Family First Credit Union

Incident Response Policy

Purpose

Family First Credit Union will set the guidelines for management and staff to use in establishing and maintaining policies and procedures to address incidents of unauthorized access to 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.

Responsibility and Authority

The Credit Union will ensure that incidents of unauthorized access to member information are addressed immediately, including notice to the membership as well as the proper authorities. 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 address incidents of unauthorized access to 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.

Family First Credit Union recognizes its responsibility to safeguard member information and will treat the private financial information of the Credit Union's members ("member information") with appropriate care in order to maintain the confidentiality, integrity and security of member information**.**

Definitions:

Event

Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring (Reference – Committee on National Security Systems) (CNSSI-4009). Events occur without supporting log evidence of incident.

Event examples:

- Employee visits website prohibited by policy
- Brief exposure of unpatched system
- Limited service disruption

Incident
An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system process, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies (Reference – NIST SP 800-53). Incidents may include, but are not restricted to, the following: violation of policy, unauthorized information system use, denial of resources and information system changes without consent.

Incident examples:

- Malicious hacker gains unauthorized access to database containing sensitive member information
- Criminal commits fraud by manipulating transaction data
- Distributed denial-of-service (DDoS) attack launched against critical Credit Union information system resources
- Ransomware deployed through phishing email campaign

References:

National Institute of Standards and Technology (NIST). Special Publication 800-53 (Rev. 4) Security Controls and Assessment Procedures for Federal Information Systems. Incident Response Control Family.
NIST. Special Publication 800-61 (Rev. 2) Computer Security Incident Handling Guide.

Guidelines:

1. **RESPONSE PROGRAM.** Management will be responsible for developing and implementing a risk-based response program to address incidents of unauthorized access to member information.

    i. **Security Response Team and Security Response Leader.** Credit Union management shall establish a security response team responsible for preventing, detecting and handling suspected incidents involving member information. The team will have a designated [team leader] as well as a deputy team leader who assumes authority in the absence of the team leader. Members of the team shall be adequately trained and equipped to develop, document and enact an Incident Response Plan. Team members should include personnel from several Credit Union departments including, but not limited to, the following: information technology, business management, legal, human resources, internal auditing, and facilities. Involving personnel from multiple departments ensures that the Incident Response Plan will cover mission-critical business processes, systems, and information assets.

In lieu of creating a security response team, the Credit Union shall appoint a single employee to be in charge of incident response. The incident response leader will work with internal personnel and third-party service providers to ensure that an Incident Response Plan is in place, incorporates appropriate third-party services, is tested, and is approved by Credit Union officials.

Lastly, either the security response team or the leader will be responsible for acquiring outsourced incident response services, as needed, to ensure that the Credit Union has access to the requisite knowledge and tools to handle security incidents.

ii. **Service Providers.** Contracts with service providers will stipulate that the provider take appropriate actions to address incidents of unauthorized access to or use of the Credit Union's member information, including notification to the Credit Union as soon as possible of any such incident, to enable the Credit Union to implement its Incident Response Plan in a timely manner.

iii. **Incident Severity Levels.** The security response team or leader will develop criteria for measuring the severity of incidents based on their impact to business functions, their impact to member information, and the amount of effort and time required to recover from them (Reference – NIST SP 800-61 pp. 32-33).

iv. **Incident Response Preparedness.** The Credit Union shall prepare an incident response toolkit containing items for effective administration and communication of the Incident Response Plan (e.g., smartphones and contact information) as well as dedicated incident response hardware and software (e.g., laptops, blank removable media, and packet sniffers). The Credit Union will be prepared to handle incidents arising from common methods of attack.

v. **Incident Detection.** The Credit Union shall monitor information system events to detect indicators of information security incidents and threats to sensitive member information. To facilitate forensic activities, event data produced by system monitoring tools will be regularly backed up and protected from unauthorized access. Examples of security incident indicators include the following: IDS/IPS alert; physical evidence of break-in or theft of assets; or a threat made to the Credit Union. The security response team leader will have the authority both to define what events constitute incidents and to define what events must be monitored.

vi. **Assessment of Incident.** The security response team will assess the nature and scope of an incident and identify what member information has been accessed or misused. The team will use the severity levels defined in Section 1.C to prioritize incident response actions.

vii. **Containment and Control.** Appropriate steps will be taken to contain and control an incident to prevent further unauthorized access to or use of member information, while preserving records and other evidence. Examples include monitoring, freezing or closing affected accounts. The security response team shall work to secure and preserve evidence by acquiring and protecting a system snapshot or record before further actions are taken. The team will establish a chain of custody for evidence and ensure that all incident response activities are documented. The team leader will witness and record the technical team members' evidence handling tasks.

viii. **Recovery.** The Credit Union recognizes that restoring the affected information system to a trusted state will require skilled technicians, dual-control procedures and a potentially significant interruption of services. Possible remediation of the vulnerabilities that resulted in the incident will be included in the recovery process. The Credit Union will, as practicable, heighten monitoring on mission-critical information system assets potentially affected by the incident.

