SAFEGUARDING MEMBER INFORMATION POLICY

(Revised March 2016)

PURPOSE

The purpose of this policy is to ensure that ETMA Federal Credit Union complies with existing federal and state laws with respect to the privacy and security of member's nonpublic personal information. To comply with these requirements, this policy will set standards addressing administrative, technical, and physical safeguards in order to:

1. Ensure the security and confidentiality of member records or information,
2. Protect against any reasonably anticipatable threats or hazards to the security or integrity of such records, and
3. Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any member.

GENERAL PROVISIONS

ETMA Federal Credit Union shall protect the confidentiality, security, and integrity of each member's nonpublic personal information in accordance with existing state and federal laws.

The credit union will maintain physical, electronic, and procedural safeguards that comply with federal standards to guard members' nonpublic personal information.

The credit union will not gather, collect, or maintain any information about its members that is not necessary in order to offer its products and services, to complete member transactions or for other relevant business purposes.

The credit union does not, and will not sell or provide any member information to third parties including list services, telemarketing firms, or outside companies for independent use.

INFORMATION SECURITY PROGRAM

The manager will be responsible for developing, implementing, and maintaining an effective information security system. The Board of Directors appoints the Supervisory Committee to assure implementation of the security program, as indicated from management and outside auditors. The Supervisory Committee will ensure that annual audits include appropriate testing of the credit union's compliance with existing state and federal laws.

To ensure compliance, the CEO and/or designee will:

1. Assess existing risks to member information
2. Develop ways to manage and control existing risk
3. Monitor third-party outsourcing arrangements to ensure compliance with credit union policies and procedures
4. Draft policies for board review and adoption, where appropriate, to ensure compliance
5. Monitor, evaluate and suggest policy adjustments to the Board of Directors, as appropriate in light of:

- Relevant changes in technology

- The sensitivity of the member information
- Internal or external threats to information
- The credit union's own changing business arrangements such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to the member information system.

6. Brief Board of Directors at least annually, in conjunction with the report of outside auditors, on the status of the comprehensive information security program, addressing issues including:

- Risk assessment
- Risk management and control decisions
- Service provider arrangements
- Results of testing
- Security breaches or violations, along with management's responses: and
- Recommendations for changes in the information security program

RISK ASSESSMENT

In order to assess the risks that may threaten the security, confidentiality, or integrity of member information or member information systems, the credit union shall:

1. Identify all reasonably foreseeable internal as well as external threats that can result in unauthorized disclosures, misuse, alterations, or destruction of member information or member information systems.
2. Determine the likelihood as well as the potential damages of the internal or external threats
3. Determine the sufficiency of the credit union's policies, procedures, and member information systems to control the identified risks.

BUILDING AND INFORMATION SYSTEM ACCESS RESTRICTIONS

1. Employees will be allowed in the building only during their normal working hours. Any exceptions must be approved by the CEO.
2. Keys and alarm codes will be issued to employees and will be used to enter the building daily. If the key is lost or misplaced, the employee who lost or misplaced their key must report it immediately to the CEO. The CEO will on occasion review alarm company reports to monitor building access.
3. Access to the cash area will be limited to employees and management. Codes to the doors leading to leading to the cash area will be given only to employees and management.
4. Entry to non-public areas will be limited to employees and credit union officials at all times. Vendors and visitors will only be allowed in non-public areas when escorted by an employee or official.
5. Access to the computer closet will be limited to designated employees. Employees will not enter the computer closet unless to complete necessary assigned duties.
6. Access to the credit union's electronic information processing and storage system will be controlled by user name and password. Ability to access the credit union's electronic system remotely will be limited to the CEO and other employees designated by the CEO. The CEO or other designated employee may give Fiserv (Core Processing System) authority to access the credit union's electronic information processing and storage system remotely in order to maintain or update operational functions.

PHYSICAL RECORDS ACCESS

1. All physical records of the credit union containing member information will be maintained in a secured area.
2. Employees will not leave member information in view of other members or the general public. Employees will not leave member information in reach of other members or the general public without safeguarding the information.
3. Physical records of the credit union containing member information will not be removed from the credit union premises except with the permission of the CEO or the Board of Directors.
4. All paper information to be disposed of containing any member information including but not limited to name, telephone number, address, account number, social security number, and account balances must be placed in the appropriate located bin for shredding.

IDENTITY AUTHENTICATION

1. All persons seeking to transact business on an account must be identified as the account owner

a. In-office transactions

- Employee viewing valid photo id
- Visual recognition for known members/account owners

b. Telephone Transactions

- Verify member's password
- Other information known only by member (social security number, mother's maiden name, details about account, direct deposit information, etc.)
- Requests for file maintenance will be taken over the phone but instead should be submitted in person, by mail, via email or fax.
- If employee is unable to successfully identify member, transactions should not be conducted.

c. Mail/fax/emailed requests for file maintenance and withdrawals will be verified by comparing signatures on the Account Card. If the employee does not believe the request is authentic, the employee should consult with management for direction.

d. Non-member requests to transact business on behalf of member, such as cash or check withdrawals made payable to third parties, will not be permitted. The only types of transactions permitted will be deposit or loan payments. Receipts for these transactions will be mailed to member's address of record.

2. Verification of Deposit - Original written release is required - a fax copy will not be accepted.

INFORMATION DISCLOSURE

1. To combat identity theft and theft of member information, employees will verify identity of all callers as described earlier in the policy. Even if the identity of the member is verified, the employee will not give out information that the member should already know if they

are the legitimate caller. If the information needs to be verified by the member, our employee will call the member back at the phone number of record, not a number provided by the caller.

2. Employees cannot verify any information about a member or a member's account to anyone, including law enforcement agencies without the member's original written authorization, a subpoena, or a court date.
3. Requests for verification of funds for a particular check will be handled if the call appears to be legitimate. For these requests, the response should be simply "the check will be good at this time" or "the check will not be good at this time". The member's balance or any other information should not be given to the caller.

CHANGE OF ADDRESS

Change of a physical, mailing or email address and/or phone number requests must be submitted in writing. Account takeover and identity theft is commonly accomplished by changing an address for accounts to an address in control of the fraudster. In order to protect our member, such information change requests must be submitted in writing.

E-MAILING

Member information will only be emailed using the Share File system. This allows sensitive information to be encrypted until the member enters their personal information.

ATTEMPT MONITORING

1. Members have access to their accounts via home banking and the internet. The credit union has established firewalls with adequate protection against unauthorized access to member records and general credit union electronic information.
2. Remote access to the credit unions primary data processing system will be disabled at all times except when enabled to permit remote access by authorized user or transmitting information.
3. Remote member to internet/home banking for member accounts will be disabled after 3 failed attempts.

SYSTEM CHANGES

System access or security parameter changes must be authorized by the CEO, or other employees as designated by the CEO. All system changes will be reviewed by the CEO to assure that the change had not compromised the system security or member information.

WIRE TRANSFERS

The manager, accounting manager and head teller will be authorized to approve wire transfers. Secret codes will be issued to each person authorized to transmit funds.

GIFT CARDS

Visa Travel Money Cards and Gift cards are secured in the vault. The manager and the accountant are responsible for maintaining records.

PROTECTION AND SECURITY

The credit union will offer credit life insurance and loan protection insurance to eligible members. CUNA Mutual will be the company that will provide life insurance.

An adequate insurance program will remain in force to protect the interest of the credit union member. CUNA Mutual Insurance will provide ETMA Packet of Insurance Protection Package and Bond Coverage. This policy will be reviewed annually.

To limit the risk of robbery the services of Bankpak and ADT are retained by the credit union.