# Family First Credit Union

Information Security Policy

## General Policy Statement:

Family First Credit Union recognizes its responsibility to safeguard member information and will treat the private financial information of Credit Union's members ("member information") with appropriate care in order to maintain the confidentiality, integrity and security of member information. The purpose of this policy is to set forth the guidelines for management and staff to use in establishing and maintaining policies and procedures to safeguard member information. The Credit Union will comply with all applicable laws and regulations governing the safeguarding of member information including NCUA Guidelines for Safeguarding Member Information (12 CFR Part 748 Appendices A and B, Part 749 Appendix B) (the "Guidelines") and all other applicable laws and regulations regarding the safeguarding of member information.

### Reference:

National Institute of Standards and Technology (NIST). Special Publication 800-53 (Revision 4) Security Controls and Assessment Procedures for Federal Information Systems.

### Guidelines:

1. **POLICY AND PROGRAM RESPONSIBILITY.**

    i. **Board Responsibility.** This Information Security Policy ("Policy") and any recommended changes shall be approved by the Board of Directors ("Board"). The Board may delegate its oversight responsibility to a Board Committee. The Board will appoint an Information Technology Committee Chairman for the Credit Union on an every other year basis.

    ii. **Management Responsibility.** Credit Union Management ("Management") through an Information Security Committee ("Committee") will be responsible for the development, implementation, and maintenance of the Credit Union's Information Security Program ("Program") and may assign these responsibilities. Management shall ensure that capital planning and investment requests include the resources needed to implement the information security program.

2. **ASSESSMENT OF RISK.** From time to time, but at least once every 12 months, Management will identify and assess the risks that may threaten the security, confidentiality, or integrity of the Credit Union's information systems, and

determine the sensitivity of member information, and the internal and external physical and cybersecurity threats to its security. Management will evaluate and adjust its risk assessment on a periodic basis and in light of any relevant changes in technology; changes in internal and external threats; changes in the member base adopting electronic banking; changes in member functionality offered through electronic banking; transactional capability; transaction volumes; and actual incidents of security breaches, identity theft, fraud, and other significant cybersecurity events experienced by the Credit Union or industry. Management shall report the annual risk assessment to the Credit Union's Board and/or Supervisory Committee for approval.

3. **RISK MANAGEMENT AND CONTROLS.** Management will conduct an initial and ongoing risk management analysis of its controls, policies, and procedures to proactively prevent, detect and respond to all identified risks and intrusions that may occur. The scope of the risk management analysis will cover, physical facilities controls, cybersecurity controls including access controls, internal controls, ongoing monitoring of risk and controls, an intrusion response plan, and a disaster recovery plan.

    i. **Assessment of Controls.** Management will assess the sufficiency of existing policies, procedures, and other arrangements in place to control risks and reduce risk exposure. The Credit Union will review controls on employee duties and existing intrusion detection systems from time to time.

    ii. **Vulnerability Testing.** The Credit Union will establish a baseline of current assessed risk. The Credit Union will conduct periodic vulnerability testing at least annually, and may engage outside security expertise to assist in such testing. The results of the vulnerability testing will be given to the IT Committee (and the Board) for review and necessary action.

    iii. **Threat Awareness.** On a regular basis, management shall monitor information security threat alerts from threat-sharing sources, which may include but is not limited to the following: the U.S. Computer Emergency Readiness Team (US-CERT), the U.S. Department of Homeland Security, reputable news sources, Credit Union peers, and service providers. Information gleaned from these sources shall be incorporated into the Credit Union's ongoing risk management efforts. For example, a newly identified threat to an information system asset used to process member information may increase the risk level associated with that information system above acceptable levels.

    iv. **Plan of Action and Milestones.** Management will respond to identified information security risks with documentation of the plans of action to

address unacceptable risks, including clear milestones outlining goals and timelines to achieve acceptable risk levels. Plan of action and milestones reports will be given to the Committee (and the Board) for review and approval.

4. **SERVICE PROVIDERS.** Management will require its service providers, by contract, to implement appropriate measures designed to protect against unauthorized access to or use of member information that could result in substantial harm or inconvenience to any member. To that end, the credit union will receive assurances that third parties will handle member information in a manner commensurate with regulatory guidance and the Credit Union's information security policies and expectations.

