MEMBERS 1ST CREDIT UNION
CHARGE-OFF POLICY

Revised May 2024 Approved 05/16/2024

PURPOSE

The Charge-off Policy has three main purposes:

- To insure the timely recognition of losses and adjustment for nonperforming assets
- To provide full and fair disclosure of statutory reserves on the financial statement
- To provide guidance for staff preparation of recommendations to the Board of Directors for charge-off action

This policy is intended to cover the charged off loan (including VISA cards) and deposit losses.

PROCESS

Every month, Members 1st Credit Union ("Credit Union") staff will prepare a written report of any deposit accounts that have been charged off due to negative balances. The Credit Union staff will also prepare a written report of loans recommended to be charged-off. Both these reports will be presented to the Board of Directors for acknowledgement and / or approval. Prior to submitting these reports, each account will be reviewed by the Collection staff. Any action by the board will be recorded in the minutes and charged-off loans and deposit items will become a permanent attachment to the minutes.

CHARGE-OFF REQUIREMENTS

Prior to an account being charged off, collection department staff will transfer all funds on deposit, that are legally available, to the loan. To avoid violating the automatic stay, members who have filed for bankruptcy will have shares transferred after a discharge and dismissal has been granted by the court.

A loan that reaches any status listed below should be submitted to the Board of Directors and recommended for charge-off:

- A loan in bankruptcy, within 60 days of receipt of notification of filing from the bankruptcy court, unless the Credit Union can clearly demonstrate and document that repayment is likely to occur. Examples of likely repayments are: payment approved by bankruptcy court under Chapter 13 repayment plan; signed reaffirmation agreement; and payments to be made by comakers or guarantors that did not file bankruptcy.

- Loans with collateral may be written down to the value of the collateral, less cost to sell. If the court lowers the amount that the borrower must pay, the Credit Union should immediately charge off that portion of debt discharged by the court.

- A delinquent loan in the hands of an attorney or collection agency, unless there are extenuating circumstances to indicate the Credit Union will collect the loan.

- An estimated loan loss, where the Credit Union has repossessed, but not yet sold, collateral on hand. The Credit Union may transfer the loan balance into the Collateral in process of Liquidation account and should charge off any outstanding loan balance in excess of the value of the property, less cost to sell. Unless the borrower redeems the collateral, the Credit Union will make the necessary General Ledger (GL) entries within 10 days after the "Notice of Intent to Sell" letter has been sent, or prior to the NCUA Call Report filing, if this occurs first.

- An estimated loan loss, where the Credit Union has foreclosed, but not yet sold the property securing the Real Estate loan at the Fair Market Value of the property. The Credit Union should transfer the loan balance into the Other Real Estate Owned (OREO) account and should charge off any loan balance in excess of the value of the property, less the cost to sell. Unless the borrower redeems the collateral, the Credit Union will make the necessary General Ledger (GL) entries within 10 days of the first "Notice of Sale" is published, or prior to the NCUA Call Report filing, if this occurs first.

- The borrower(s) is deceased and there is little or no likelihood of recovery from the estate or it has been determined that no estate will be opened. In the event an estate is opened, the Collection staff will ensure that the estate has been properly and appropriately notified of the existence of obligation and will file a claim with the appropriate probate court.

- The loan has a deficiency balance from the sale of the collateral and the borrower(s) indicated an unwillingness to make further payments.

- The loan is determined uncollectible by the Collections staff regardless of the number of months delinquent.

- The borrower has been determined to be a "skip" and the credit union has had no contact for more than 90 days.

- A fraudulent loan, no later than 90 days of discovery or when the loss is determined, whichever is shorter and there is no realistic chance that it will be collected.

- The loan is more than 6 months delinquent, unless one or more of the following conditions exist:
    - The borrower is making 75% of the contractual payments, within the last 90 days but cannot qualify for refinancing or modification by the credit union.
    - The Credit Union or the member is waiting for settlement of a documented insurance/bond claim.
    - The borrower is deceased and the Credit Union has substantial reason to expect settlement from the estate, co-makers, guarantors, or relatives.
    - The member is complying with a court ordered payment and is making the payments on time with no missed payments.
    - The credit union has had contact with member and can document reasons for believing loan will be brought to a current status within a reasonable time.

Should any recommended charge-off not be approved by the board, the action and reason(s) will be noted in the meeting minutes.

POST CHARGE-OFF

Charged-off debts should be reviewed from time to time, including those debts assigned to an outside attorney or third-party collection agency, in order to determine whether any changes in the circumstances of the borrower or other party responsible for payment may make recovery possible.

When attempting to collect on a charged-off account, the Credit Union will strive to collect the principal and accumulated interest.

If a member approaches the Credit Union to settle a charge-off account, the proposal should be communicated to the CEO. At that time, it will be decided if the amount offered by the member is acceptable as payment in full. If the settlement leaves an outstanding balance of $600 or greater, a form 1099-C will be completed by Visifi and reported to the Internal Revenue Service, as required (see Exhibit "A" - "What to know about 1099-A & 1099-C" for full list of required events as identified by Internal Revenue Service).

If the amount of the settlement is not acceptable, the CEO will communicate with the Collection staff in an attempt to obtain a just and full repayment of both the principal and interest.

DENIAL OF SERVICES

It is the policy of Members 1st Credit Union to deny credit and other services to those members who have caused the credit union to incur a loss of any sort, and who have not voluntarily repaid the loss or are not in the process of voluntarily repaying the loss. This policy applies to all losses, whether the loss was by bankruptcy or otherwise.

A member who has repaid, in full, the loss incurred by the Credit Union may be eligible to reopen a share account and regain full membership status. In such a case, credit bureaus are informed to reflect the payment in full and subsequent appropriate reporting status.

RECORDS RETENTION

Records will be retained indefinite for all charged-off accounts.

