2600. THIRD PARTY DUE DILLIGENCE POLICY

Revised: **July 18, 2013**
Ratified: **April 19, 2019**

TABLE OF CONTENTS

VENDOR MANAGEMENT PROGRAM

Resource One Credit Union relies heavily on third parties to provide certain critical information services. Resource One Credit Union will exercise appropriate due diligence in selecting its service providers, require its service providers by contract to implement appropriate measures designed to meet the objectives of these guidelines, and monitor service provider compliance. As part of this monitoring, the Credit Union will review audits, summaries of test results, and/or other equivalent evaluations of its service providers.

The Credit Union will also review the service provider's due diligence process for any of its significant supporting agents (e.g., subcontractors, support vendors, and other parties). Depending on the services being outsourced and the level of in-house expertise, the Credit Union should consider whether to hire or consult with qualified independent sources. These sources include consultants, user groups, and trade associations that are familiar with products and services offered by third parties.

VENDOR SELECTION

Resource One Credit Union's due diligence efforts go a long way in reducing our exposure to risk. Establishing a track record of due diligence will demonstrate that the Credit Union did the best it could do to limit loss. Documentation of Resource One Credit Union's due diligence efforts will also help reduce liability and enforcement consequences of any loss or security breach that may occur.

Vendor Risk Assessment

An initial risk analysis should be conducted for each potential vendor. At a minimum, the risk analysis will utilize the Vendor Risk Rating Matrix (shown on the next page) to assign a Vendor Risk Rating of *Low, Medium, or High* risk. A vendor is assigned a risk rating based on the ***highest risk level*** attributable to the contract, or sum of all contracts, with the vendor. Exceptions to the assigned risk may be granted by senior management, but the reasoning behind the decision must be documented.

The risk rating is an indicator of the level of due diligence the Credit Union requires for each vendor initially and thereafter.

- Low-risk vendors typically require little or no further analysis or due diligence.
- Medium-risk vendors should be evaluated to determine the appropriate level of due diligence required initially based on the products and services provided. An annual due diligence review will generally be required.
- High-risk vendors require an in-depth due diligence review initially. An annual due diligence review is required.

Risk Categories

The following list of categories defines risks that may be associated with each service provider. It is not all inclusive and should only be used as a guide. Ultimately, the depth of due diligence will vary depending on the scope and importance of the outsourced services as well as the risk to the Credit Union from these services.

- **High risk** – The service provider will have a direct connection to any Resource One Credit Union network, will maintain a live web presence, will have unlimited access to member information, or will provide a direct relationship that could potentially compromise sensitive member information or cause reputation risk to the Credit Union. Any of these circumstances should immediately prompt the Credit Union to establish a thorough evaluation of the service provider. Examples of these include service centers, e-statement vendors, web hosting, and IT service support providers.
- **Medium risk** – The service provider will have access to member data by means of transmissions or updates or will provide the Credit Union with a service that will be used to store member information. Examples of these include statement vendors, off-site storage facilities, etc.
- **Low risk** – The service provider has minimal or no access to member data and merely provides a service to the Credit Union. Examples of these include cleaning services, office supply vendor, mail service, etc.

VENDOR RISK RATING MATRIX			
Factor	**Low Risk**	**Medium Risk**	**High Risk**
Business impact if product or service is discontinued	Minimal impact on the Credit Union	Significant, but non-critical impact	Critical impact
Member Contact	None	Indirect	Direct
Annual Contract Amount	< $10,000	$10,000 – $50,000	> $50,000
Contract Term	< 1 year	1-3 years	> 3 years
Potential for significant cost or financial loss	Low	Moderate	High
Access to sensitive member information (SMI) or systems on which it is stored for either members or employees	No access, except for possible unintentional exposure.	Limited Access	Full Access

Exit Strategy	Immediate replacement available	Many available vendors – minimal start-up time	Limited number of available vendors or long lead time required to convert
Expense to replace the product or service	Low	Moderate	High

Vendor List

The Credit Union will retain a complete vendor list, including low-risk vendors, with the risk rating noted for each vendor.

Vendor Due Diligence [1]

Due diligence requires a reasonable inquiry into a vendor's ability to meet our requirements for the proposed service and/or product. The level of due diligence and the party responsible for the due diligence will be based on the initial vendor risk rating. The higher the level of risk, the more thorough the due diligence will need to be. Senior management will be responsible for the due diligence of any vendor determined to be high risk. Medium to low risk vendors will be the responsibility of a department manager or higher, as assigned by a member of senior management. All due diligence documents, including risk rating forms will be kept with the vendor due diligence file.[2]

A risk assessment will be completed prior to engaging in any critical or significant third party relationship and should be revisited as part of contract renewal or anytime the relationship with the vendor changes in any significant way.

