MAIN STREET COMMUNITY FOUNDATION

PRIVACY PROTECTION
AND
INFORMATION SECURITY POLICY

PURPOSE OF THE POLICY

The Privacy Protection Policy of the Main Street Community Foundation (the "Foundation") is a statement of the Foundation's firm commitment to maintain the privacy of Protected Personal Information obtained from employees, donors, grantees, vendors and other individuals. The policy shall guide the actions of the Board of Directors, the President and CEO and such Committee members and staff who may serve the Foundation regarding the protection and safeguarding of the confidential nature of personal, non-public information that it may obtain. Protected Personal Information includes, for example, social security numbers, driver's license numbers, credit or debit numbers, account numbers, and health insurance numbers ("Protected Personal Information").

POLICY:

The Foundation collects only such Protected Personal Information as is required for the Foundation to comply with its record-keeping and reporting obligations.

The Foundation will not disclose Protected Personal Information except on a strict business need-to-know basis and to the extent required or permitted by law. Examples of the business need-to-know basis include staff, accountants or auditors involved in tax reporting, probate reporting or reporting to donors directly. The Foundation will use commercially reasonable safeguards to prevent unauthorized access and disclosure of Protected Personal Information. Although security cannot be guaranteed, the Foundation will maintain physical, electronic, and procedural safeguards to minimize the risk of unauthorized access or disclosure of such information.

Protected Personal Information for which the Foundation no longer has a need shall be destroyed. The Foundation will destroy, erase, shred, or make unreadable its business records that contain Protected Personal Information prior to disposing such information. The Foundation may dispose of Protected Personal Information by contracting with a person or firm engaged in the business of securely disposing of records that contain confidential information.

Employees of the Foundation are prohibited from accessing, using, disclosing, or revealing Protected Personal Information for unauthorized purposes. Employees only may acquire and use Protected Personal Information for legitimate business purposes and must safeguard the privacy of the information and take reasonable measures to ensure the Protected Personal Information is protected from disclosure and misappropriation.

Professionals, such as accountants, auditors, attorneys, will only be given access to such Protected Personal Information is necessary for them to complete the task for which they

have been engaged. Such professionals shall be require to demonstrate a capability of safeguarding the privacy of the information disclosed.

Consistent with this policy, the Foundation may impose disciplinary measures for actions not in compliance with the policy. All complaints or allegations of violations of the policy will be investigated and the Foundation will take appropriate action.

SPECIFIC PROTECTIONS

The following topics describe how the Foundation safeguards Protected Personal Information in specific locations:

Social Security Numbers

The Foundation does not collect or store social security numbers except from i) employees for required federal and state income reporting; ii) officers for signature authorizations required by banks and depository institutions; and iii) certain vendors for 1099 reporting.

Physical Files

The physical files of the Foundation are kept in locked file cabinets except when in actual use by an employee in the course of that employee's job function. File cabinets and office doors in individual offices are locked when the employee is not present.

Electronic Files

Protected Personal Information is housed on the Foundation's server. Access to the server is only from workstations within the Foundation's office and is password protected. Electronic files are encrypted at rest. Electronic transmissions of Protected Personal Information are encrypted.

The following information is never sent electronically:

- Social Security Numbers
- Bank Account Numbers
- Wire Instructions
- Credit Card Numbers

All computers are protected by anti-virus and anti-malware programs running regularly scheduled scans.

Employees are not permitted to install or download programs or other software.

Firewall

The Foundation maintains a "border" firewall to block outside access to the Foundation's computer network. The Foundation's IT consultant performs random checks.

Passwords

The Foundation uses strong passwords utilizing a mix of letters, numbers and symbols. Passwords are changed upon any change in personnel, or upon other appropriate events. Vendor supplied passwords are changed immediately. Individual workstations utilize password protected screen savers to lock individual computers after a period of inactivity.

Laptops Or Other External Devices/Wireless Or Remote Access

The President of the Foundation has a laptop and secure access to the internal network. No other employee, board member or volunteer has remote access. There is no wireless access to the internal network.

Website

Protected Personal Information is not collected or stored on the Foundation's website. The Foundation uses a third party vendor to host the website. The Foundation does not permit access to its internal network from the website

E-mail addresses

The e-mail addresses of donors, employees board members, committee members and others are collected on a voluntary basis and are only used within the Foundation or for communications between the Foundation and the person owning the address. The Foundation does not share, sell or rent e-mail addresses to anyone outside the organization.

Electronic Payments

The Foundation uses a third party vendor for electronic donations and payments. The vendor is required to have Payment Card Industry Data Security Standards compliant security and privacy protection policies. The Foundation regularly reviews the third party security and privacy protection policies.

EMPLOYEE TRAINING

All employees are given a copy of this policy upon hire and are required to commit to follow the policy. Refresher training is provided on a periodic basis.

All board members, committee members and volunteers are given a copy of this policy and are and are required to commit to follow the policy.

Employees are required to report suspicious activity, particularly e-mail requests, pop-up notices, etc. Employees shall be taught to recognize phishing or other scam attempts. Employees are required to independently verify any requests for sensitive information