REVIEW

The board of directors will review the Charge-off policy on an annual basis.

Exhibit "A"

WHAT TO KNOW ABOUT 1099-A & 1099-C

Internal Revenue Service (IRS) requires the Credit Union to file Forms 1099-A and/or 1099-C under certain circumstances. **Keep in mind that once these forms have been filed with IRS, the Credit Union will have cancelled the amount owed and can no longer attempt to collect on this debt.**

Form 1099-A - "Acquisition or Abandonment of Secured Property":

- When to file – In the year following the calendar year in which you acquire an interest in the property or first know or have reason to know that is has been abandoned.
- Required to file if debt owed is $600.00 or more.
- "Secured Property" means any real property (i.e., a personal residence) and intangible property that is totally or partially held for business or investment use.
- "Acquisition" occurs when the property is foreclosed upon. (Short Sale and Deed in Lieu of Foreclosure are not 1099-A reportable events. Instead, Form 1099-S should be filed.)
- "Abandonment" occurs when the borrower intended to and has permanently discarded the property from use.
- Potential tax consequences to borrower – Capital Gains Tax

Form 1099-C – "Cancellation of Debt":

- When to file – In the year following the calendar year in which the identifiable event occurs.
- Required to file if debt owed is $600.00 or more for single borrower. Required to file on each borrower if held jointly and debt owed is $10,000 or more.
- "Debt" can be all or part of Principal, Interest, Fees Penalties & cost owed but must be at a minimum, the stated Principal amount.
- "Identifiable Event" means:

    1) A debt discharged in bankruptcy if the Credit Union knows from its books and records that the debt was used for business or investment purposes.
    2) A debt discharged by an agreement between the Credit Union and the member to cancel the debt at less than full consideration.
    3) A debt discharged as a result of the Credit Union's decision to discontinue the collection activity and cancel the debt.
    4) A debt that cannot be collected through the court system due to the expiration of the statute of limitations.
    5) A debt cancelled in receivership or foreclosure in a State or Federal court.
    6) A debt cancelled following the Credit Union's election of foreclosure remedies.
    7) A debt cancelled trough a probate or similar hearing.

- Potential tax consequences to borrower – Reportable income.

General:

- Copy of 1099-A & 1099-C must be filed with IRS and debtor are required to receive a copy of form.
- Record Retention is 4 years from the date of the filed return.
- Form 1099-C can be filed in lieu of Form 1099-A if completing boxes 4, 5 & 7 on Form 1099-C.

Examples of identifiable events and required Form 1099-C filing

1) *A debt discharged in bankruptcy if the Credit Union knows from its books and records that the debt was used for business or investment purposes –*

Example: Most debts discharged in bankruptcy do not require a Form 1099-C. Only those that the Credit Union knows were made for business or investment purposes must be reported. Since Members 1st Credit Union does not offer business purpose loans, this identifiable event should not apply.

2) *A debt discharged by an agreement between the Credit Union and the member to cancel the debt at less than full consideration –*

Example: Joe owes $3,000.00 on a loan. He lost his job and is unable to pay back the full balance. He offers to pay a lumpsum of $2,000.00 and asks that the Credit Union forgives the rest. The Credit Union agrees. They are required to file Form 1099-C for the $1,000.00 deficiency. If the agreement and payment is made in different tax filing periods, the reporting must be filed in the year that the **payment was received**.

3) *A debt discharged as a result of the Credit Union's decision to discontinue the collection activity and cancel the debt –*

Example 1) Janet has a $1,200.00 balance on a loan with the Credit Union. The Credit Union has been unable to collect and learned that Janet has lost her job, moved back with her parents, and has no assets. The Credit Union makes a decision to stop collection activities and charges off the balance. The Credit Union is required to file Form 1099-C for $1,200.00.

Example 2) Jeff cashed a check in the amount of $800.00. The check was returned as unpaid and Jeff's checking account was overdrawn by the full amount of the check. The Credit Union has been unable to collect the funds owed and makes a decision to stop the collection activities and charge off the full negative balance. The Credit Union is required to file Form 1099-C for $800.00 **plus any fees assessed if applicable**.

4) *A debt that cannot be collected through the court system due to the expiration of the statute of limitations –*

Example: John owes the Credit Union $2,000.00 on a debt from a long time ago. The Credit Union decides to attempt collection of the balance owed. John claims that the expiration of the statute of limitations has expired and the defense is upheld in the court. Once the appeal period has expired, the Credit Union is required to file 1099-C for full amount owed.

5) *A debt cancelled in receivership or foreclosure in a State or Federal court –*

Example: If the Credit Union and the member agrees on a short-sale or transfer of title in lieu of foreclosure, and the Credit Union is able but chooses not to pursue collection of the deficiency, the Credit Union is required to file 1099-C for the deficiency.

6) *A debt cancelled following the Credit Union's election of foreclosure remedies* –

Example: The Credit Union forecloses on a property and sells it for less than what is owed. If the Credit Union attorney informs the Credit Union that they are prohibited from collecting the deficiency, the Credit Union is required to file Form 1099-C for the remaining balance.

7) *A debt cancelled trough a probate or similar hearing* –

Example: When Jill passed away, she owed the Credit Union $1,500.00 on an unsecured loan. The Credit Union files a claim against Jill's estate in local Probate Court. The court determines that there are not enough assets in the estate to pay the Credit Union any of the funds owed. The Credit Union is required to file Form 1099-C for the full amount owed.

MEMBERS 1ST CREDIT UNION
CORPORATE CREDIT CARD POLICY

Revised 06/2016 Approved 05/16/2024

Non-personalized corporate credit cards are available for use by employees.

Policy relating to the use of the cards is as follows:

A. Employees should use the card whenever feasible to pay for travel and other business-related expenses.

B. All credit card receipts should be attached to the expense voucher or credit card invoice.

C. Only business-related expenses should be charged to the credit card. Personal expenditures are strongly discouraged. Failure to reimburse the Credit Union for expenses that are personal will be grounds for disciplinary action up to and including termination.