1 Please see Appendix H for a sample *Vendor Risk Rating Form*.

2 Vendor Management forms that include due diligence checklists are provided in Appendix I (new vendor) and Appendix J (existing vendor).

More specifically, review the following:

- **Expectations for Outsourced Functions** – The Credit Union should clearly define the nature and scope of their needs and identify the needs the third party will meet. In order to tailor controls to mitigate risks posed by a third party, the relationship manager must have an understanding of a prospective third party's responsibilities and all of the processes involved with prospective third party programs.
- **Staff Expertise** – Is Credit Union staff qualified to manage and monitor the third party relationship? How much reliance on the third party will be necessary?
- **Criticality** – How important is the activity to be outsourced? Is the activity mission critical? What other alternatives exist?
- **Risk-Reward or Cost-Benefit Relationship** – Management of costs is a major driver in vendor relationship management. Proper attention to establishment of relationships and subsequent follow-up has the potential to yield major cost savings. It is expected that those responsible for vendor relationships will have a good knowledge of the cost advantages/disadvantages associated with that relationship.
- **Insurance** – Will the arrangement create additional liabilities? Is Credit Union insurance coverage sufficient to cover the potentially increased liabilities? If the third party carries "key man" insurance or other insurance, will it protect the Credit Union?
- **Impact on Membership** – How will the Credit Union gauge the positive or negative impacts of the arrangement on the members? How will we manage member expectations?
- **Exit Strategy** – Is there a reasonable way out of the relationship if it becomes necessary to change course in the future? Is there another party that can provide any services deemed critical?

Risk assessments for less complex or less critical third party services may be part of a broader risk management program or documented in Board minutes.

Background Check

Proven performance is essential with regard to business relationships and staff performing due diligence with regard to service providers shall contact Credit Unions or any other clients of the service provider in order to document and support references. By obtaining this information, the level of satisfaction other parties have experienced with the prospective vendor may be determined, including any negative experiences they may have encountered. External sources such as the Better Business Bureau and Federal Trade Commission may be included in this process to determine reputation and complaint histories as is available in their public files. Any service provider should have experience in

implementing and supporting the job. The Credit Union should also evaluate the qualifications and experience of key employees.

Technical and industry expertise may be scrutinized as follows:

- Evaluate the service provider's ability to respond to service disruptions.
- Evaluate the experience of the service provider in providing services in the anticipated operating environment.
- Identify areas where the Credit Union would have to supplement the service provider's expertise to fully manage risk.
- Consider whether additional systems, data conversions, and work are necessary.
- Where necessary, perform onsite visits to better understand how the service provider operates and supports its services.

The Credit Union should also review and consider any lawsuits or legal proceedings involving the third party or its principals that may potentially be cause for concern. Additionally, the Credit Union should ensure that third parties or their agents have any required licenses or certifications and that they remain current for the duration of the arrangement.

Business Model

Before entering into a third party arrangement, the relationship manager should thoroughly understand the third party's business model. The third party's business model is simply the conceptual architecture or business logic employed to provide services to its clients. For medium and high risk vendors, if the third party's business plan is available, it should be reviewed. The relationship manager should also understand and be able to explain the third party's role in the proposed arrangement and any processes for which the third party is responsible.

The Credit Union should understand the third party's sources of income and expense, considering any conflicts of interest that may exist between the third party and the Credit Union. For example, if a third party's revenue stream is tied to the volume of loan originations rather than loan quality, its financial interest in underwriting as many loans as possible may conflict with the Credit Union's interest in originating only quality loans. The Credit Union should identify any vendor-related parties (such as subsidiaries, affiliates, or subcontractors) involved with the proposed arrangement and understand the purpose and function of each.[3] Examiners will consider the potential effects of identified conflicts of interest and ensure that the Credit Union has mitigated risks where reasonable.

3 Further due diligence may be required of some of these related parties if they play a critical role in providing the Credit Union with the proposed service.

Cash Flows

Potentially one of the most important considerations when establishing a third party relationship is the determination of how cash flows move between all parties in the proposed arrangement. Credit Union officials should be able to explain how cash flows move (both incoming and outgoing) between the member, the third party, and the Credit Union. The Credit Union should be able to independently verify the source of these cash flows and match them to related individual accounts. The Credit Union will ensure cash flows are being tracked and identified accurately.

