Family First Credit Union

Website Policy

General Policy Statement:

Family First (Credit Union) maintains a website that is hosted by EarthLink Web Hosting. All content is developed and maintained by GCUA (Georgia Credit Union Affiliates). Using the World Wide Web (Web) is strongly encouraged in that it provides the Credit Union with a tool to convey information quickly and efficiently on a broad range of topics relating to its products, services, activities, objectives, policies and disclosures.

The Credit Union offers the following services electronically:

Informational Website
Online Banking
Mobile Banking
Mobile Check Deposit
Online Bill Pay
On-line Consumer Loan Application
Money Desktop
Financial Calculators
Resources and Links
Form and Application Database
Credit Card Account Access (Link)
Flashcard (Link)
Check Ordering (Link)
Car Buying Service (Link)
ACCEL Member Financial Counseling (Link)
Budget Smart (Link)
Money Cents (Link)
Accidental Death and Dismemberment Insurance (Link)
First Mortgage Loans (Link)
Credit Reports (Link)

Guidelines:

1. POLICY AND PROGRAM RESPONSIBILITY

i. The Credit Union will establish an oversight committee, made up of the following staff, to maintain and monitor the Credit Union's website:

- Executive Management
- Marketing Management

- Information Technology Management
- Operations Management
- Compliance Management

ii. Each division of the oversight committee is responsible for maintaining the Credit Union's website operations. Any new website ideas or initiatives must be reviewed by the oversight committee or approved by the CEO which will prioritize, develop, acquire, and maintain any approved website applications.

iii. Management has established long-term strategic and short-term tactical plans for its E-commerce activities. The Board of Directors has approved these plans. The Information Technology Manager provides management with regular reports on its website transactions.

iv. Management together with the appropriate departments shall work together to provide the necessary resources to adequately support website operations to include equipping staff with the appropriate tools and staff training.

2. **COPYRIGHTED MATERIAL**. Copyrighted material will be used only when allowed by prevailing copyright laws and may be used only if the materials relate to the website's mission and should be approved by Management prior to use.

3. **EXTERNAL LINKS.** When external links to non-Credit Union websites are included, the Credit Union is responsible for ensuring that a disclaimer is made that neither the Credit Union nor the organization endorses the product at the destination, nor does the Credit Union exercise any responsibility over the content at the destination.

4. **RISK ASSESSMENT**

i. The Credit Union regularly tests the efficiency of its E-commerce systems to ensure proper working order and to prevent security weaknesses.

ii. Management has classified the level of data sensitivity, as well as the potential security risks in the event of a security breach. Management has procedures in place to handle the different levels of intrusion.

iii. The Credit Union regularly monitors security risks associated with technological and operational changes in E-commerce and maintains a current list of critical website applications and data that is categorized, quantified, and prioritized.

5. COMPLIANCE AND LEGAL

i. The Credit Union ensures that its website will comply with all applicable laws and regulations. The Credit Union also monitors all changes in laws and regulations that affect E-commerce, and updates its E-commerce policies, practices, and systems accordingly in a prompt manner.

ii. The Credit Union has secured bond coverage for all of its website policies and procedures. Management has ensured that bond coverage is sufficient in the event of any loss due to an electronic transaction. Bond coverage is regularly assessed to ensure the sufficiency of coverage.

iii. The Credit Union provides disclosures regarding its website policies and procedures to members who have entered into E-Commerce relationships with the Credit Union. The disclosures also provide a list of the service providers who have a direct business relationship with the Credit Union. In addition, the Credit Union will place appropriate warnings on its website, clearly stating that unauthorized access or use of the website is not permitted and may constitute a crime punishable by law.

iv. The Credit Union maintains a website privacy disclosure that is available to all members who visit the Credit Union website. The Credit Union monitors and enforces compliance with its website privacy disclosures.

v. The Credit Union monitors its website on a regular basis to ensure that all disclosures are accurate and up-to-date. The Credit Union will create procedures to validate transactions, e-mails, and other contractual obligations relating to its website.

6. AUDIT AND CONSULTING SERVICES

i. The Credit Union's website activities will be subject to both independent audits and quality reviews, at least annually, and more frequently when appropriate. At a minimum, these reviews will cover website: security, penetration testing, regulatory compliance, privacy, application development and maintenance, incident response and business continuity, and virus detection and protection. The Credit Union management will correct the issues of concern uncovered by the independent audit and/or quality review.

ii. The Credit Union management regularly requires performance testing of its website to identify and prevent potential vulnerabilities.