D. Each credit card statement will be audited by the Supervisory Committee, at a minimum, on a quarterly basis.

Failure to adhere to this policy will result in an immediate revocation of the credit card.

POLICY

In order to manage cybersecurity and protect our members from cyber threats, Members 1st Credit Union ("Credit Union") will conduct an ongoing cybersecurity risk assessment. The Credit Union will be using the Cybersecurity Assessment Tool (CAT) which is released by Federal Financial Institutions Examination Council (FFIEC) and can be found at https://www.ffiec.gov/cyberassessmenttool.htm.

The Credit Union's Chief Executive Officer (CEO), with other staff support, is responsible for conducting the assessment annually; review, approve, and support plans to address risk management and control weaknesses; analyze and present results to Board of Directors.

RISK ASSESSMENT

The assessment consists of two parts: Inherent Risk Profile and Cybersecurity Maturity. Upon completion of both parts, management can evaluate whether the Credit Union's inherent risk and preparedness are aligned.

By using the assessment, the Credit Union will be able to enhance the oversight and management of the Credit Union's cybersecurity by:

- Identifying factors contributing to and determining the Credit Union's overall cyber risk.
- Assessing the Credit Union's cybersecurity preparedness.
- Evaluating whether the Credit Union's cybersecurity preparedness is aligned with its risks.
- Determining risk management practices and controls that are needed or need enhancement and actions to be taken to achieve the desired state.
- Informing risk management strategies.

PART 1 - INHERENT RISK PROFILE

The Inherent Risk Profile identifies activities, services, and products organized in the following categories:

• **Technologies and Connection Types -** Certain types of connections and technologies may pose a higher inherent risk depending on the complexity and maturity, connections, and nature of the specific technology products or services. This category includes the number of Internet service provider (ISP) and third-party connections, whether systems are hosted internally or outsourced, the number of unsecured connections, the use of wireless access, volume of network devices, end-of-life systems, extent of cloud services, and use of personal devices.
• **Delivery Channels -** Various delivery channels for products and services may pose a higher inherent risk depending on the nature of the specific product or service offered. Inherent risk increases as the variety and number of delivery channels increases. This category addresses whether products and services are available through online and mobile delivery channels and the extent of automated teller machine (ATM) operations.
• **Online/Mobile Products and Technology Services -** Different products and technology services offered by the Credit Union may pose a higher inherent risk depending on the nature of the specific product or service offered. This category includes various payment services, such as debit and credit cards, person-

to-person payments, originating automated clearing house (ACH), retail wire transfers, wholesale payments, merchant remote deposit capture, treasury services and clients and trust services, global remittances, correspondent banking, and merchant acquiring activities. This category also includes consideration of whether the Credit Union provides technology services to other organizations.

• **Organizational Characteristics -** This category considers organizational characteristics, such as mergers and acquisitions, number of direct employees and cybersecurity contractors, changes in security staffing, the number of users with privileged access, changes in information technology (IT) environment, locations of business presence, and locations of operations and data centers.

• **External Threats -** The volume and type of attacks (attempted or successful) affect the Credit Union's inherent risk exposure. This category considers the volume and sophistication of the attacks targeting the Credit Union.

Management can determine the Credit Union's overall Inherent Risk Profile based on the number of applicable statements in each risk level for all activities. For example, when a majority of activities, products, or services fall within the Moderate Risk Level, management may determine that the Credit Union has a Moderate Inherent Risk Profile. Each category may, however, pose a different level of inherent risk. Therefore, in addition to evaluating the number of instances that the Credit Union selects a specific risk level, management should also consider evaluating whether a specific category poses additional risk.

The following are definitions of risk levels:

• **Least Inherent Risk** – The Credit Union generally has very limited use of technology. It has few computers, applications, systems, and no connections. The variety of products and services are limited. The Credit Union has a small geographic footprint and few employees.

• **Minimal Inherent Risk** – The Credit Union generally has limited complexity in terms of the technology it uses. It offers a limited variety of less risky products and services. The mission-critical systems are outsourced. The Credit Union primarily uses established technologies. It maintains a few types of connections to members and third parties with limited complexity.

• **Moderate Inherent Risk** – The Credit Union generally uses technology that may be somewhat complex in terms of volume and sophistication. The Credit Union may outsource mission-critical systems and applications and may support elements internally. There is a greater variety of products and services offered through diverse channels.

• **Significant Inherent Risk** – The Credit Union generally uses complex technology in terms of scope and sophistication. It offers high-risk products and services that may include emerging technologies. The Credit Union may host a significant number of applications internally. It allows either a large number of personal devices or a large variety of device types. The Credit Union maintains a substantial number of connections to members and third parties. A variety of payment services are offered directly rather than through a third party and may reflect a significant level of transaction volume.

• **Most Inherent Risk** – The Credit Union uses extremely complex technologies to deliver myriad products and services. Many of the products and services are at the highest level of risk, including those offered to other organizations. New and emerging technologies are utilized across multiple delivery channels. The Credit Union may outsource some mission-critical systems or applications, but many are hosted internally. The Credit Union maintains a large number of connection types to transfer data with members and third parties

PART II - CYBERSECURITY MATURITY

The Cybersecurity Maturity part of the Assessment is intended to determine the Credit Union's maturity level within each of the following five domains:

- Domain 1: Cyber Risk Management and Oversight
- Domain 2: Threat Intelligence and Collaboration
- Domain 3: Cybersecurity Controls
- Domain 4: External Dependency Management
- Domain 5: Cyber Incident Management and Resilience

Within each domain are assessment factors and contributing components. Under each component, there are declarative statements describing an activity that supports the assessment factor at that level of maturity.