Financial Review

When contracting for critical services or when a substantial investment or advance fee is required, the Credit Union should examine the service provider's financial statements to determine the strength of the business. Weakly capitalized companies or those exhibiting weak earnings may not be able to provide the standard of service that the Credit Union requires or may even collapse, leaving the Credit Union unable to provide services for members for extended periods of time. The Credit Union will analyze the service provider's most recent audited financial statements and annual reports as well as other indicators (e.g., publicly traded bond ratings) if available. In addition, the Credit Union will:

- Consider factors such as how long the service provider has been in business and the service provider's market share for a given service and how it has fluctuated.
- Consider the significance of the institution's proposed contract on the service provider's financial condition.
- Evaluate technological expenditures. Is the service provider's level of investment in technology consistent with supporting the institution's activities? Does the service provider have the financial resources to invest in and support the required technology?

Return on Investment

Credit union officials shall use appropriate resources to project expected revenue, expenses, changes in member service, changes its operational efficiencies and overall impact on the Credit Union earnings upon investing in the services of a third party provider.

Accounting Considerations

The Credit Union should be aware that third party relationships might create accounting complexities. The Credit Union must have adequate accounting infrastructures to appropriately track, identify, and classify transactions in accordance with Generally Accepted Accounting Principles (GAAP). In some instances, a certified public accountant's guidance may be necessary to ensure proper accounting treatment. The Credit Union's audit scope should provide for independent reviews of third party arrangements and associated activities.

Insurance Requirements

1. As a contingency for any potential negative impact, Credit Union management shall review the vendor's insurance coverage (if applicable), including fidelity bond and policies covering such matters as errors and omissions, property and casualty losses, and fraud and dishonesty with regard to any addition or change to third party service providers. Necessary changes shall be identified and facilitated to cover any perceived inequities in existing policies.

General Security Concerns

When a potential vendor will maintain or process sensitive member information on behalf of the Credit Union or will otherwise be granted access to member information through its providing of services to the Credit Union, the Credit Union will require that the service provider's business processes include appropriate physical, administrative, and technical safeguards to protect member information against loss or unauthorized use. The safeguards will include appropriate measures to ensure proper disposal of consumer information in a manner consistent with the disposal of member information. The vendor should also have processes in place to ensure that any subcontractor it uses employs appropriate security measures. Therefore, the vendor selection process will include a review of the measures a service provider takes to protect member information. The vendor will be required to provide:

- A copy or executive summary of the third party service provider's information security policy/program.
- A copy of the third party service provider's most recent Service Organization Report (SOC 1, SOC 2, or SOC 3) performed under SSAE16 (Statement on Standards for Attestation Engagements), and/or an executive summary of any other third party vulnerability or risk assessment and/or penetration test as appropriate.

Internet and/or Web-Hosting Service Providers

The Credit Union will ensure that service providers that are being considered to provide Internet or web-hosting will implement appropriate traffic management controls such as packet load balancing, appropriate size of the Internet pipe/connection, and proper egress rule configuration. The Credit Union will confirm that appropriate steps will be taken to help protect or harden any Internet gateway devices outside the Credit Union's direct management.

Application Security

Low Risk Applications

Application security due diligence assessments are not required for:

- Operating systems.
- Generic office products (e.g., Microsoft Word, Excel, PowerPoint).
- Applications that are not used to support Credit Union products or services.
- Other non-credit union industry type applications.

Medium or High Risk Applications

For applications that present medium or high risk (e.g., application is Internet accessible, application processes or has access to sensitive data, Internet Banking module, core processor, bill pay system, online loan applications, etc.), the Credit Union will ensure that applications that are being considered for use have been developed and will be maintained in a manner that appropriately addresses risks to security, confidentiality, availability, and integrity of data. Application security considerations will be included in the request for information or request for proposal to the vendor. The *Application Security Due Diligence Checklist* should be used to document the findings.[4]

The Credit Union will ensure that the application has incorporated security at all stages of development and quality assurance processes. The application vendor should be able to demonstrate that their processes include rigorous testing and well-defined recurring processes to identify and monitor vulnerabilities, notify users of vulnerabilities, and provide remediation or corrective measures (e.g., patches).

The following items should be included in the evaluation:

- The vendor's processes for development and validation of the application security before, during, and after it has been purchased.
- The vendor's notification processes whenever security vulnerabilities are identified by the vendor, reported by customers, or reported in the media.
- Process and timing for providing mitigation or remediation solutions to identified security vulnerabilities.
- Determine if the vendor has an industry-recognized third party conduct application vulnerability assessments on applications which include security. If so, request a copy or executive summary of the most current results.

Secure Development Attestation

Depending on the risk profile, a written attestation stating that the software development process follows secure development practices and is periodically tested may suffice for some applications.

Third Party Security Testing/Vulnerability Assessment

For applications that present higher risks, the Credit Union will require evidence of adhering to sound processes and validation through independent third party vulnerability assessments or testing and/or audits. Before purchase or during the request for information or proposal process, obtain the name of the third party conducting the test and/or audits, the frequency with which they are performed, the date of the last assessment, and a copy or executive summary of the most recent assessment. Review the information to determine whether the application has any known open vulnerabilities

4 Please refer to Appendix F.

and the nature of those vulnerabilities and if they are a cause for concern. If the vulnerability has not already been remediated, understand the vendor's plan and timeframe for doing so.