7. **VENDOR MANAGEMENT** (optional). The Credit Union has obtained a vendor to install and/or maintain its website. The Credit Union has exercised due diligence

in selecting its vendor to ensure that proper security measures are in place to protect member account information. The Credit Union will work with the web hosting vendor to ensure the operational integrity and security of the computer and network supporting the website are maintained. The Credit Union will develop procedures to monitor vendor relationships to ensure that they continue to meet the needs of the Credit Union (i.e., hardware, software, network services, content accuracy, availability, usability, security, and privacy). The Credit Union will periodically review security procedures employed by vendor to ensure it meets the Credit Union's minimum requirements.

8. MEMBER SERVICE AND SUPPORT

i. Management will take steps to ensure that adequate staff levels and training are in place to address member support issues.

ii. The Credit Union discloses to its members the terms and conditions by which its E-commerce and website transactions are conducted, such as:

a) The Credit Union's website is secure and member account information is kept confidential.

b) Whether the website uses cookies, how they are used, and what the consequences are for not accepting them.

c) How member information can be corrected.

d) How member information is used.

e) How members can receive additional credit union services (advertisements of other credit union products), and how they can opt out of those services.

f) When members will be notified of credit decisions.

g) How members can request more information or inquire into a refusal of credit.

h) Methods of accepted bill payment.

i) When payment will be posted to the member's account (for after-hours transactions).

j) How members can stop payment.

k) The sources of information (i.e. interest rates).

l) Inform members of maintenance or other technical issues that may affect access to E-commerce or website activities through online messages.

m) Where members can go to resolve errors, pose questions, or register complaints.

n) Inform members of their right to receive paper copies of member account information and procedure to obtain paper copies.

9. PERSONNEL

i. Employees with access to member account information will receive a copy of the Credit Union's website policy, must sign a compliance policy statement (confidentiality and information security) when hired by the Credit Union. Employees will be notified of the importance of maintaining the confidentiality of member account information and will be made aware of the Credit Union's policies, procedures, standard practices, and disciplinary actions that will be taken against the employee for non-compliance with the Credit Union's privacy and information security policies and procedures. The Credit Union policy prohibits staff from inappropriately disclosing member account information to any third party.

ii. The Credit Union limits access to sensitive information to specific employees to ensure confidentiality of member account information. Employees have been trained on the proper procedures for filing reports to the appropriate regulatory and law enforcement agencies. Management will routinely monitor employees for compliance with the Credit Union's stated policies, procedures, and standards.

iii. The Credit Union has conducted background checks on its employees, and will thoroughly investigate any allegation of employee misconduct.

iv. Management has instituted a training program in order to maintain continuity of employee support in the event of a termination, transfer, promotion, etc. Employees involved with the Credit Union's website transactions are kept up-to-date with changes in the policies and procedures of the Credit Union.

10. SYSTEM ARCHITECTURE AND CONTROLS

i. The Credit Union maintains an inventory of hardware and software to ensure continuity of service in the event of a technological failure, natural disaster, or intentional destruction of its electronic systems. The Credit Union (or its vendor) maintains procedures to allow the Credit Union to restore its previous configuration in the event a software modification adversely affects the website.

ii. The Credit Union has implemented a disaster recovery system as part of its business continuity plan. This system will be monitored regularly and updated as needed as a result of changes in technology, legislation, and infrastructure.

11. SECURITY INFRASTRUCTURE AND CONTROLS

i. The Credit Union maintains security measures consistent with the requirements of federal and state regulations, including risk management systems designed to prevent unauthorized access, both internal and external, to member information.

ii. Management monitors employees with access to member account information to ensure they are in compliance with the Credit Union's established security policies and procedures.

iii. All member account information is stored on servers protected (See Fiserv CUnify Web SOC report for details about security in place on CUnify Web) to prevent unauthorized access and/or damage. These protections are monitored on a regular basis to assess potential security weaknesses.

iv. Access to member accounts is restricted to members through the use of user ID numbers and passwords. Account passwords that are not entered correctly after five (5) times will result in an automatic log-off to the session.

12. PERFORMANCE MONITORING

The Credit Union has established and implemented performance standards and monitoring procedures for its website activities. These standards and procedures are designed to ensure that the Credit Union's E-commerce and website activities are available and efficiently meet member needs and expectations. These procedures are updated on a regular basis, as a result of changes in long-term and short-term plans, as well as in response to member needs.