5. **SECURITY OF PHYSICAL FACILITIES.**

   i. **Physical Access Authorizations.** Access to locations containing member information is restricted to persons with "need-to-know" access to member information. Management shall maintain a list of employees who have physical access to media storage containing member information, or information systems that store, process, or transmit member information. The list shall be reviewed on a Credit Union-defined frequency. Management shall issue credentials for access to facilities based on the physical access authorization process.

   ii. **Physical Access Control.** Management shall control access to non-public Credit Union facilities using Credit Union-defined physical access control devices/systems (e.g. physical locks, key card readers). An inventory of access control devices/systems shall be maintained. A procedure will be established to revoke keys or disable key cards when employees are transferred or separated.

   iii. **Monitoring Physical Access.** The Credit Union shall monitor physical access to areas where the information system resides using access logs. The Credit Union will monitor intrusion alarm systems and surveillance cameras.

   iv. **Visitor Control.** Visitors to the Credit Union without a "need-to-know" authorization will be escorted as necessary within the nonpublic and administrative areas of the Credit Union, and off-site storage areas by a Credit Union employee with "need-to-know" authorization.

v. **Physical and Environmental Protections for Information Systems.** The following controls shall be deployed, as feasible, to protect the Credit Union's information systems from physical and environmental threats:

a) Emergency power shut-off capability (easily accessible to authorized personnel)
b) Automatic emergency lighting
c) Fire protection and detection devices
d) Temperature and humidity controls
e) Water damage protection (accessible and functional master shutoff or isolation valves)
f) Additional controls may be deployed, as necessary
g) Physical Security Checks as relates to Staff Controls for Information Handling.

vi. **Staff Controls for Information Handling.**

a) **Preventing Inadvertent Disclosure.** Credit Union staff who handle member information ("Users") will take all necessary steps to assure that member information is not inadvertently disclosed to people who do not have a "need-to-know" authorization. When not in use, or when not under direct visual supervision, member information must be stored in a secure storage area such as a locked vault, a cabinet, or a locked desk. Reproduction of member information is permitted only as necessary to perform required work.

b) **Transport.** Physical transport of member information will require the use of a trusted courier such as internal mail staff, the US Postal Service, UPS, Federal Express, or a contracted courier service. All member information and documents sent via such couriers must be enclosed in an opaque and sealed envelope. Whenever member information is sent over external computer networks, it must be sent in encrypted form.

c) **Destruction.** When member information is no longer required (but the computers will be used elsewhere), and when legal or regulatory requirements for its retention no longer apply, it must be destroyed according to approved methods as authorized by Compliance Officer. Destruction will include rendering the information unreadable and include complete eradication of residual electronic information required by FACTA and other applicable laws and regulation to be destroyed. The Credit Union will ensure that all contracts between the Credit Union and service providers who have access to or store member information will

include contractual requirements that the service provider dispose of member information in a manner consistent with FACTA and other applicable laws and regulations. The Credit Union will ensure that vital records will not be destroyed.

vii. **Theft Protection.** All Credit Union computer and network equipment must be physically secured with anti-theft devices if located in an open office environment. Local area network servers must be placed in locked cabinets, locked closets, or locked computer rooms. Transportable computers must be placed in locked cabinets, or secured via other locking systems when in the office but not in use. Computer and network gear may not be removed from Credit Union offices unless the User has first obtained permission from Information Technology Manager.

6. **CONTROLS FOR ACCESS SECURITY.**

i. **Responsibilities of Information Supervisor, Custodians, and Users.**

a) **Supervisor.** The Information Supervisor or her/his delegate(s) within the Credit Union, bear the responsibility for the acquisition, development, and maintenance of production applications which process member information. For each type of member information, the Supervisor will determine the critical nature of the information and define which Users will be permitted to access it, and define its authorized uses.

b) **Custodian.** A Custodian is a Credit Union staff person who is in physical or logical possession of member information. All departments and staff positions are considered Custodians. Whenever member information is maintained on a personal computer, that User is also the Custodian. A Custodian is responsible for safeguarding member information and maintaining security measures defined by the Supervisor.

c) **Users.** Users are responsible for complying with any Credit Union member information security policy, procedure, and standard. Questions about the appropriate handling of a specific type of member information should be directed to either the member information Custodian or the Supervisor.

ii. **Member Information Classification and Confidentiality.**

a) **Information Sensitivity Classification.** Member information is generally designated as nonpublic and may be disclosed only to persons who have been authorized to receive it. Authorization is granted by the Supervisor, consistent with the Credit Union's Privacy Policy, and otherwise on a "need-to-know" basis. Unless specified otherwise by the CEO, all Credit Union employees have access and "need-to-know" authorization for member information.