If the vendor does not have a third party who conducts application vulnerability assessments, ask the vendor to describe their internal methodology. Assess the methodology using the guidance in the FFIEC IT Handbook Software Development and Acquisition.[5]

Legal Review

To address legal risk, Credit Union management shall engage the advice and counsel of attorneys to review service provider contracts and ensure a clear understanding of contractual rights and responsibilities. The Credit Union shall exercise its right to modify contracts to make them fair and equitable, as is determined appropriate. Based on the complexity and degree of the contract to assess terms and potential liability, management may choose to waive legal review in cases that are determined to represent a very low risk or limited liability to the organization.

In addition to a legal review of contracts and written agreements relevant to a prospective third party arrangement, it may be prudent for the Credit Union to obtain a legal opinion about any services provided by the third party under the arrangement. For example, if a third party is engaged to perform loan collections for the Credit Union, a legal review of their collection methods may be prudent to ensure debt collection and reporting practices comply with applicable state and federal laws.

The Credit Union must ensure compliance with state and federal laws and regulations, and contractually bind the third party to compliance with applicable laws (e.g., Regulation B, Regulation Z, HMDA, etc.). Since the Credit Union may ultimately be responsible for consumer compliance violations committed by their agents, the Credit Union should be familiar with the third party's internal controls for ensuring regulatory compliance and adherence to the agreed upon practices.

Services Requiring Red Flag Considerations

Whenever the Credit Union engages a third party to perform an activity in connection with one or more covered accounts, the Credit Union will take steps to ensure that the third party activities are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. The responsible Credit Union manager will ensure relevant red flags have been identified and procedures have been established that either require the service provider to report the red flag to the Credit

5 This handbook can be found at http://ithandbook.ffiec.gov/it-booklets/development-and-acquisition.aspx.

Union or require the service provider to take appropriate steps to prevent or mitigate identity theft.

Business Resumptions and Contingency Plans

To ensure continued operation of critical Credit Union services, the Credit Union should review the service provider's business recovery procedures and summary of any tests results. Once a service provider has been selected, the service provider's plan will be incorporated into the Credit Union's *Disaster Recovery Plan* when appropriate.

Exit Strategy

Each vendor contract will require an exit strategy should the Credit Union or the vendor be unable or unwilling to fulfill its contractual obligations. The Credit Union will need to list the strategy and provide a timetable as to the length of time it will take to deploy the strategy; also, the Credit Union should list the likelihood that an exit strategy will be necessary based on the length of time the vendor has been in business and its level of financial and market stability (client base, etc.).

CONTRACT MANAGEMENT

Once a vendor has been selected, a clearly drafted contract will protect the Credit Union and provide structure for expectations and issue resolutions. The level of detail and importance of contract provision varies with the scope and risks of the services and products provided. Contracts for high or medium risk may be reviewed by legal counsel and the CFO; the Director of Information Technology will also review contracts related to software, hardware, and information systems. Contracts for low-risk vendors may be reviewed by the CFO and/or the department manager.

Vendors and other independent third parties that provide support or service in conjunction with the Credit Union's financial services activities will be required to enter into a written contract or other suitable agreement that details the vendor's responsibilities pertaining to data security and privacy.

Vendor contracts and agreements will bind each third party service provider to the same standards and levels of data confidentiality and controls as those instituted by the Credit Union. Where warranted, the Credit Union will monitor service providers to confirm that they have satisfied their contractual obligations.

Typically, at a minimum, third party contracts should address the following:

- Scope of arrangement, services offered, and activities authorized.
- Responsibilities of all parties (including subcontractor oversight).
- Service level agreements addressing performance standards and measures.

- Performance reports and frequency of reporting.
- Penalties for lack of performance.
- Ownership, control, maintenance, and access to financial and operating records.
- Ownership of servicing rights.
- Audit rights and requirements (including responsibility for payment).
- Data security and member confidentiality (including testing and audit).
- Business resumption or contingency planning.
- Insurance.
- Member complaints and member service.
- Compliance with regulatory requirements (e.g. GLBA, Privacy, BSA, etc.).
- Dispute resolution.
- Default, termination, and escape clauses.