- Domain 1 - Cyber Risk Management and Oversight addresses the board of directors' oversight and management's development and implementation of an effective enterprise-wide cybersecurity program with comprehensive policies and procedures for establishing appropriate accountability and oversight. The assessment factors are:
    - Governance which includes oversight, strategies, policies, and IT asset management to implement an effective governance of the cybersecurity program.
    - Risk Management which includes a risk management program, risk assessment process, and audit function to effectively manage risk and assess the effectiveness of key controls.
    - Resources include staffing, tools, and budgeting processes to ensure the Credit Union's staff or external resources have knowledge and experience commensurate with the Credit Union's risk profile.
    - Training and Culture includes the employee training and member awareness programs contributing to an organizational culture that emphasizes the mitigation of cybersecurity threats.

- Domain 2 - Threat Intelligence and Collaboration includes processes to effectively discover, analyze, and understand cyber threats, with the capability to share information internally and with appropriate third parties. The assessment factors are:
    - Threat Intelligence which refers to the acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities that offer courses of action to enhance decision making.
    - Monitoring and Analyzing which refers to how the Credit Union monitors threat sources and what analysis may be performed to identify threats that are specific to the Credit Union or to resolve conflicts in the different threat intelligence streams.
    - Information Sharing encompasses establishing relationships with peers and information-sharing forums and how threat information is communicated to those groups as well as internal stakeholders.

- Domain 3 - Cybersecurity Controls are the practices and processes used to protect assets, infrastructure, and information by strengthening the Credit Union's defensive posture through continuous, automated protection and monitoring. The assessment factors are:
    - Preventative Controls deter and prevent cyber-attacks and include infrastructure management, access management, device and end-point security, and secure coding.
    - Detective Controls include threat and vulnerability detection, abnormal activity detection, and event detection, may alert the Credit Union to network and system irregularities that indicate an incident has or may occur.
    - Corrective Controls are utilized to resolve system and software vulnerabilities through patch management and remediation of issues identified during vulnerability scans and penetration testing.

- Domain 4 - External Dependency Management involves establishing and maintaining a comprehensive program to oversee and manage external connections and third-party relationships with access to the Credit Union's technology assets and information. The assessment factors are:
    - Connections incorporate the identification, monitoring, and management of external connections and data flows to third parties.
    - Relationship Management includes due diligence, contracts, and ongoing monitoring to help ensure controls complement the Credit Union's cybersecurity program.

- Domain 5 - Cyber Incident Management and Resilience includes establishing, identifying, and analyzing cyber-events; prioritizing the Credit Union's containment or mitigation; and escalating information to appropriate stakeholders. Cyber resilience encompasses both planning and testing to maintain and recover ongoing operations during and following a cyber-incident. The assessment factors are:
    - Incident Resilience Planning & Strategy incorporates resilience planning and testing into existing business continuity and disaster recovery plans to minimize service disruptions and the destruction or corruption of data.
    - Detection, Response, & Mitigation refers to the steps management takes to identify, prioritize, respond to, and mitigate the effects of internal and external threats and vulnerabilities.
    - Escalation & Reporting ensures key stakeholders are informed about the impact of cyber incidents, and regulators, law enforcement, and members are notified as required.

Maturity Levels are defined as follows:

- Baseline - Baseline maturity is characterized by minimum expectations required by law and regulations or recommended in supervisory guidance. This level includes compliance-driven objectives. Management has reviewed and evaluated guidance.
- Evolving - Evolving maturity is characterized by additional formality of documented procedures and policies that are not already required. Risk-driven objectives are in place. Accountability for cybersecurity is formally assigned and broadened beyond protection of member information to incorporate information assets and systems.
- Intermediate - Intermediate maturity is characterized by detailed, formal processes. Controls are validated and consistent. Risk-management practices and analysis are integrated into business strategies.

- Advanced - Advanced maturity is characterized by cybersecurity practices and analytics that are integrated across lines of business. Majority of risk-management processes are automated and include continuous process improvement. Accountability for risk decisions by frontline businesses is formally assigned.
- Innovative - Innovative maturity is characterized by driving innovation in people, processes, and technology for the Credit Union and the industry to manage cyber-risks. This may entail developing new controls, new tools, or creating new information-sharing groups. Real-time, predictive analytics are tied to automated responses.

Management determines which declarative statements best fit the current practices of the Credit Union. All declarative statements in each maturity level, and previous levels, must be attained and sustained to achieve that domain's maturity level. Attained and sustained requires affirmative answers to either "Yes" or "Yes with Compensating Controls" for each of the declarative questions within a maturity level. While management can determine the Credit Union's maturity level in each domain, the Assessment is not designed to identify an overall cybersecurity maturity level.

Management may determine that a declarative statement has been sufficiently sustained based on proven results. Certain declarative statements may not apply to the Credit Union if the product, service, or technology is not offered or used. Declarative statements that may not be applicable are clearly designated and would not affect the determination of the specific maturity level.

Management can review the Credit Union's Inherent Risk Profile in relation to its Cybersecurity Maturity results for each domain to understand whether they are aligned. In general, as inherent risk rises, the Credit Union's maturity levels should increase. The Credit Union's inherent risk profile and maturity levels will change over time as threats, vulnerabilities, and operational environments change. Thus, management should consider reevaluating its inherent risk profile and cybersecurity maturity periodically and when planned changes can affect its inherent risk profile (e.g., launching new products or services, new connections).

Using the maturity levels in each domain, management can identify potential actions that would increase the Credit Union's overall cybersecurity preparedness. Management can review declarative statements at maturity levels beyond what the Credit Union has achieved to determine the actions needed to reach the next level and implement changes to address gaps. Management's periodic reevaluations of the inherent risk profile and maturity levels may further assist the Credit Union in maintaining an appropriate level of cybersecurity preparedness. In addition, management may also seek an independent validation, such as by the internal audit function, of the Credit Union's Assessment process and findings.

