Definitions

*These terms are defined by the **NCUA Part 748**.*

Member: An individual who has an established, ongoing relationship with {COMPANY-NAME}. This includes both members and non-members who have co-signed on loans. Examples of non-members include, but are not limited to, the following:

- Non-member joint account holders
- Non-members holding an account in a state-chartered credit union under state law

Service provider: A third party that maintains, processes, or otherwise is permitted access to member information while performing services for {COMPANY-NAME}.

Member information: Any record maintained by, or on behalf of, {COMPANY-NAME} that contains information regarding an individual who has an established, ongoing relationship with {COMPANY-NAME}. This includes records, data, files, or other information in paper, electronic, or other form that are maintained by, or on behalf of, any service provider on behalf of {COMPANY-NAME}.

Member information system: Any electronic or physical method used to access, collect, store, use, transmit, protect, or dispose of member information.

Overview

This policy addresses the following topics:

- Board Involvement
- Risk Assessment
- Management and Control of Risk
- Member Information Security Controls
  - Vendor Management Review Program
  - Software Inventory
  - Hardware Inventory
  - Critical Systems List
  - Records Management
  - Clean Desk Policy
  - Hardware and Electronic Media Disposal Policy
  - IT Acquisition Policy
  - Incident Response Plan
  - Information Sharing
- Training
- Testing

Purpose

The purpose of this policy is to ensure that {COMPANY-NAME} complies with existing federal and state laws, and to ensure that information regarding members is kept secure and confidential.

Policy Detail

It is the policy of {COMPANY-NAME} to protect the confidentiality, security, and integrity of each member's non-public personal information in accordance with existing state and federal laws. {COMPANY-NAME} will establish and maintain appropriate standards relating to administrative, technical, and physical safeguards for member records and information.

{COMPANY-NAME} will maintain physical, electronic, and procedural safeguards, which comply with federal standards, to guard members' non-public personal information.

{COMPANY-NAME} will not gather, collect, or maintain any information about its members that is not necessary to offer its products and services, to complete member transactions, or for other relevant business purposes.

{COMPANY-NAME} does not sell or provide any member information to third parties, including list services, telemarketing firms, or outside companies for independent use.

The Board of Directors must approve the Safeguarding Member Information Policy, required by NCUA Part 748 Appendix A.

{COMPANY-NAME}'s Information Security Officer is responsible for annually reviewing the program, making any needed adjustments, and coordinating staff training. {COMPANY-NAME} Management is responsible for ensuring that its departments comply with the requirements of the program.

Information Security Program

Management is responsible for developing, implementing, and maintaining an effective information security program to:

- Ensure the security and confidentiality of member records and information
- Protect against any anticipated threats or hazards to the security or integrity of such records
- Protect against unauthorized access to, or use of, such records or information that would result in substantial harm or inconvenience to any member

Management shall report to the Board of Directors, at least annually, on the current status of {COMPANY-NAME}'s Information Security Program. The Board of Directors will also be notified of any security breaches or violations and the management team's response and recommendations for changes in the Information Security Program.

Board Involvement

On an annual basis, the Board of Directors is required to provide the NCUA and DFI Regional Director with a certification of {COMPANY-NAME}'s compliance with NCUA Part 748. The certification is contained in the Report of Officials submitted after the annual election of officials. Prior to the certification, {COMPANY-NAME}'s Information Security Officer will provide the Board with a status report of {COMPANY-NAME}'s Safeguarding Member Information Program.

Risk Assessment

{COMPANY-NAME} maintains a risk assessment that identifies potential threats to member information and evaluates the potential impact of the threats.

On an annual basis, the risk assessment is reviewed and updated by the Information Security Officer and {COMPANY-NAME}'s Management. {COMPANY-NAME}'s controls are then updated accordingly.

Management and Control of Risk

In order to manage and control the risks that have been identified, {COMPANY-NAME} will:

- Establish written procedures designed to implement, maintain, and enforce
- {COMPANY-NAME}'s information security program
- Limit access to {COMPANY-NAME}'s member information systems to authorized
- employees only
- Establish controls to prevent employees from providing member information to unauthorized individuals
- Limit access at {COMPANY-NAME}'s physical locations containing member information, such as building, computer facilities, and records storage facilities, to authorized individuals only
- Provide encryption of electronic member information including, but not limited to, information in transit or in storage on networks or systems to which unauthorized individuals may have access.
- Ensure that member information system modifications are consistent with
- {COMPANY-NAME}'s information security program

- Implement dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for, or access to, member information
- Monitor {COMPANY-NAME}'s systems and procedures to detect actual and attempted
- attacks on, or intrusions into, the member information systems
- Establish response programs that specify actions to be taken when {COMPANY-NAME} suspects or detects that unauthorized individuals have gained access to member information systems, including appropriate reports to regulatory and law enforcement agencies
- Implement measures to protect against destruction, loss, or damage of member information due to environmental hazards, such as fire and water damage or technical failures
- Regularly test, monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of member information, business arrangements, outsourcing arrangements, and internal or external threats to {COMPANY-NAME}'s information security systems

Member information security controls /R

{COMPANY-NAME} has established a series of member information security controls to manage the threats identified in the risk assessment. The controls fall into ten categories.