Minimum Information Security Contract Requirements

When a vendor will maintain or process sensitive member information on behalf of the Credit Union or will otherwise be granted access to sensitive member information through its provision of services to the Credit Union, the Credit Union will enter into a written contract that must include the following provisions in regard to information security:

- A requirement that the third party service provider will comply with all applicable state and federal privacy and information security laws and regulations.
- Acceptable confidentiality and non-disclosure provisions.
- An agreement that the service provider is responsible for the security of member information and will maintain information security procedures to protect member and consumer information from compromise or disclosure to the same degree it protects its own confidential information, but no less than industry standards would prescribe.
- Provisions that define acceptable use of Credit Union information and resources by the service provider or subcontractors used by the service provider.
- A requirement for the third party service provider to obtain contractual obligations of non-disclosure and confidentiality with any subcontractors used that have access to or maintain sensitive member information.
- That any member information provided by the Credit Union to service provider shall at all times, including after termination of the agreement, remain the property of the Credit Union.

- A provision that states the service provider will develop, implement, and maintain as part of its information security program appropriate measures to properly dispose of member and consumer information.
- That the service provider agrees to take action to address unauthorized access to the Credit Union's member information.

- That the service provider agrees to disclose any physical or electronic breach of security resulting in unauthorized access to member information or systems where member information is maintained. That when a breach in security occurs, the service provider will report to the Credit Union the nature of the intrusion, the effect on Credit Union information, and any corrective and responsive actions taken by service provider in response to the intrusion.
- An outline of the responsibilities, duties, controls, and liability of each party including the exchange of information.
- When appropriate, documentation on the ownership of data and processes by each party including software details such as source code agreements, escrowing software, etc.
- When appropriate, a description of reports that will be provided to the Credit Union to evaluate the service provider's adherence to the agreed upon service levels and the frequency of distribution.
- If appropriate, that the service provider agrees to ongoing application vulnerability assessments.

Contracts may also contain:

- That the service provider will indemnify the Credit Union for claims arising as a result of the negligence of service provider.
- That the costs of providing notice to the Credit Union's members as a result of negligence on the part of the service provider be paid by the service provider.

Contract Approval

The level of detail and relative importance of contract provisions will vary with the scope and risks of the products and services provided. All contracts will be reviewed by a member of senior management who will then determine whether the contract also needs to be reviewed by legal counsel. If legal counsel is used, that counsel will typically only address the contract from a legal perspective. Senior management will be responsible for reviewing the contract from all perspectives, including information security. Senior management will be responsible for the final approval of all contracts, including renewals.

Contract Cancelation

Cancellation of a contract must follow agreed upon contract language and be executed at the same or higher level of the organization as the original contract execution.

Contract File Retention

Vendor Due Diligence/Contract files will be stored for three (3) years after contract expiration. Retain copies of all contracts/agreements and other essential documentation of

the negotiations and due diligence performed in the file. Physical vendor contracts will be maintained at the Belleview office and backup copies will be uploaded to the Portal as available.

Responsibilities

- The CEO is responsible for:
  - Approving medium and high-risk vendor contracts.
  - Appointing a relationship manager for all vendors.
- Relationship manager is responsible for:
  - Assigning a Vendor Risk Rating using the Vendor Risk Rating Form.
  - Completing a vendor risk assessment.
  - Completing a vendor due diligence review.
  - Maintaining vendor files.
  - Effectively acting as vendor liaison.

RELATIONSHIP MANAGEMENT

The management of vendor relationships will be centralized and required documentation maintained by an employee designated by the manager. The following activities will be conducted as a matter of periodic review. The *Existing Vendor Due Diligence Checklist* will be used to document this review.[6]

- Review to assure the appropriate risk rating is assigned.
- A relationship file is prepared to maintain relevant documentation and correspondence.
- Annual financial statements may be requested and reviewed by management.
- If applicable, one of the Service Organization Reports (SOC 1, SOC 2, or SOC 3) performed under SSAE16 (Statement on Standards for Attestation Engagements) will be obtained annually.
- The service provider's compliance with service level agreements and the contract will be monitored.

6 Please refer to Appendix J (existing vendor).

RISK MEASUREMENT, MONITORING, AND CONTROL OF THIRD PARTY RELATIONSHIPS

In addition to careful due diligence when entering third party arrangements, the Credit Union must establish ongoing expectations and limitations, compare program performance to expectations, and ensure all parties to the arrangement are fulfilling their responsibilities. Third party arrangements and risk profiles will vary; thus, the Credit Unions will tailor risk mitigation efforts to the specific nature of programs and services and the materiality of risks identified.

Controls

Controls ensure the relationship with third party service providers satisfies expectations and the service provider meets contractual responsibilities. As part of these controls, Resource One Credit Union shall maintain updated policies and procedures, assign specific staff responsibility for monitoring and reporting practices sufficient to oversee service provider activities along with informing management of compliance with contracts and goals.

Policies and Procedures

Resource One Credit Union management shall continue to develop and implement detailed ~~policy~~ procedural guidance setting forth responsibilities that the program grows at a controlled pace and reflects acceptable risk tolerances.