MEMBERS 1ST CREDIT UNION
INFORMATION SECURITY AND INCIDENT RESPONSE POLICY

Revised 05/2024 Approved 05/16/2024

GENERAL POLICY STATEMENT

Members 1st Credit Union ("Credit Union") recognizes its responsibility to safeguard member information and will treat the private financial information of Credit Union's members with appropriate care in order to maintain the confidentiality, integrity, and security of member information. 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 safeguard member information and 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 (Part 748) (the "Guidelines").

POLICY AND PROGRAM RESPONSIBILITY

This Information Security Policy and any recommended changes shall be approved by the Board of Directors. The Board will appoint the CEO of the Credit Union as the person responsible for the program. The CEO will maintain this position until the Board chooses to make a change in this appointment.

Credit Union CEO will be responsible for the development, implementation, and maintenance of the Credit Union's Information Security Program and may assign these responsibilities.

ASSESSMENT OF RISK

From time to time, the CEO 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 threats to its integrity. The CEO will evaluate and adjust its risk assessment on a periodic basis and in light of any relevant changes in technology.

RISK MANAGEMENT AND CONTROLS

The CEO 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, access controls, internal controls, and ongoing monitoring of risks and controls.

The CEO 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 of employee duties and existing intrusion detection systems from time to time.

SECURITY OF PHYSICAL FACILITIES

- **Visitor Control;** Access to locations containing member information is restricted to persons with "need-to-know" access to member information. 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.

- **Staff Controls for Information Handling;** Credit Union staff who handles member information 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.

- **Transport;** Physical transport of member information will require the use of a trusted courier. All member information and documents sent via such courier must be enclosed in an opaque and sealed envelope. Whenever member information is sent over external computer networks, it must be sent as a password protected attachment, or by utilizing eDoc service.

- **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 CEO. Destruction will include rendering the information unreadable and include complete eradication of residual electronic information required by Fair and Accurate Credit Transaction Act (FACTA) and other applicable laws and regulations to be destroyed. The Credit Union will ensure that all 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.

- **Theft Protection;** All Credit Union computer and network equipment must be physically secured if located in an open office environment. Local area network servers must be placed in an area that is not accessible to the general public. 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 the CEO.

CONTROLS FOR ACCESS SECURITY

The CEO bears the responsibility for the acquisition, development, and maintenance of production applications which process member information. For each type of member information, the CEO will determine the critical nature of the information and define which Users will be permitted to access it, and define its authorized uses.

All staff is responsible for safeguarding member information and maintaining security measures defined by the CEO. All staff is also responsible for complying with the Credit Union member information security policy, procedure, and standards. Questions about the appropriate handling of a specific type of member information should be directed to the CEO.

MEMBER INFORMATION CLASSIFICATION AND CONFIDENTIALITY

- **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 CEO, 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 to and "need-to-know" authorization for member information.

- **Password Complexity on Home Banking**. Members can self-register on the Credit Union's website in order to have access to their account information through Home Banking. Per the Credit Union's core processor, VisiFI, members utilizing the Credit Union's Internet-based service will be required to create a User ID and password. The password must be at least eight (8) characters in length and contain at least one letter and one non-letter and cannot contain the member's User ID or account number. Before a member can access his/her account, a two-factor authentication is in place where a confirmation code is sent to the member's email address on file with the Credit Union. This confirmation code must be entered into the home banking site before the member has access to the account information.

  Members have an option to register their PC devices for one-time uses or for permanent uses. If the one-time use is selected, the two-factor authentication process will take place each time but not if the permanent use has been selected. If a member has registered his/her device for permanent use and tries to access the account information from a different device, a non-robot image procedure is in place which is designed to stop any automated login attempts.

  The Credit Union will encourage members to change their passwords on a regular basis. Members will be locked out of the system after three (3) failed log-in attempts.

- **Passwords Complexity on Credit Union workstations.** 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. The employees will be required to establish alphanumerical passwords that are at least eight (8) characters in length in order to access their workstation's operating systems but highly encourages the employees to increase the number of characters to 12 or 14 if possible. Additional password requirements apply to each applicable processing system that an employee has been given permission to access, such as core processing system, Debit and Credit Card systems, Corporate Credit Union, Mortgage software etc. The password complexity, number of required characters in a password, password change frequency, lock-outs, log-on attempts, tokens etc. are all set by each vendor and follows bank security best practices.

- **Default Classification.** Unless designated as public information, member information will be classified and treated as nonpublic.

- **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. Staff must verify the existence of a signed agreement prior to disclosure to non-employees.

- **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.

ACCESS CONTROL SYSTEM DESIGN

All 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. All computer users will obtain screen saver.

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

MANAGING SYSTEM PRIVILEGES

Requests for new user IDs and changed privileges must be approved by the CEO. 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.

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 CEO. 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.

CONTROLS FOR INTERNAL SECURITY

- **Standards;** The CEO is 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.

- **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 CEO or outsourced service provider, only after permission by the CEO.

- **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.

- **Password Protection;** When member information is transmitted over any communication network provided by an organization outside the Credit Union, it must be sent as a password protected email attachment, or utilizing eDoc, unless the vendor has provided a secure portal to upload documents. Member information entrusted to the Credit Union by a third party must be encrypted or password protected when sent over external network systems.

- **Network Changes;** With the exception of emergency situations, all changes to Credit Union computer networks must be approved in advance by the CEO. Emergency changes to the Credit Union networks may be made only by persons authorized by the CEO.

- **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 CEO.

- **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.

- **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.

REMOTE ACCESS VIA VIRTUAL PRIVATE NETWORK (VPN) ACCESS

From time to time, special accommodations for employees to work remotely will be allowed with the prior approval of the CEO. If approval has been granted, all employees working remotely should adhere to the full context of this Information Security Policy and all technology and privacy-related policies and procedures. An annual memo will be provided to each employee that has been granted remote access.

