity of Protected Information and systems.
- Protect against unauthorized use of systems or Protected Information that could result in substantial harm to a natural person or your business.
- Include the routine of self-audits to ensure protections are still in place and working effectively.

Attached are product specific requirements and guidelines for your review. Please contact us at 1.800.453.8700 with any questions.

Mercantile Bank

WIRE SERVICES

The expanded use of technology makes banking easier, but also brings new security risks. The following are suggested best practices to ensure effectiveness and security of online wire transactions.

TRANSACTION SECURITY

- Authenticate all wire instructions and requests
    - Confirm wire instructions by calling the official, published phone number for the recipient.
- Beware of sudden changes in payment instructions
    - Do not call a new number or respond to an unexpected email that contains new wire instructions.
- Use encrypted email for correspondence of sensitive information.

TRANSACTION PROCESSING

- Funds sent through online wire transfer are available for immediate withdrawal by the recipient.
    - Wired funds are considered the property of the recipient and wire transfers may be final.
- After processing, additional information may be required for compliance reasons.
- International Wire Transfers should be originated in local currency.
- Sending a wire transfer with incorrect information will result in a delay of funds.

SECURITY

The expanded use of technology makes banking easier, but also brings new security risks. Below are security best practices recommended by Mercantile Bank.

PASSWORD SECURITY

- Use strong password or password phrase that is unique to each program.
- Safeguard passwords.
- Utilize Multifactor Authentication wherever made available.
- Do not share your password with anyone.
- Change password if ever you suspect it has been compromised.

SYSTEM SECURITY

- Restrict use of computer for business purposes only.
- Protect your IT system – implement anti-virus/spyware software, firewalls, anti-phishing, and keystroke logging prevention.
- Install updates/patches when published.
- Ensure all data, including Protected Information, is encrypted or masked.
- Log off computer or device when not in use.

SYSTEM ACCESS

- Limit system access only to those needing access.
- Limit access to data that contains Protected Information, including servers, drives, files, and data rooms only to those requiring access.
- Keep all paper records in a secure location.
- Do not store Protected Information on unencrypted portable devices.
- Transmit Protected Information over the Internet in a secure session.

STAFF EDUCATION

- Make staff aware of phishing and fraud scams.
- Train employees to be alert for suspicious activity.
- Notify staff and bank immediately of a potential security breach.

GENERAL CONTROLS

- Review your Business Insurance policy for coverage for cybersecurity fraud.
- Reconcile and monitor accounts daily.
- Implement fraud mitigation tools offered by the bank.