Risk Measurement and Monitoring

The Credit Union must be able to measure the risks of third party programs, but also the performance of third parties in terms of profitability, benefit, and service delivery. For example, if outsourcing loan servicing functions, the Credit Union must be able to identify individual loan characteristics, repayment histories, repayment methods, delinquency status, and any loan file maintenance relative to serviced loans. To the extent that the Credit Union relies on the third party to provide this type of measurement information, clear controls must be contractually established and be subject to periodic independent testing to ensure the accuracy of the information.

The Credit Union must have an infrastructure (e.g., staffing, equipment, technology, etc.) sufficient to monitor the performance of third party arrangements. In many cases, the Credit Union may outsource processes or functions due to a lack of internal infrastructure or experience. Outsourcing does not eliminate the Credit Union's responsibility for the safety and soundness of those processes and functions. Senior management will ensure they have the knowledge, skills, and abilities necessary to monitor and control third party arrangements.

Control Systems and Reporting

After the Credit Union has conducted internal risk assessments and due diligence over prospective third parties, on-going controls must be implemented over the third party arrangement to mitigate risks.

Senior management is responsible for these on-going controls and establishing internal controls and audit functions to assure appropriate safeguarding of member and Credit Union assets. Senior management may delegate due diligence to appropriate staff members as warranted, but is responsible for reviewing the information gathered and making the final decisions as well as implementing, maintaining, and enforcing these procedures. As part of this process, senior management must be familiar with and understand the reports available from the third party.

While control systems need not be elaborate for less complex third party arrangements, internal controls and audit functions will be established that are reasonably sufficient to assure senior management that third parties are appropriately safeguarding member assets, producing reliable reports, and following the terms of the third party arrangement. Additionally, senior management will tailor internal controls as necessary to ensure staff observes policy guidance for third party relationships.

Senior management will measure the performance of third party programs in relation to the Credit Union policy guidance, contractual commitments, and service levels at least annually.

THIRD PARTY NETWORK CONNECTIONS

The objective of these network connection standards and procedures is to ensure that reasonable measures are implemented to provide for a secure method of connectivity between Resource One Credit Union and all third party (partnering) companies and to provide a formalized method for the request, approval, and tracking of such connections.

Third Party Connection Requests and Approvals

All third party network connections must be reviewed and approved by the Director of Information Technology. In some cases, approval may be given at a lower level with pre-authorization.

Safeguarding Member Information – NCUA Compliance

When a third party company will have access to sensitive member or consumer information or member information systems through a network connection, as a part of the request and approval process for a network connection, their contract with the Credit Union will be reviewed. If the contract does not provide for compliance with the objectives of

NCUA regulations addressing the Safeguarding of Member and Consumer Information, an officer or senior manager of the partnering company will be required to sign an affidavit stating that the partnering company is in compliance with the objectives of NCUA regulations addressing the Safeguarding of Member Information and any other appropriate information security and privacy provisions required, but not covered by the current contract.[7] The third party service provider will be responsible for ensuring all possible measures have been taken to ensure the integrity and privacy of the Credit Union's confidential information.

Network Security

The third party will be solely responsible for ensuring that "authorized company employees" are not security risks and upon Resource One Credit Union's request, the third party will provide Resource One Credit Union with any information reasonably necessary for Resource One Credit Union to evaluate security issues relating to any authorized company employee.

Third Party Services and Access

In general, services provided over the third party/partner connections should be limited to only those services needed and to only those devices (hosts, routers, etc.) needed. Blanket access will not be provided for anyone. The default stance will be to deny all access and then only allow those specific services that are needed. In no case will the partner connection to Resource One Credit Union be used as the Internet connection for the partnering company. The standard set of allowable services is listed below:

- Support and Maintenance – When provided by a vendor, access to perform support and maintenance is allowed; however, communication with the Credit Union is required.
- Host data interface – Vendor specific interfaces with Credit Union systems (e.g., Internet Banking interface).

Network Connectivity Options

Third party access to Resource One Credit Union computer systems may be granted only when approved by the Director of Information Technology. The following connectivity options are the standard methods of providing a third party/partner network connection.

7 Please see Appendix M for a sample letter requesting an *Affidavit of Compliance* be signed to supplement the contract prior to allowing a network connection and Appendix L for a copy of an *Affidavit of Compliance* (depending on the services being provided, usually items 1, 3, and 5 will be required unless already included in the contract; remove the other *Affidavit of Compliance* items that are not needed).

Anything that deviates from this standard must have a waiver sign-off by the Director of Information Technology.