b) **Password Complexity**. The Credit Union will require members utilizing the Credit Union's Internet-based services to use several controls to appropriately authenticate members access to Credit Union products, services and systems including:

- ✓ Create alphanumeric passwords that are at least eight (8) characters in length. The Credit Union will encourage members to change their passwords on a regular basis required once per year;
- ✓ Dual layer authentication;
- ✓ Layered security to segregate public and private networks including controls to access and member protection; and
- ✓ Other controls necessary to protect the privacy and integrity of Credit Union and member information.

c) **Default Classification.** Member information will be classified and treated as nonpublic, as per the definition of member information in NCUA guidelines (Appendix A to Part 748)..

d) **Disclosure.** Disclosure of member information to any staff person or nonaffiliated third party without a "need-to-know" authorization is prohibited. Employees must be familiar with and agree to the confidentiality provisions and member information security provisions in the Credit Union's Employee Handbook. Member information Custodians must verify the existence of a signed confidentiality agreement prior to disclosure to non-employees.

iii. **System Access Controls.** The Credit Union will create system access controls to restrict access to and safeguard member information that is collected and stored by the Credit Union.

a) **Employees.** The Credit Union will use pre-employment background checks and employment job descriptions to address employee access to member information, dual controls/segregation, and duties for processing transactions and

handling member information. Employees may require rescreening, as necessary, when their job duties change and include increased information handling and/or security responsibilities

b) **Passwords.** Password controls will be implemented to limit system access to member information. Passwords may not be stored in computers without access control systems, written down and left where unauthorized persons might discover them, or in other locations where unauthorized persons might discover them. Passwords may not be shared or revealed to anyone else besides the authorized user.

iv. **Access Control System Design.**

a) **Internal Network Connections.** All Credit Union computers connected to internal computer networks will have an approved password-based access control system. All computers handling member information will employ approved password-based access control systems.

b) **External Network Connections.** All in-bound connections to Credit Union computers from external networks must be protected with an approved dynamic password access control system. Users connected to external networks are prohibited from leaving modems turned on while data communications software is enabled, unless an authorized dynamic password system has been installed.

c) **Boot Protection and Screen Savers.** All computer users will obtain boot protection through a fixed password and a screen saver. Multi-user Credit Union systems must employ automatic log-out systems that terminate a User's session after a certain period of inactivity.

d) **Unique User-IDs and Passwords.** All critical access control systems must utilize user-IDs and passwords unique to each User, in order to protect Users from unwarranted suspicion associated with computer crime and abuse and to help maintain the integrity of member information by reducing unexplained errors and omissions.

e) **Unsuccessful Logon Attempts.** Critical access control systems will be configured to allow only a Credit Union-defined number of failed logon attempts to authenticate a user (over a defined timespan) before the account automatically locks for a defined

timespan or until it is unlocked by a systems administrator.

v. **Managing System Privileges.**

a) **Access Requests.** Requests for new user IDs and changed privileges must be in writing and approved by the User's manager before a Systems Administrator fulfills these requests.

b) **Compliance and Confidentiality Statement/Agreement.** All Users wishing to use Credit Union multi-user computer systems must sign a compliance and confidentiality agreement prior to being issued a user ID.

c) **Access Denial.** All user IDs that are inactive automatically have the associated privileges suspended or revoked. When Users are transferred to a different job, their system privileges will be changed to reflect their new job duties. At employment separation, all Credit Union property in employee's possession must be returned to the Credit Union, and all system access privileges shall be terminated. Management reserves the right to revoke the system privileges of any User at any time.

d) **Prohibited Activities.** Users must not test, or attempt to compromise Credit Union computer or communication system security measures unless specifically approved in advance and in writing by the Information Technology Manager. Incidents involving unapproved system cracking (hacking), password cracking (guessing), file decryption, bootleg software copying, short-cuts bypassing system security measures, pranks or practical jokes, or similar unauthorized attempts to compromise security measures may be unlawful, and will be considered serious violations of this Policy.