Virtual Private Network (VPN) connections provide a convenient way for staff to remotely access the Credit Union core processing system VisiFi. VPN technology provides an encrypted tunnel through a public network so information transmitted to and from systems are not easily readable by unauthorized parties. Like any remote connection, they must be carefully managed and secured.

Staff using computers that are not Credit Union owned equipment must configure the equipment to comply with the Credit Union's policies as a condition of use. All employees using VPN connections are responsible for their remote Internet Service Provider (ISP) and coordinating the initial installation and configuration of approved VPN software through VisiFI IT Department. Only one VPN is allowed on each device and each computer connected to VPN must use up-to-date virus and malware protection software.

Each VPN has its own unique user name and password as well as a second layer of protection with either a text / PIN or call-back each time an employee attempts to connect. This connection should only be used as needed and be disconnected when not in use.

The Credit Union does not have a shared network so no lines of communication can be established between the Credit Union data and employee working remotely.

INTRUSION PREVENTION AND DETECTION

The CEO is responsible for the compilation, regular maintenance, and testing of contingency plans for all Credit Union information systems. Authorized service personnel will be contacted in the event of a hacker intrusion, a virus infection, ransomware attack, cybersecurity incident and other security-related events. The Credit Union shall also ensure that its service provider discloses any information regarding any breach of security resulting from unauthorized intrusion into the Credit Union's member information system maintained by the service provider.

To reduce the possibility of intrusions, the Credit Union will follow the following prevention guidelines:

- **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.

- **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 enabled on their computers and not bypass the scanning process.

- **Eradication Process.** If Users suspect infection by a computer virus, ransomware attacks, cybersecurity incidents and other security-related events, they must immediately stop using the infected computer and contact the CEO.

- **Clean Back-Ups.** To assist with the post-virus-infection restoration of normal microcomputer activities, all computer software must be copied prior to its initial usage, and such copies must be stored in a secure location.

- **Software Sources.** To prevent problems with viruses, ransomware attacks, cybersecurity incidents and other security-related events, Credit Union computers and networks must not run software that comes from sources other than those approved by the CEO or other authorized person at the Credit Union.

- **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.

- **Service Providers.** Contracts with service providers will require the service provider to 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 response program in a timely manner.

INTRUSION RESPONSE

Management will be responsible for developing and implementing a risk-based response program to address incidents of unauthorized access to member information through hacker intrusion, a virus infection, ransomware attack, cybersecurity incident and all other security-related events.

In the event of an intrusion, the Credit Union will undertake the following actions as soon as possible:

- ~~**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 Intrusion Response Plan. The intrusion must also be included in the annual Information Security report and presented to the Board of Directors.

- ~~**Assessment of Incident.**~~ Assess the nature and scope of the incident and identify each member information system and types of member information that have been accessed or misused;

- Notify ~~appropriate authorities, to include~~ Vermont Department of Financial Regulations (VT DFR)

- Notify National Credit Union Association (NCUA); See Appendix "A" for NCUA's "Cyber Incident Reporting Quick Reference Guide" under NCUA 12 CFR, Part 748. A reportable cyber incident is any "substantial" cyber incident that leads to one or more of the following:

  - A substantial loss of confidentiality, integrity, or availability of a network or member information system that results from the unauthorized access to, or exposure of sensitive data, disrupts vital member services, or has a serious impact on the safety and resiliency of operational systems and process.
  - A disruption of business operations, vital member services, or a member information system resulting from a cyberattack or exploitation of vulnerabilities.
  - A disruption of business operations or unauthorized access to sensitive data facilitated through, or caused by, a compromise of a Credit Union service organization, cloud service provider, or other third-party data hosting provider or by a supply chain compromise.

- Notify Allied Solutions, LLC/AmTrustCyber regarding Cyber incident notification at 877 - 207-1047

- 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;
- ~~Notify members when such notice is warranted and in accordance with the Guidance and notice format promulgated by the NCUA/Federal Trade Commission (FTC); and~~

- ~~Take appropriate and prompt corrective measures.~~

~~**INCIDENT RESPONSE PROGRAM**~~

- ~~**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.~~

- **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 Intrusion Response Plan, Management will report the incident to its bonding company, casualty insurance company,

- Notify local law enforcement agencies, Vermont Department of Financial Regulations (VT DFR) and National Credit Union Association (NCUA) and

- File a Suspicious Activity Report (SAR) as necessary

- Notify Members. Members will be notified of an intrusion 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.

- Staff Training. Management will develop procedures to ensure that staff is trained to appropriately handle member inquiries and requests for assistance. This training will be conducted both prior to and after an actual incident.

MEMBER NOTICE

Notification to members will be made timely in order to minimize the Credit Union's reputation and legal risks. The Credit Union will notify Allied Solutions, LLC/AmTrustCyber at 877 - 207-1047 for further notification guidance.

- **Investigation.** Once the Credit Union becomes aware of an incident of unauthorized access, the CEO 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.

- **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 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.

CONTENT OF MEMBER NOTICE

Notice to members will contain the following information:

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

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

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

- 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;

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

- 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;

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

- 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 Web site address and toll-free telephone number.

BACK-UP RESPONSIBILITY AND SCHEDULES

To protect the Credit Union's information systems from loss or damage, the CEO is responsible for ensuring that periodic back-up of critical member information is performed by the Credit Union's core processor, VisiFI. VisiFI needs to store all data in a safe location and physically protect against unauthorized access and provide a response program to address incidents of unauthorized access to member information, pursuant to their policy.

In addition, documents and spreadsheets stored on individual computers, should be backed-up periodically and stored in a safe place.

