4100. INFORMATION SECURITY POLICY

Revised: **June 2016**
Ratified: **April 2019**

TABLE OF CONTENTS

Introduction

This Information Security Policy supersedes any and all other information security policies that may have been previously documented.

Purpose

The purpose of this policy is to provide guidance to Resource One Credit Union management in the creation and implementation of an Information Security Program designed to protect the confidentiality, security, and integrity of member information and member information systems in compliance with the provisions of the Gramm-Leach-Bliley Act and Guidelines for Safeguarding Member Information published by the NCUA under 12 CFR Part 748.0 Appendix A to establish standards addressing administrative, technical, and physical safeguards in order to:

1. Ensure the security and confidentiality of member records or information.
2. Protect against any anticipated threats or hazards to the security or integrity of such records.
3. Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any member.
4. Ensure the proper disposal of member information and consumer information.

Protecting confidentiality includes honoring members' requests to opt out of disclosures to non-affiliated third parties as described in 12 CFR Part 1016.1(a)(3).

This policy will establish standards addressing appropriate response procedures for unauthorized access of member information, including member notification procedures as required by Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice published by the NCUA under 12 CFR Part 748.0 Appendix B. This policy will also address the establishment of an Identity Theft Prevention Program to be included as part of the Information Security Program.

Consequences of Non-Compliance

Compliance with this Information Security Policy is mandatory. Violations may result in disciplinary action up to and including termination of employment or services with the Credit Union and/or referral to the appropriate state or federal law enforcement authorities.

Governance

1. Information Security Officer – The Board of Directors, on July 18, 2013, at a duly convened meeting, designated the Resource One Credit Union Director of Information Technology to serve as the Information Security Officer of Resource One Credit Union and such appointment is properly recorded in the minutes of that meeting. The Information Security Officer shall have the authority and responsibility, subject to the approval of this Board, for the development and administration of an Information Security Program that equals or exceeds the information security standards prescribed by NCUA regulations and other applicable federal and state laws and regulations.
2. Board Approval – This Information Security Policy was approved by the Board of Directors at a duly convened meeting on June 16, 2016
3. Board Supervision – The Board of Directors is aware of its responsibility to comply with NCUA Guidelines for Safeguarding Member Information and supervise the Information Security Officer in the development, implementation, and maintenance of the provisions of the written Information Security Program and related activities as contained herein. Hence, the Information Security Officer shall report annually to the Board on the implementation, administration, maintenance, and effectiveness of the Information Security Program. Such reports may be made more frequently or on an as-needed basis at the discretion of the President/CEO or the Information Security Officer or as called upon by the Board of Directors.

Annual Statement of Compliance

As required by NCUA, Resource One Credit Union will certify–compliance with Part 748 of the NCUA Rules and Regulations annually using NCUA's online information management system. Credit Union directors will also file Oath of Office with the Texas Credit Union Department.

Risk Assessment

It is the policy of Resource One Credit Union to identify and assess the risks that may threaten the security, confidentiality, or integrity of member information systems.

Resource One Credit Union will:

- Assess the sufficiency of policies, procedures, member information systems, and other arrangements in place to control identified risks.
- Identify and determine the sensitivity of member information and assess the risks that may threaten the security, confidentiality, or integrity of member

information systems and all non-public member information whether in storage, processing, or transit.

- Monitor, evaluate, and adjust its risk assessment practices and Information Security Program in light of any relevant changes to technology, the sensitivity of member information, and internal or external threats to information security.

It is the Credit Union's intention to mitigate any foreseeable and identified information security risks to the extent reasonably possible to ensure the security and safety of member information. If it is determined by the Information Security Officer that it is not reasonably possible to eliminate or mitigate an identified vulnerability or risk, any decision to accept unmitigated risk and the reasoning behind it must be documented and presented to Senior Management for written approval.

Risk Management and Control

Access Controls

It is the policy of Resource One Credit Union to control and permit only authorized individuals and entities access to member information, member information systems, controls to authenticate and grant access to member information systems, and to locations such as buildings, computer facilities, and records storage facilities containing member information.

Dual Control and Segregation of Duties

It is the policy of Resource One Credit Union to implement dual control procedures and segregation of duties as appropriate.

Employee Background Checks

It is the policy of Resource One Credit Union to conduct background checks for employees with responsibilities for or access to member information.

Protection Against Destruction of Member Information

It is the policy of Resource One Credit Union to provide for protection against destruction of member information due to potential physical hazards, such as fire and water damage, and provide and maintain response programs to preserve the integrity and security of member information in the event of computer or other technological failure including, where appropriate, reconstructing lost or damaged member information.

E-Commerce

It is the policy of Resource One Credit Union to establish, implement, and maintain standards and procedures that reasonably ensure the security of information and transactions when performing e-commerce activities.

Response to Unauthorized Access

It is the policy of Resource One Credit Union to establish, implement, and maintain response and notification programs that specify actions to be taken when unauthorized access to member information systems is suspected or detected.

Encryption

It is the policy of Resource One Credit Union to provide for encryption of electronic member information where appropriate.

Monitoring Systems and Procedures

It is the policy of Resource One Credit Union to utilize monitoring systems and procedures consistent with industry standards to detect and retain a record of actual and attempted attacks or intrusions into member information systems.