- **Vendor management review program**
  {COMPANY-NAME} will exercise appropriate due diligence when selecting service providers. When conducting due diligence, management will conduct a documented vendor review process as outlined in the Vendor Due Diligence Procedure. {COMPANY-NAME} will also consider obtaining SSAE 16 reports from prospective service providers.
  All service providers, who may access member information, must complete a Vendor Confidentiality Agreement requiring the provider to maintain the safekeeping and confidentiality of member information in compliance with applicable state and federal laws. Such agreements must be obtained prior to any sharing of member information. Once the agreement has been completed, management will, according to risk, monitor service providers by reviewing audits, summaries of test results, or other evaluations.
- **Software inventory**
  {COMPANY-NAME} will maintain an inventory of its desktop, server, and infrastructure software. The information from this collection will provide critical information in identifying the software required for rebuilding systems. A template incorporated into the software inventory ensures that the security configuration and configuration standards are enforced. The template will also provide personnel with a quick resource in the event of a disaster. The software inventory list will be reviewed and updated on a continual basis.

- **Hardware inventory**
  {COMPANY-NAME} will maintain an inventory of its desktop, server, and infrastructure hardware. The information from this collection will provide critical information in identifying the hardware requirements for rebuilding systems. A template incorporated into the hardware inventory ensures that {COMPANY-NAME} standards are enforced. The template will also provide personnel with a quick resource in the event of a disaster. The hardware inventory list will be reviewed and updated on a continual basis.
- **Critical systems list**
  {COMPANY-NAME} will maintain a listing of its critical systems. This listing will support critical reliability functions, communications, services, and data. The identification of these systems is crucial for securing member information from vulnerabilities, performing impact analysis, and in preparing for unscheduled events that affect the operations of {COMPANY-NAME}.
- **Records management**
  The industry wide general principles of records management apply to records in any format. {COMPANY-NAME} will adhere to policies and procedures for protecting critical records from all outside and unauthorized access. Access to sensitive data will be defined as to who can access which data and under what circumstances. The access will be logged to provide accountability.
  {COMPANY-NAME} will adhere to the required state statues, NCUA, Data Classification Procedures, and federal guidelines designated for record retention. {COMPANY-NAME} will adhere to the Records Retention Policy for the proper process to dispose of records. Record disposal will be well documented. An inventory will be maintained of the types of records that are disposed of, including certification that the records have been destroyed.

- **Clean desk policy**
  {COMPANY-NAME} employees will comply with the Clean Desk Policy. This policy was developed to protect sensitive data from being readily available to unauthorized individuals.
- **Hardware and electronic media disposal procedure**
  {COMPANY-NAME} will take precautions, as outlined in the Hardware and Electronic Media Disposal Policy, to ensure sensitive data cannot be retrieved from retired hardware or electronic media.
- **IT acquisition policy**
  {COMPANY-NAME} will adhere to policies and procedures for acquisition of computer related items. Computer related purchases will be reviewed by designated IT personnel for compliance with security plans and alignment with operational and strategic plans. An annual review of acquisition policies and procedures will occur with input from the Information Security Officer.
  A review of technology needs will occur during the annual budgeting and work planning processes. Needs will be classified into either current year plans or long range needs. The acquisition of technology solutions will be assessed to ensure that both current and future needs are met.
- **Incident response plan /R**
  Incident response is defined as an organized approach to addressing and managing the aftermath of a security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.
  As required in the Incident Response Plan, {COMPANY-NAME} will assemble a team to handle any incidents that occur. Necessary actions to prepare {COMPANY-NAME} and the Incident Response Team will be conducted prior to an incident as required in the Incident Response Plan.

Below is a summary of the steps the IT Department, as well as {COMPANY-NAME} management, would take:

- The IT Department will immediately investigate the intrusion to:
  - Prevent any further intrusion to the system
  - Determine the extent of the intrusion and any damage caused
  - Take any steps possible to prevent any future such intrusions
- The IT Department will notify Administrative Management and Risk Management of the intrusion. Administrative Management will be responsible for notifying the Board of Directors.
- The IT Department will follow escalation processes and notification procedures as outlined in the Incident Response Plan. Examples include, but are not limited to, notifications to staff, regulatory agencies, law enforcement agencies, FBI, NCUA, or the public.
- If applicable, the Director of Compliance Bank Secrecy Act Officer (BSA) will be notified and will file a Suspicious Activity Report with FinCEN.
- If applicable, notices will be sent to affected members in compliance with the requirements of Wisconsin State Civil Codes.

Training

{COMPANY-NAME} recognizes that adequate training is of primary importance in preventing IT security breaches, virus outbreaks, and other related problems. {COMPANY-NAME} will conduct regular IT training through methods such as staff meetings and computer based tutorial programs. In addition, employees will be trained to recognize, respond to, and where appropriate, report any unauthorized or fraudulent attempts to obtain member information.

All new employees will receive IT Security Training, as part of their orientation training, emphasizing security and IT responsibility. The Training Specialist, or designee, is responsible for training new employees on Information Security.

Testing

The Information Security Officer annually audits {COMPANY-NAME}'s Safeguarding Member Information Program. The Information Security Officer provides a formal report of its findings to Senior Management, the Security Officer, and the Board of Directors.

{COMPANY-NAME} will require periodic tests of the key controls, systems, and procedures of the information security program. In accordance with current industry standards, the frequency and nature of such tests shall be determined by the IT Department.

The Information Security Officer will be responsible for reviewing the results of these tests and for making recommendations for improvements where needed.