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
- Bank will never request your password or secure access code through verbal or electronic request