CREDIT UNION SYSTEMS AND FACILITIES USE

Unless a contractual agreement specifies otherwise, all information stored on, or transmitted by, Credit Union computers and communications systems is Credit Union property. This includes information stored on removable media, such as USB flash drives and external CD / DVD drives. A separate list of acceptable USB drives and other external devices will be kept and adherence to this approved list of devices will be reviewed frequently. For privacy and confidentiality purposes, member information and the devices the information is stored on, are not allowed to be taken off the Credit Union premises. Exceptions must be approved by the CEO prior to removal. 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.

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.

Employees are prohibited from using Credit Union time, facilities, equipment or supplies for private gain or advantage. Users must take steps to prevent member information from being inadvertently damaged or destroyed. Magnetic media should be kept away from heat (such as direct sunlight) as well as magnetic fields.

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. Unless specifically authorized by the CEO, 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.

Employees are discouraged from accessing the Internet with Credit Union computers and networks except in the course of Credit Union business. Management will conduct periodic reviews of web browsing histories on each individual workstation. If during these reviews, visited web sites are found that would be considered inappropriate or illegal, employee disciplinary actions will be taken.

Users must not place Credit Union material on any publicly accessible computer system (including Internet web pages) unless first approved by the CEO.

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.

PATCH MANAGEMENT

Effective patch management will assist the Credit Union management in mitigating the risks associated with software vulnerabilities and in ensuring that the security and availability of computer systems are not compromised.

The Credit Union relies on commercially developed software to support the business processes and information technology infrastructure. Common types of software include Windows operating system, VisiFI core processing system, Microsoft business applications (e.g., word processing, spreadsheet, and database programs), and system services (e.g., anti-virus programs, firewalls, etc.). Commercially developed software may contain flaws that create security and performance vulnerabilities. These vulnerabilities may cause system unavailability or corrupt critical system components or data. Although software vendors often develop updates, or "patches," to correct identified weaknesses, it is the Credit Union's responsibility to update systems or install patches in a timely manner.

In order to mitigate risks associated with commercial software vulnerabilities, the Credit Union has developed the following procedures and practices:

- Oversight and accountability are assigned to the CEO.
- Periodic risk assessments will be performed. These risk assessments will be included in the IT Risk Assessment and presented to the Board of Directors on an annual basis.
- Each workstation will be set to automatically download and install software updates and patches.

- Any new software will be reviewed by the CEO prior to download in order to evaluate potential software vulnerabilities.

- The Credit Union will utilize Belarc Advisor software, or something similar, in order to build a detailed profile of each computer's installed software and hardware, network inventory, missing patches, anti-virus status and security benchmarks. This allows for prompt identification of vulnerabilities and relevant patches, timely implementation, evaluation, and testing of the patches and tracking of both implemented and rejected patches. Any missing security patches identified on the Belarc report will be updated by the Operations Specialist, CEO, or COO. These report profiles will be reviewed by outside Consultant and kept by the CEO.

- In order to provide assurance that vulnerabilities have been identified and appropriate patches have been installed, the Credit Union will rely on an independent outside IT Consultant to conduct ongoing audits. These audits will be performed, at a minimum, on an annual basis.

- A list of the Credit Unions' hardware inventory will be maintained, including the operating systems, specific applications, and the location of the hardware (refer to "Disaster Recovery and Business Continuation Plan" for detailed list).

- In order to identify relevant patch information, the Credit Union will consistently review vendor web sites and third-party public service security web site https://nvd.nist.gov/.

- After a patch has been identified, an impact assessment of the application of the patch will be performed, including a technical evaluation, a business impact assessment, and a security evaluation.

    - The technical evaluation assesses whether the patch will correct a problem with the services and features of the application that are being used by the institution.

    - The business impact assessment determines if applying the patch, or not applying the patch, will impact business processes and when may be an appropriate time for patch installation (i.e., immediately, after hours, or over the weekend).

    - The security evaluation determines whether there are security implications that were not identified during the technical evaluation. Even though there may be no performance benefit to applying a patch, there may be security benefits. Patches may also be installed on software that may be loaded on a system but is currently inactive.

- The Credit Union will work closely with all their vendors to ensure that new patches are evaluated as soon as possible.

- Each patch should be tested prior to installation to ensure that it will function as expected and be compatible with other systems. Patches should be tested at a system level as well as in a quality assurance environment prior to their installation in the production environment. This will ensure their compatibility with the system and with other components in the environment. Evaluation and testing should also ensure that the installation of a patch or software update does not open vulnerabilities previously corrected or produce new vulnerabilities. Application of

patches in the production environment is subject to normal change management procedures to minimize the risk of disruption due to installation of the patch. Testing should also occur in the production environment after installation. In some cases, systems may need to be shut down to test and install a patch, which makes the system unavailable for a period of time. In the case where multiple patches may need to be installed, care should be taken to ensure that they are installed in the proper order. Otherwise, the patches may not be effective or cause additional problems.

- If the Credit Union reinstalls software, previously installed patches may need to be reinstalled (in the original order) in order to be effective. The original install media for the reinstalled software (e.g., CD-ROM) should be maintained as well as all subsequent patches that were installed in the production environment.

PROGRAM REVIEW

The CEO will 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 CEO's report to the Board.

An independent third party will test the program. Testing will include an assessment of exterior defenses, internal security, physical security, and administrative procedures.

The CEO is responsible to provide training to Credit Union staff to recognize, respond, and report to regulatory and law enforcement agencies, any unauthorized or fraudulent attempts to obtain member information. The Credit Union will comply with the risk management process for outsourcing services, as outlined in the Vendor Management policy.

Appendix "A" (2 pages)

Cyber Incident Reporting Quick Reference Guide

When to Report

A federally insured credit union that experiences a reportable cyber incident must report the incident to the NCUA as soon as possible and no later than 72 hours after the credit union reasonably believes that it has experienced a reportable cyber incident.