7. **CONTROLS FOR INTERNAL SECURITY.**

i. **Standards.** The Operations and IT Managers are responsible for setting standards of conduct for Credit Union employees and users of member information including compliance with the provisions of this Policy and all member information security procedures conveyed to them verbally or in writing.

ii. **Dual Controls.** Configuration or setting changes for any information security systems or controls, e.g., firewall and other monitoring systems, or any other elements of the Credit Union's Information System that could

directly affect member information are made by the Information Technology Department, or outsourced service provider, only after approval by the Information Technology Manager and the Operations Manager.

iii. **Display of Information**. All computer display screens must be positioned such that the information cannot be readily viewed through a window, by persons walking in a hallway, or by persons waiting in reception and related areas.

iv. **Clean Desk**. All member information that is printed on physical paper will be out of site and secured at the end of each day.

v. **Encryption.** When member information is transmitted over any communication network provided by an organization outside the Credit Union, it must be sent in encrypted form. Member information entrusted to the Credit Union by a third party must be encrypted when sent over external network systems.

vi. **Layered Security**. Segregating public and private networks, deploying overlapping controls for access and asset protection

vii. **Held in Storage.** Whenever member information is not actively used, it must be stored in encrypted form if unauthorized individuals can access it.

viii. **Permissible Methods.** Encryption of member information at rest (in storage) or in transit (on a network) must be achieved via commercially available products approved by the Information Technology Manager. All encryption algorithms, modes of operation, and key management systems must be consistent with internal standards issued by the Information Technology Manager.

ix. **Information Loss.** Whenever encryption is used, employees must not delete the sole readable version of the member information unless they have first demonstrated that the decryption process is able to reestablish a readable version of the member information.

x. **Encryption Keys.** Encryption keys used for member information are always classified as member information. Access to such keys must be strictly limited to those who have "need-to-know" authorization. Likewise, encryption keys must always be encrypted when sent over a network.

xi. **Broadcast Systems.** Portable phones using radio technology as well as cellular phones must not be used for data transmissions containing member information unless the connection is encrypted. Likewise, other

broadcast networking technologies, such as radio-based local area networks or wireless ("wi-fi") networks, must not be used for member information unless the link is encrypted.

xii. **Network Changes.** All changes to Credit Union computer networks must be documented in a work order request and approved in advance by the Information Technology Manager. All changes will be made by the Information Technology Department. Emergency changes to the Credit Union networks may be made only by persons authorized by the Information Technology Manager.

xiii. **New Systems Set-Up.** Employees must not establish electronic bulletin boards, local area networks, modem connections to existing local area networks, new types of real-time connections between two or more in-house computer systems, or other multi-user systems for communicating information without the specific approval of the Information Technology Manager.

xiv. **Systems Removal and Disposal**. Computer Equipment with an internal disk drive(s) ("hard drive") being removed for relocation or disposal must have the disk drive(s) render any information unreadable. If the equipment is being relocated to another Credit Union user, the disk drive(s) may be erased using software specifically designed to render any data on the disk drive(s) unusable. If the equipment is being discarded, sold or given away, the disk drive(s) must be removed and physically destroyed prior to removal.

xv. **Application Development.** All software development and software maintenance activities performed by in-house staff must subscribe to the Credit Union's Information System policies, standards, procedures, and systems development conventions regarding testing, training, and documentation.

a) **Written Specifications.** All software developed by in-house employees, and intended to process critical, valuable, member information, must have a written formal specification, which includes a discussion of both security risks and controls (including access control systems and contingency plans).

b) **Security Sign-Off Required.** Before being used for production processing, new or substantially changed application systems must have received written approval from the Information Technology Manager.

xvi. **Handling Security Information.** Information about security measures for Credit Union computer and network systems is confidential and may not be released to persons not possessing "need-to-know" access.

## 8. ACH SECURITY FRAMEWORK

The Credit Union will provide data security measures for member's non-public personal information initiated, processed or stored in the ACH Network according to the ACH Security Framework requirements of the NACHA Rules. These measures will include:

i. Protecting the confidentiality and integrity of members' non-public personal information;

ii. Protecting against anticipated threats or hazards to the security or integrity of members' non-public personal information; and

iii. Protecting against unauthorized use of members' non-public information that could result in harm to a member.