Testing of Key Controls, Systems, and Procedures

It is the policy of Resource One Credit Union to regularly test the key controls, systems, and procedures of the Information Security Program to confirm that they control the risks and achieve the overall objectives of the Credit Union's Information Security Program. The frequency and nature of such tests will be determined by the annual information security risk assessment and will be adjusted as necessary to reflect changes in internal and external conditions. These tests will be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

System Modifications

It is the policy of Resource One Credit Union to implement procedures to confirm that member information system modifications are consistent with the Credit Union's Information Security Program.

Disposal of Member Information and Consumer Information

It is the policy of Resource One Credit Union to develop, implement, and maintain as part of its Information Security Program appropriate measures to properly dispose of member information and consumer information.

Contract Provisions and Third Party Oversight

It is the policy of Resource One Credit Union to implement contract provisions and oversight mechanisms to protect the security of member and consumer information maintained or processed by service providers.

When contracting with third party vendors providing web-based applications or application services, it is the policy of Resource One Credit Union to ensure that the application has been developed and will be maintained in a manner that appropriately addresses risks to the confidentiality, availability, and integrity of the data.

It is the policy of Resource One Credit Union to exercise appropriate due diligence in managing and monitoring its outsourcing arrangements to confirm that its service providers have implemented an effective information security program to protect member information and member information systems consistent with the Resource One Credit Union Information Security Policy and ensure the proper disposal of member and consumer information in compliance with NCUA Guidelines. Where indicated by the Credit Union's risk assessment, part of this monitoring will include the review of audits, summaries of test results, or other equivalent evaluations of its service providers.

Identity Theft Prevention Program

It is the policy of Resource One Credit Union to develop, implement, and maintain as part of its Information Security Program an Identity Theft Prevention Program to detect, prevent, and mitigate identity theft in connection with opening covered accounts and servicing existing covered accounts. Indicators of potential identity theft will be identified and procedures to detect and respond appropriately to these indicators (or red flags) will be established. The program will be updated periodically, but at least annually, to reflect changes in risks to members or to the safety and soundness of the Credit Union from identity theft.

Staff Training

In order to reasonably assure that the Information Security Program is effective and meets current industry standards, and to best ensure that the Resource One Credit Union's Information Security Officer is knowledgeable in fulfilling his assigned responsibilities under the program, it is the policy of Resource One Credit Union that the Information Security Officer receive and document proper periodic training as appropriate. This may consist of, but need not be limited to, the following:

- Meetings with and instructions or guidance given by the Board of Directors, the President/CEO, or other superiors.
- Annual attendance by the Information Security Officer at an information security seminar.
- Membership in and attendance at meetings of professional information security associations by the Information Security Officer.
- Meetings and discussions with information security officers or committees in the area.
- Subscription to and review of at least two monthly information security publications.

It is the policy of Resource One Credit Union that the Information Security Officer shall prepare, implement, maintain, and supervise a program for the training of Credit Union staff to:

- Recognize, respond to, and report to a supervisor or to the Information Security Officer any unauthorized or fraudulent attempts to obtain member information.
- Appropriately respond to member inquiries and requests for assistance when sensitive member information has been compromised.
- Dispose of member and consumer information using appropriate methods.
- Detect identity theft red flags and respond appropriately.

Reporting

It is the policy of Resource One Credit Union that the Information Security Officer shall ensure that adequate records are retained and that a periodic report is submitted to the Board of Directors. The periodic report to the Board shall address the Credit Union's compliance with the regulations, risk assessment, risk management and control, results of testing, details of attempted and/or actual security breaches or violations and responsive actions taken, the overall status of the Information Security Program, and any recommendations for improvements in the Information Security Program.

Resource One Credit Union will file Suspicious Activity Reports in a timely manner. The Credit Union will maintain a copy of any SAR that is filed and the original or business record equivalent of all supporting documentation as required. Additionally, Credit Union management will notify its Board of Directors or a committee designated by the Board of Directors of any SAR filed.

Resource One Credit Union will notify the NCUA Regional Director of any catastrophic act (a disaster, natural or otherwise, resulting in an interruption in vital member services projected to last more than two consecutive business days) that occurs at any of its branches.

The Resource One Credit Union Information Security Officer shall oversee the creation and maintenance of Information Security Standards and Procedures to implement the above Information Security Policy established by the Board of Directors.

Historical Record of Policy Changes

GastleGarde was hired to conduct an IT Audit. During their audit, they observed day-to-day operations and procedures. Those observations were then combined with current policies and procedures and they produced an updated Security Standard & Procedures. Existing policies were incorporated into the standards and procedures. Rather than extracting those policies, the Policy Committee recommends updating the current policies with the information contained in the standards and procedures.

Revised: June 2013
Ratified: July 2013

The Information Security Policy was completely rewritten.

Revised: June 2016
Ratified: June 2016

The policy was revised as part of our annual security audit conducted by CastleGarde. The purpose was updated to include honoring member opt out requests and consequences of Non-Compliance (page 2).

The Annual Statement of Compliance section was updated to comply with the NCUA's filing requirements (page 3).

A revision to the section pertaining to the Risk Assessment was amended to include that any decision to accept unmitigated risk and the reasoning must be documented and presented to Senior Management for approval (page 4).

Testing of Key Controls, Systems and Procedures was modified to state that tests will be conducted or reviewed by independent third parties (page 5).