How to Report

To report a cyber incident, federally insured credit unions may notify the NCUA through the following channels:

- Call the NCUA at **1-833-CYBERCU** (1-833-292-3728) and leave a voicemail; or,
- Use the **National Credit Union Administration Secure Email Message Center** to send a secure email to cybercu@ncua.gov.

What to Report

Federally insured credit unions should be prepared to provide the following information, if known, at the time of reporting.

- **Reporter Name and Title:** Name and title of individual reporting the incident
- **Callback Number:** Best callback number for the NCUA to contact regarding the incident
- **Charter Number:** Do not include leading zeros
- **Credit Union Name:** Name of affected credit union
- **Date and Time Identified:** The date and time the credit union reasonably believes a reportable cyber incident took place
- **Description:** A general description of the reportable cyber incident: ○ What services were impacted? ○ Was sensitive data or member information compromised? ○ What impact did it have on operations?

At the time of initial notification, do not send the NCUA:

- **Sensitive personally identifiable information;**
- **Indicators of compromise; • Specific vulnerabilities; or • Email attachments.**

CYBER INCIDENT REPORTING CARD

Have this card ready when contacting the NCUA to report a cybersecurity incident. It outlines key information you should gather to share with us for an effective response.

Reporter Name and Title: _____
Callback Number: _____
Charter Number: _____
Credit Union Name: _____
Date and Time Identified: _____
Description: _____
_____
_____
_____

Do not send sensitive personally identifiable information; indicators of compromise; specific vulnerabilities; or email attachments.

Call 1-833-CYBERCU (1-833-292-3728) or use the NCUA Secure Email Message Center (https://web1.zixmail.net/s/login?b=ncua

MEMBERS 1ST CREDIT UNION
INFORMATIONAL TECHNOLOGY RISK ASSESSMENT PROGRAM

Revised 05/2022 Approved 05/16/2024

POLICY

It is the policy of Members 1st Credit Union (Credit Union) to conduct an ongoing risk assessment (see Exhibit "A") in accordance with the Information and Technology Security Compliance regulations and guidelines.

The Risk Assessment will identify reasonably foreseeable internal and external risks that could result in service interruption or unauthorized disclosure, misuse, alteration, or destruction of confidential information. It will also evaluate the likelihood and potential damage of the identified threats and assesses the sufficiency of safeguards in place to control the identified risks.

The risk assessment will be conducted in accordance to the predetermined frequency and final assessment presented to the Board of Directors upon completion.

It is the responsibility of the CEO of the Credit Union, in conjunction with the Credit Union's Supervisory Committee, to ensure the compliance of this policy.

PROCESS

The Risk Assessment process includes the following:

- Identification of information that needs to be reviewed
- Identification of businesses and/or owners
- Collection of documentation
- Assessment of data sensitivity and business function
- Identification of threats, risks, concerns and issues
- Determination of level of vulnerability and probability of risk
- Recommendation of required controls and safeguards to mitigate risks identified in the risk assessment results

ANALYSIS

The Risk Assessment evaluation and determination will be based on events such as:

- Security breaches (breaches that can affect the Credit Union both external and internal, programming fraud, computer viruses, or denial of service attacks)
- System failures (Common causes of system failures include network failure, interdependency risk, interface failure, hardware and software failure and internal telecommunication failure)
- External events (threats that are weather-related events, earthquakes, terrorism, cyber-attacks, cut utility lines or wide spread power outages that bring about system or facility failures)
- Systems development and implementation problems (inadequate project management, cost and time overruns, programming errors, failure to integrate and/or migrate successfully from existing systems, or failure of system to meet business requirements)
- Capacity shortages (shortages in capacity result from lack of adequate capacity planning, including the lack of accurate forecasts of growth)

AUDIT CYCLE

The Risk Assessment will be ongoing and the audit frequency will be determined by the risk score assessed at the previous exam and will be at a minimum:

- Low Risk – 36 months audit cycle
- Medium Risk – 24 months audit cycle
- High Risk – 12 month audit cycle

TRAINING

Ongoing training will be provided to staff and volunteers in all areas related to Information Technology Risk Assessment as needed. These training sessions will be documented.

Exhibit "A"

MEMBERS 1ST CREDIT UNION IT RISK ASSESSMENT DECEMBER 31, 20XX

What is the likelihood that something could go wrong with Business Processes	Likelihood of Occurance (1 through 5)	Prior Audit or Examination Results (1 through 5)	Impact Analysis (1 through 5)	Total	Overall Risk Assessment (Low to High) average	Assignment of Responsibility	Risk Mitigation	Audit Frequency	Date Last Audited	Date of Next Audit	Responsible Party/Auditor	Comments
BSA				0	0							
Internet Banking/EPL				0	0							
Disaster Recovery/BC Plans				0	0							
Core Processing & Security (VisiFI)				0	0							
Information Security Program/Policy				0	0							
Information Security Plan				0	0							
Internal Detection System				0	0							
IT Policies				0	0							
Vulnerability Assessment				0	0							
Network Security				0	0							
E-Mail Security				0	0							
ACH /EFT Processing				0	0							
Telephone Banking				0	0							
ATM's				0	0							
PC's and USB's												
Vendor Management				0	0							
Fedline				0	0							
Software Licensing				0	0							
	0	0	0	0	**0**							
OVERALL CREDIT UNION ASSESSMENT RATING												
				LOW RISK ON THE IT ASSESSMENT								

Rating Examples		
Likelyhood of Occurrence (security breach) (rate between 1-5)	1 = lowest risk	5 = highest risk
Prior Exam results (rate between 1-5)	1 = no recommen	5 = major recommendations
Impact Analysis (rate between 1-5)	1 = no legal/finar	5 = significant legal/financial issues

Scoring Examples
Score 60-90 = High Risk
Score 30-59 = Medium Risk
Score 0- 29= Low Risk