ACH data is accessed via our Active Directory Environment. Each user is assigned permissions based on their position and each employee is given the least permissions necessary. ACH data is stored on our internal file server which is accessed only via the Active Directory authentication and user permissions. No ACH data has been destroyed since we began creating ACH data using the Catalyst online system. All core related ACH data is housed on the Fiserv CUnify online system. Access to this system is controlled by the Active Directory Server and CUnify security permissions. ACH transmission is controlled via the Catalyst ACH Online system TranZact accessed via SSL and Multifactor password tokens. All Catalyst ACH transmissions are submitted thru the TranZact system. Fiserv CUnify online transmissions are made via secure MPLS to the Fiserv CUnify data center. ACH data transmitted to the Federal Reserve is conducted via the Fedline ACH VPN appliance in accordance to Federal Reserve recommended security settings, Fedline users authenticate via browser based SSL certificate and the FedLine security token which is a two-factor security device used to uniquely identity individuals accessing the Federal Reserve.

9. **INTRUSION DETECTION.** The Information Security Committee is responsible for the compilation, regular maintenance, and annual testing of contingency plans for all Credit Union information systems, including the creation of an Intrusion Response Plan and coordination of an Intrusion Response Team. This Team is mobilized in the event of a hacker intrusion, a virus infection, and other security-related events. The Credit Union shall also ensure that its contracts with service providers require the service providers to disclose any information regarding any breach of security resulting from unauthorized intrusion into the

credit union's member information system maintained by the service provider.

i. **Actions Taken in the Event of an Intrusion.** In the event of an intrusion, the Credit Union will undertake the following actions as soon as possible:

a) Assess the nature and scope of the incident and identify each member information system and types of member information that have accessed or misused;

b) Notify the appropriate authorities as set forth below;

c) Take prompt and appropriate measures to prevent further unauthorized access or use of member information which may or may not including monitoring, freezing or closing affected accounts if feasible and appropriate, while preserving records and other evidence;

d) Notify members when such notice is warranted and in accordance with the Guidance and notice format promulgated by the NCUA/FTC; and

e) Take appropriate and prompt corrective measures.

ii. **Preventing Computer Viruses and Similar Intrusions**. A computer virus may cause slower computer response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of Credit Union's computers.

a) **Screening Programs Enabled.** To assure continued uninterrupted service, for individual computers and networks, all computer Users must keep current versions of approved virus screening software that the Information Technology Manager enabled on their computers and not bypass the scanning process. If possible, approved virus screening software shall be centrally managed by the Information Technology Manager or Department.

b) **Eradication Process.** If Users suspect infection by a computer virus, they must immediately stop using the infected computer and contact the Information Technology Manager.

c) **Software Sources.** To prevent problems with viruses, and Trojan horses, Credit Union computers and networks must not run software that comes from sources other than those approved by

the Information Systems Manager or other authorized person at the Credit Union.

iii. **Disaster Recovery.** The Credit Union will take whatever measures necessary to protect against destruction, loss, or damage of member information due to potential environmental hazards, such as fire and water damage or technical failures and outside intrusions. The Information Security Program will test for disaster recovery alone but will be included in the overall Disaster Recovery Plan for the Credit Union.

a) These measures shall include the development of a disaster recovery plan to prepare for catastrophic acts. The Credit Union will evaluate potential threats, establish business impact levels, and determine critical systems and necessary resources through ongoing risk assessment activities. The disaster recovery plan will include the following information and procedures, at minimum:
   - ✓ Roles and responsibilities;
   - ✓ Record preservation methods;
   - ✓ Alternate storage and processing site provisions;
   - ✓ Alternate telecommunications service provisions;
   - ✓ Communication methods for employees and members; and,
   - ✓ Notification of regulators.

b) Management will train employees on their roles and responsibilities in the disaster recovery plan. The Credit Union will test contingency and disaster recovery assumptions annually. Testing results will be documented and reported to Credit Union officials. Disaster recovery and contingency plans will be coordinated with the Credit Union's risk assessment and Business Continuity Plan. The disaster recovery plan will be documented and submitted to the Board and/or Supervisory Committee for approval.

c) **Back-Up Responsibility and Schedules.** To protect the Credit Union's information systems/facilities from loss or damage, the Information Technology Manager is responsible for making periodic back-ups. All critical member information resident on Credit Union computer systems and networks must be periodically backed-up. The Information Technology Manager will define which member information and which programs/systems are to be backed-up, the frequency of back-up, the type of back-up, and the method of back-up. Secure storage of back-up media is the responsibility of the Information Technology Manager. Storage media from multi-user systems may be stored in fireproof safes, at a separate location at least several city blocks away from the system being

backed-up and physically protected against unauthorized access.

iv. **Monitoring.** Management will be responsible for regularly monitoring its information systems for detection of any intrusions. Computer systems handling member information must securely log all significant computer security relevant events. The Information Technology Manager , or person designated by the Information Technology Manager , will monitor and review system logs in real time, at least daily, and will implement a real time alert mechanism. Log records will contain information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome, and the identity of any individuals or subjects associated with the event. Logs containing computer security relevant events must be retained for at least 12 months. During this period, logs may be accessible only by authorized persons.

