Family First Credit Union
E-Commerce Policy

General Policy Statement:

Family First Credit Union will follow the guidelines set forth below for the electronic financial services, products, functions, or activities that the Credit Union performs, provides, or delivers to its members through electronic means ("e-commerce"). Examples of electronic services include automated teller machines, electronic fund transfers, wireless services, remote banking services, online account transaction processing through a website (including bill payment services), website hosting services, account aggregation services, and Internet access services to perform or deliver products or services to Credit Union's members. Aspects of the Credit Union's e-commerce policy relating to the Credit Union's e-commerce operation and activities involve functions and policies set forth in the Credit Union's policies on Information Security, Marketing, Lending, Deposit Activities, Risk Management, and other Credit Union policies that address the Credit Union's e-commerce activities. These policies must be consulted and adhered to as part of the Credit Union's e-commerce policy.

Guidelines:

1. **E-COMMERCE STRATEGY AND MANAGEMENT.** Credit Union Management will prepare and maintain an articulated strategy for engaging in e-commerce and receive the Board of Director's approval.

    i. **Develop a Plan.** Credit Union Management will develop a plan for using e-commerce systems and services, based on the needs of the Credit Union's members and the Credit Union's overall business goals.

    ii. **Services**. Credit Union Management will determine the e-commerce services the Credit Union may offer, for example:

        a) Internet/World Wide Web Services
        b) Wireless Services
        c) Remote Banking (direct dial in) Services
        d) Remote Deposit Capture
        e) Mobile Banking
        f) Online Bill Paying Services
        g) ATM and POS Services
        h) Account Transaction Processing Services, such as:

            • Account Inquiry
            • Check Requests

- Loan Applications
- Bill Payment
- Funds Transfers
- Third Party Transfers
- On-Line Wire Transfers
- Stored Value Cards
- CUnify Web
- E-Wallets
- Automated Clearing House (ACH) Originations
- Any other e-commerce activities and services.

iii. **E-Commerce Oversight Group.** Credit Union Management will establish a centralized e-commerce oversight group ("E-Commerce Group"), comprised of Credit Union management representatives from marketing, compliance, operations (loan and deposit), information systems and security areas of the Credit Union.

iv. **Reports.** 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 E-Commerce Group. The report will include a measurement of e-commerce performance, system/service security and integrity, updated risk assessments, access and physical controls, intrusion detection, data security, business continuity planning, internal and external system tests.

v. **Vendor Management.** Credit Union Management will determine which e-commerce services should be outsourced and which e-commerce services will use in-house systems and personnel. Security related due diligence and compliance of all vendor contracts with federal and state regulations must be addressed at least annually and reported to the Board.

vi. **Member Service and Support**. Credit Union Management or the E-Commerce Group will create a process to adequately track and resolve member support issues (e.g., member technical support, incident reports, and FAQs).

2. **E-COMMERCE SYSTEM ARCHITECTURE**. The Credit Union's Information Technology Manager or Credit Union Management, as appropriate, will develop and maintain appropriate Information Systems and E-Commerce System architecture and computer hardware and software to facilitate the Credit Union's e-commerce strategy and activities as follows:

i. **Diagrams.** The Credit Union's Information Technology Manager will create and maintain network, system and application diagrams (i.e. topologies).

ii. **Hardware and Software**. The Credit Union's Information Technology Manager will prepare and maintain an inventory of e-commerce hardware and software including all licenses with expiration, termination and renewal dates.

3. **RISK ASSESSMENT.** Prior to implementation, the Credit Union's Board of Directors, Management, and E-Commerce Group will assess the risks associated with its e-commerce activities. The E-Commerce Group will periodically update and re-assess the risks associated with the Credit Union's e-commerce activities. It also will re-assess the risks whenever a new e-commerce delivery system, vendor, service provider or product is adopted by the Credit Union. Risks to be assessed include:

   i. Operational and transactional risks, including outsourcing arrangements for technology services.

   ii. Type of member (person or business).

   iii. Transactional capabilities.

   iv. Volume of transactions.

   v. Confidentiality of member information involved in e-commerce activities

   vi. Legal and compliance risks.

   vii. Security risks.

   viii. Risks to the Credit Union's reputation and business continuity.