- Leased line (e.g., T1)
- Encrypted Tunnel
- Frame relay on ISDN
- Dial-up connection
- FTP with specific source and destination

The Director of Information Technology will monitor all aspects of third party connections. All third party connections will be reviewed on a quarterly basis and information regarding specific third party connections will be updated as necessary. Obsolete third party connections will be terminated.

WebEx Connections

Occasionally, the Credit Union may allow vendors to remotely access R1CU systems using WebEx to 1) provide support for an initial server or application installation, and/or 2) to provide ongoing support for an existing vendor software/hardware solution. All connections must be approved by a member of the IT Department or senior management.

To ensure WebEx connections are securely and effectively managed and adequately tracked the Credit Union will:

Limit access to WebEx services to designated senior management and IT staff by means of web filtering software. Senior Management will have the ability to initiate support only on select workstations, while IT staff will be capable of launching support at both the server and workstation level.

- Ensure the vendor providing the support has fulfilled the requirements of the aforementioned section, *Third Party Connection Requests and Approvals*.
- Require written documentation (e.g., email, etc.) from the vendor outlining the connection request, reasoning, and authorization for the session.
- Establish a secure VPN connection between the vendor and the Credit Union prior to starting a remote session to any Credit Union device.
- Approve each remote session and authorize each subsequent connection to other machines.
- Close all unused applications prior to executing the WebEx session to prevent inadvertent disclosure.
- Monitor the vendor's actions for the duration of the session.
- Force completion of the session once the support is complete.

- Maintain a Change Control/Change Management log that documents the allowed access event along with the vendor's initial connection request (e.g., email), as supporting documentation.

ONGOING VENDOR DUE DILIGENCE

Senior management will be responsible for maintaining a vendor list, including the risk rating noted for each vendor. The degree of due diligence will depend on the initial vendor risk assessment. Due diligence for a low-risk vendor may be nominal, while high-risk vendors require more thorough due diligence. All due diligence records performed should be kept with the vendor management files.[8]

When service providers will have full access to sensitive member or consumer information or maintain systems that contain sensitive member information, information security due diligence will be performed annually unless an exception has been granted by the CFO. The decision and the reasoning behind the decision must be documented.

Evaluation of Information Security Provisions – Existing Contracts

When service providers will have access to sensitive member or consumer information or maintain systems that contain member information, existing contracts will be reviewed before renewal to ensure that all current regulatory requirements have been met. Contracts that renew automatically will be reviewed whenever regulatory requirements for contracts with vendors change. Older contracts do not always contain provisions required by newer regulations.[9] If the Credit Union finds that some provisions are missing, one solution is to ask the service provider to sign an *Affidavit of Compliance* containing the missing provisions rather than requiring a new contract before the existing contract expires.[10]

- Provisions requiring the service provider to comply with all applicable federal and state laws and regulations addressing privacy, safeguarding member information, and response to unauthorized access to member information and member notice. If missing, use item 1 from the *Affidavit of Compliance*.
- Acceptable confidentiality and non-disclosure provisions. If missing, use item 3 from the *Affidavit of Compliance*.

8 Please refer to Appendix J for an *Existing Vendor Due Diligence Checklist*.

9 Please refer to Appendix O for a sample letter requesting that the service provider sign an *Affidavit of Compliance* to supplement their contract to bring it into compliance.

10 See Appendix N for an *Affidavit of Compliance* containing all required information security provisions (if some of the provisions are already included in the contract being reviewed, delete those items before sending to the service provider for signature).

- Provision that states the service provider will develop, implement, and maintain as part of its information security program appropriate measures to properly dispose of member and consumer information. If missing, use item 2 from the *Affidavit of Compliance*.
- Provisions addressing the service provider's responsibility for security of the Credit Union's member information. If missing, use item 3 from the *Affidavit of Compliance* – 4th paragraph omitting the opening "To that end."
- Provisions that define acceptable use of Credit Union information and resources by the service provider or subcontractors used by the service provider. If missing, use item 3 from the *Affidavit of Compliance* – 1st paragraph.

- Provision that the service provider is required to include appropriate language in their contracts with subcontractors who have access to member information or member information systems to protect the confidentiality and non-disclosure of non-public member information. If missing, use item 5 from the *Affidavit of Compliance*.
- Provision requiring the service provider to take action to address incidents of unauthorized access to the Credit Union's member information. If missing, use item 4 from the *Affidavit of Compliance* – 2nd paragraph.
- Provision that requires the service provider to report any physical or electronic breach of security that may compromise the privacy, integrity, or security of member information to the Credit Union. The service provider should agree to report to the Credit Union:
  - The nature of the intrusion.
  - The effect on Credit Union information.
  - Any corrective and responsive actions taken by service provider in response to the intrusion.

  If missing, use item 4 from the *Affidavit of Compliance*.
- When appropriate, a provision that states the service provider agrees to current and ongoing application vulnerability assessments. This provision has not been included in the *Affidavit of Compliance*; if required, this item will need to be added.