10. **RESPONSE PROGRAM.** Management will be responsible for developing and implementing a risk-based response program to address incidents of unauthorized access to member information, pursuant to the Credit Union's Incident Response Policy.

11. **CREDIT UNION SYSTEMS AND FACILITIES USE POLICY.**

i. **Off-Site Physical Security.** At alternative worksites, reasonable precautions should be taken to protect Credit Union hardware, software, and member information from theft, damage, and misuse. The Credit Union maintains the right to conduct inspections of telecommuter offices with one or more days advance notice. All employees who keep member information at their homes in order to do Credit Union work must have furniture, which can be locked, for the proper storage of this information. Telecommuter employees will have adequate means to communicate with Credit Union response personnel in the event of security incidents.

a) **Off-Site Systems.** Computer systems provided by the Credit Union may **not** be modified in any way without the knowledge and authorization of the Information Technology Manager. Similarly, employees may not bring their home computers into the office to process member information without prior approval from the Information Technology Manager. Employees in the possession of portable, laptop, notebook, palmtop, and other transportable computers containing member information must not leave these computers unattended at any time.

b) **Portable Storage Media.** Whenever member information is written to a floppy disk, magnetic tape, smart card, or other storage media, the storage media must be marked. When not in use, this media must be locked in a safe, furniture, or a similarly secured location. Member information stored on portable storage media will be encrypted.

c) **Removal of Information.** Member information may not be removed from Credit Union premises unless there has been prior approval from the Information Technology Manager. This policy includes member information stored on portable computer hard disks, floppy disks, hard-copy output, paper memos, and the like. An exception is made for authorized off-site back-ups.

d) **Remote Printing.** Printers must not be left unattended if member information is being printed or will soon be printed. The persons attending the printer must be authorized to examine the information being printed. Unattended printing is permitted only if the area surrounding a printer is physically protected such that persons who are not authorized to see the material being printed may not enter.

ii. **Personal Use.** Unless a contractual agreement specifies otherwise, all information stored on or transmitted by Credit Union computer and communications systems is Credit Union property. Management reserves the right to examine all information stored in or transmitted by these systems. Employees will have no expectation of privacy associated with the information they store in or send through these systems.

a) **Activity Monitoring.** Employees may be subject to electronic monitoring while on Credit Union premises and while using Credit Union information systems. In areas where there is a reasonable expectation of privacy, such as rest rooms, dressing rooms, and locker rooms, no electronic monitoring will be performed.

b) **Information Inspection and Removal.** At any time and without prior notice, Management reserves the right to examine archived electronic mail, personal file directories, hard disk drive files, and other information stored on Credit Union information systems. The Credit Union additionally retains the right to remove from its information systems any material it views as offensive or potentially illegal.

c) **Personal Use and Precautions.** Employees are prohibited from using Credit Union time, facilities, equipment or supplies for private gain or advantage. Personal use is allowed pursuant to the Credit Union's Electronic Communications/Acceptable Use policy. Users must take steps to prevent member information from being inadvertently damaged or destroyed. Smoking, eating, and drinking may not be done while using computers. Likewise, magnetic media should be kept away from heat (such as direct sunlight) as well as magnetic fields.

iii. **Software Licenses.** The Credit Union purchases licenses granting the use of software programs used by employees in the conduct of Credit Union business. Unauthorized software copying is prohibited. Users may not copy software provided by Credit Union to any storage media (floppy disk, magnetic tape, etc.), or disclose software to outside parties without written permission from the Information Technology Manager. Ordinary back-up copies are an authorized exception to this policy. Unless specifically authorized by the Information Technology Manager, Credit Union employees may not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security.

iv. **Internet Connections.** Employees are discouraged from accessing the Internet with Credit Union computers and networks except in the course of Credit Union business. (see the credit unions' Electronic Communications/Acceptable Use policy)

v. Internet access is permitted only through Credit Union firewalls. Employees are not permitted to employ dial-up lines and an Internet Service Provider (ISP) to reach the Internet from computers located in Credit Union offices, without express approval of the Information Technology Manager.