ix. **Internal Reporting.** Following discovery of an intrusion or disaster to the Credit Union's systems or facilities, the CEO or acting Senior Management officer shall report to the Chairman of the Board and to the Supervisory Committee as soon as reasonably possible following a receipt of a report of an intrusion or disaster and the initial implementation of the Incident Response Plan.

x. **External Reporting.** Following discovery of an intrusion or disaster to the Credit Union's systems or facilities and upon completion of internal reporting and implementation of the Incident Response Plan, management will report the incident to its bonding company, casualty insurance company, local law enforcement agencies, the appropriate regulatory agency and complete and file a Suspicious Activity Report (SAR) as necessary.

xi. **Post-Incident Activities**

a) After an incident has been handled, the security response team will produce a report containing, but not limited to, the following information regarding the incident:

- Scope
- Cause and costs
- Short-term and long-term impacts
- Short-term and long-term recovery expectations
- Lessons learned

b) By documenting lessons learned, the security response team will determine what aspects of the Incident Response Plan must improve and consider adding or improving information security controls to avoid repeat incidents. Vulnerabilities that were not remediated as part of incident handling will be documented and a plan of action will be devised to remediate them. Incident response evidence shall be retained for attacker prosecution purposes. All post-incident activities must be reported to Credit Union officials and approved by the Board and/or Supervisory Committee.

xii. **Denial-of-Service and Ransomware Incidents.** To mitigate the impact of denial-of-service (i.e. attrition) attacks, the security response team will, if possible, leverage boundary protection devices to filter traffic, increase capacity and bandwidth, and/or employ service redundancy (Reference – NIST SP 800-53). To respond to a ransomware attack, the security response team will work to recover the data from backups if possible, or contact a predetermined third-party service provider capable of rendering assistance.

xiii. **Notifying Members.** As per NCUA requirements specified in 12 CFR Part 748 Appendix B, members will be notified of an incident when it is warranted. When an incident occurs on information systems maintained by service providers, the Credit Union will notify the appropriate regulatory authority and its members. (The service provider contract may authorize the service provider to meet these obligations, but the Credit Union incident response leader will be ultimately responsible to ensure that this is done.) More details regarding member notification policies are provided in Section 2 of this Policy.

xiv. **Staff Training.** Management will develop procedures to ensure that staff is trained to appropriately handle member inquiries and requests for assistance. Staff shall be trained to be able to detect suspicious activity and to know how and to whom to report the activity. This training will be

conducted both prior to and after an actual incident. Members of the incident response team shall receive adequate training to carry out their duties in the Incident Response Plan. General training and specialized training shall occur upon hire or initial adoption of responsibilities and at a Credit Union-defined frequency.

xv. **Incident Response Testing.**

a) Management will test the effectiveness of the incident response plan. Examples of effectiveness testing methods include checklists, tabletop exercises, and scenario simulations. Examples of scenarios include, but are not limited to, the following:

- Employee reports suspicious email (i.e. phish)
- Compromised application database revealed by log review
- Intrusion detection system alert triggered on (unscheduled)

b) Incident response testing results shall be documented, incorporated as lessons learned in incident response improvement efforts, and reported to Credit Union officials. Incident response testing shall occur at a Credit Union-defined frequency. All incident response testing plans will be submitted to the Board and/or Supervisory Committee for approval.

2. MEMBER NOTICE. Notification to members will be made timely in order to minimize the Credit Union's reputation and legal risks. Member notice procedures shall adhere to NCUA guidance in 12 CFR Part 748 Appendix B.

i. **Investigation.** Once the Credit Union becomes aware of an incident of unauthorized access, the Information Technology Manager or security response team will conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the likelihood is high, the affected member(s) will be notified as soon as possible. However, if an appropriate law enforcement agency determines that such notice would interfere with a criminal investigation and provides a written request for delayed notification, notice to the member(s) will be provided as soon as it would no longer interfere with the investigation.

ii. **Affected Members.** Notification may be limited to those members to whom the Credit Union knows to have been affected by an intrusion whenever the Credit Union believes misuse of the information has occurred or is reasonably possible. If a group of files has been accessed improperly, but the Credit Union is unable to specify the affected members and the misuse of their information is likely, the Credit Union

will notify all of the members in the group.

iii. **Content of Member Notice.** Notice to members will contain the following information:

a) A description of the incident in general terms and the type of member information that was the subject of unauthorized access or use;

b) What the Credit Union has done to protect the members' information from further unauthorized access;

c) The telephone number that the member can call for further information and assistance;

d) A reminder that the member needs to remain vigilant over the next 12 to 24 months, and to promptly report incidents of suspected identity theft to the Credit Union;

e) A recommendation that the member review account statements and immediately report any suspicious activity to the Credit Union;

f) A description of fraud alerts and an explanation of how the member may place a fraud alert in the member's consumer reports to put the member's creditors on notice that the member may be a victim of fraud;

g) A recommendation that the member periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted; and

h) Information about the availability of the Federal Trade Commission's (FTC) online guidance regarding steps a consumer can take to protect against identity theft. The notice will encourage the member to report any incidents of identity theft to the FTC, along with the FTC's website address and toll-free telephone number.