4. **COMPLIANCE AND LEGAL ISSUES.** The Credit Union's Board of Directors, Management, and E-Commerce Group will ensure that the Credit Union's e-commerce activities comply with applicable federal and state regulations and that its electronic delivery systems and services are legally sufficient to protect the Credit Union.

   i. **Legal Review.** E-commerce contracts, third party service provider contracts, and other transactions will be reviewed by the Credit Union's Management and if needed, legal counsel. All e-commerce contracts should be clearly written and sufficiently detailed to provide assurances for performance, reliability, security, confidentiality, and reporting.

ii. **Compliance Review.** Credit Union Management and the E-Commerce Group will perform a compliance review of all e-commerce products, services, and member agreements and disclosures prior to implementation. Credit Union Management and the E-Commerce Group will perform periodic compliance examinations, no less than annually, subsequent to the product or service implementation. Such a compliance review will include compliance with all applicable state and Federal regulations and guidance..

iii. **Bond Coverage.** The Credit Union's Board of Directors and Management will maintain adequate bond coverage to cover the Credit Union's anticipated e-commerce activities, pursuant to the Credit Union's Bond and Insurance Coverage policy.

5. **AUDIT AND CONSULTING.** Credit Union Management and the E-Commerce Group will develop and maintain appropriate audit and consulting services to facilitate and protect the Credit Union's e-commerce activities as follows:

   i. **Audit.** Credit Union Management and the E-Commerce Group, or their authorized agent(s), will perform periodic internal and external (Service Organization Controls (formerly SAS 70), if available, and financial statement) audits and quality reviews.

   ii. **Test**. Credit Union Management and the E-Commerce Group will supervise, and outsource where appropriate, the performance of system vulnerability testing, as set forth more fully in the Credit Union's Information Security Policy.

   iii. **Correct.** Credit Union Management and the E-Commerce Group will prioritize issues disclosed in the most recent audit or quality review and correct any identified vulnerabilities or outstanding issues.

6. **PERSONNEL.** Credit Union Management and the E-Commerce Group will develop and maintain appropriate recruitment, training, and employee access to e-commerce systems to facilitate and protect the Credit Union's e-commerce activities as follows:

   i. **Recruit and Train.** Credit Union Management will recruit e-commerce technical staff and train Credit Union employees with respect to e-commerce strategy.

   ii. **Segregate.** Credit Union Management will segregate duties between conflicting e-commerce related responsibilities.

   iii. **Employee Access**. Credit Union should consult the Credit Union's Information Security Policy for the Credit Union's policy relating to employee

> access to e-commerce systems due to status changes, i.e. terminations, transfer, or promotion.

7. **DATA SYSTEM AND SECURITY**. Credit Union Management and the E-Commerce Group will ensure the adequacy of data systems to support the Credit Union's e-commerce goals. The Credit Union's policy for the system security is set forth more fully in the Credit Union's Information Security Policy.

   i. **Disaster Contingency Plan.** Credit Union should consult the Credit Union's Information Security Policy for the policy relating to e-commerce and the Credit Union's disaster contingency plan.

   ii. **System Diagrams.** The Credit Union's Information Technology Manager and E-Commerce Group will plan and maintain e-commerce system diagrams and information.

   iii. **Monitoring and Reporting**. The Credit Union will monitor activity and use of e-commerce to detect unauthorized access. In the event that systems are breached Local, State and Federal laws will be followed and the appropriate authorities will be contacted, including reporting to the NCUA Regional Director.

   iv. **Classification of Data.** The Credit Union Management and E-Commerce Group will create classification of different types of data based on its value to the Credit Union, sensitivity, and degree of harm if the data is compromised, lost, or accessed by unauthorized persons.

   v. **Security System Requirements.** Credit Union Management and the E-Commerce Group will create and maintain requirements for security systems and procedures to protect critical data and facilities, as set forth in the Credit Union's Information Security policy.

   vi. **Threats to Data Security**. Credit Union Management and the E-Commerce Group will monitor threats to data security, as set forth in the Credit Union's Information Security policy.

8. **MEMBER AWARENESS**. The Credit Union will take measures as necessary to educate members to the risks of account fraud and identity theft.