a) **Third Party Identification.** Release of specific member related member information to that specific member shall be only through the Credit Union encrypted Internet Banking system or over the telephone if the Internet Banking system cannot provide secure transmission of the message.

b) **Disclaimers and Removal of Public Postings.** Whenever an employee posts a message to an Internet discussion group (listserv), an electronic bulletin board, or another public information system, this message must be accompanied by words clearly indicating that the comments do not represent the official position

of the Credit Union. Any electronic mail sent by Credit Union employees to Internet discussion groups, electronic bulletin boards, or other public forums may be reviewed and removed by Information Technology Manager if determined to be inconsistent with the Credit Union's business objectives or existing policy.

c) **Setting-Up Web Pages.** Users must not place Credit Union material on any publicly accessible computer system (including Internet web pages) unless first approved by the Information Technology Manager. Similarly, users are prohibited from establishing any electronic commerce arrangements over the Internet unless first obtaining approval by the Information Technology Manager.

d) **Handling Materials Down-Loaded from the Internet.** All software and files down-loaded from non-Credit Union sources via the Internet (or any other public network) should be screened with virus/intrusion detection software, prior to decompression and prior to being run or examined via another program such as a word processing package.

12. **PROGRAM REVIEW.**

i. **Independent Review of Information Technology Function**. Annually, the Supervisory Committee will approve and engage a qualified organization to perform an independent review of the Information Technology Function to comply with Georgia Department of Banking and Finance rule 80-2-6-.01(5). The results of the independent review will be submitted to the Supervisory Committee and reported to the Board of Directors.

ii. **Program Review.** Subsequent to annual vulnerability testing, the Information Technology Manger and the Information Technology Committee will seek to adjust, as appropriate, the Program in light of any relevant changes in technology, the sensitivity of Credit Union member information, internal or external threats to member information, and Credit Union changing business arrangements and changes to member information systems. The findings of this review will form the basis of the annual report to the Board.

iii. **Security Controls Testing.** Management will regularly test the key controls, systems and procedures of the Program to confirm that they control the risks and achieve the overall objectives of the Program at least annually. An independent third party or staff independent of the

individuals who develop or maintain the program will test the program. Testing will include an assessment of exterior defenses, internal security, physical security, and administrative procedures. A managed security service may be used to periodically scan firewall and web servers for resident hacking programs as the Committee deems necessary.

iv. **Training.** Management will train Credit Union staff to recognize, respond, and report to regulatory and law enforcement agencies, any unauthorized or fraudulent attempts to obtain member information. Additionally, staff shall be trained to recognize and report insider threat behaviors, including but not limited to, attempts to gain unauthorized access to sensitive member information and policy violations. The Compliance and Training Officer or the Information Technology Manager is responsible for training the Information Systems staff, Custodians, and Users in the provisions of this Policy, and pertinent Program procedures and standards. Specialized training and development programs will be provided to employees who have information security responsibilities.

v. General and specialized information security training activities will be documented. A Training Calendar will be maintained for all staff training including specific IT training as well as the IT Department staff training. Documentation shall be retained according to the Credit Union's information retention schedule. Training on the Disaster Recovery Plan and Procedures will be conducted at least annually for all staff members. Training on specific job duties and responsibilities will be conducted during orientation of new staff members as well as ongoing specific job-related IT risks. IT Training for IT risks to the credit union will be conducted at lease annually.

vi. The IT Department staff will receive training on the core data processor, Fiserv CUnify, at least twice a year.

vii. The IT Department staff will receive training on IT related current risks and other industry related topics at least quarterly.

viii. **Outsourcing of Services**. Management will implement a risk management process for outsourcing services, under the direction of the Board, pursuant to the Credit Union's Vendor Due Diligence and Oversight policy (See Policy Third Party Due Diligence & Oversight).

13. **INFORMATION HANDLING AND RETENTION.** Management will be responsible for ensuring that member information is retained and disposed according to Credit Union guidelines. Information retention procedures will be coordinated with related areas of the information security program including, but

not limited to, security incident response planning, business continuity planning and disaster recovery planning.

## Review

The Information Security Policy must be reviewed at least annually by the Information Technology Committee and changes or updates reported to the Board of Directors.

## I have read and understand The Information Security Policy.

Dated this_____day of_____,_____

Employee Name _____

Employee Signature _____