Evaluation of the Service Provider's Information Security Program

The Credit Union should review a medium or high risk service provider's information security program or summary of a medium or high risk service provider's information security program annually (if the service provider makes a Service Organizations Control Report - SOC 2 available to you, often key components of the information security program are included and can be reviewed that way). If the Credit Union determines that an annual review is not needed, the decision and the reason behind the decision must be documented and retained in the service provider's due diligence/contract file.

The information security program should contain key elements that:

- Ensure the security and confidentiality of member records and information.
- Provide standards to protect against any anticipated threats or hazards to the security or integrity of such records.
- Protect against unauthorized access to or use of such records or information that would result in substantial harm or inconvenience to any member and/or consumer.

- Provide for appropriate measures to properly dispose of member information and consumer information.

Evaluation of The Service Provider's Risk Assessment

The Credit Union will review a medium or high risk service provider's risk assessment annually. This could be in the form of one of the Service Organization Reports (SOC 1, SOC 2, or SOC 3) performed under SSAE16 (Statement on Standards for Attestation Engagements); however, other types of assessments may be acceptable, or even more appropriate in some cases, such as a penetration testing summary or a vulnerability assessment. For those vendors providing applications to the Credit Union, the Credit Union will review annually the application vulnerability assessment or an executive summary of the assessment.[11]

If the Credit Union determines that an annual review of the service provider's risk assessment is not needed, the decision and the reason behind the decision will be documented and retained in the service provider's due diligence/contract file. Key elements to consider:

- Performed at arm's length by an independent company.
- Vulnerability testing.
- Evaluation of operating and security controls.

Annual Application Due Diligence Review

For applications that present higher risks, the Credit Union should require evidence of adhering to sound processes and validation through independent third party vulnerability assessment or testing and/or audits on a periodic basis. A copy or executive summary of the most recent assessment should be requested at least annually.[12] Review the information to determine whether the application has any known open vulnerabilities and the nature of those vulnerabilities and if they are a cause for concern. If the vulnerability has not already been remediated, understand the vendor's plan and timeframe for doing so. The *Application Security Due Diligence Checklist* should be used to document the findings.[13]

If the vendor does not have a third party who conducts application vulnerability assessments, ask the vendor to describe their internal methodology for providing any

11 An example of a letter to a vendor requesting application security compliance assurance may be found in Appendix N.

12 If the Credit Union decides an annual review is not necessary, the decision and the reasoning behind the decision should be documented.

13 Please refer to Appendix F.

application updates. Assess the methodology using the guidance in the FFIEC IT Handbook Software Development and Acquisition.[14]

DOCUMENTATION OF DUE DILIGENCE AND OVERSIGHT

The Director of Information Technology will maintain a Due Diligence/Contract File for each third party service provider who has access to member information or member information systems. The file will contain as appropriate:

- A copy of the Credit Union's contract with the third party service provider.
- A copy of the *Vendor Risk Rating Form*.[15]
- A copy of the New *Vendor Due Diligence Checklist* and all *Existing Vendor Due Diligence Checklists*.[16]
- An *Affidavit of Compliance - Confidentiality and Non-Disclosure* if the contract does not already contain acceptable confidentiality and non-disclosure provisions.[17]
- An *Affidavit of Compliance - Security Breach Notification* if appropriate language is not contained in the contract.[18]
- Unless provided in the contract, an *Affidavit of Compliance* stating that the third party service provider will comply with all applicable state and federal privacy and information security laws and regulations.[19]
- Unless provided for in the contract, an *Affidavit of Compliance* stating that the third party service provider is in compliance and will ensure the proper disposal of member information and consumer information.[20]
- If the contract was subject to legal review, a summary of the legal review.
- If the vendor/service provider was subject to financial review, a summary of the financial review.
- Proof of bonding or insurance when applicable.
- A summary of the background investigation if one was conducted.

14 This handbook can be found at http://ithandbook.ffiec.gov/it-booklets/development-and-acquisition.aspx.

15 Please refer to Appendix H.

16 Please refer to Appendix I and J.

17 The language in item 3 of the *Affidavit of Compliance* located in Appendix L may be used.

18 The language in item 4 in the *Affidavit of Compliance* located in Appendix L may be used.

19 The language in item 1 of the *Affidavit of Compliance* located in Appendix L may be used.

20 The language in item 2 of the *Affidavit of Compliance* located in Appendix L may be used.

- A copy or executive summary of the third party service provider's information security policy.[21]
- A copy of the third party service provider's most recent Service Organization Report (SOC 1, SOC 2, or SOC 3) performed under SSAE16 (Statement on Standards for Attestation Engagements), and/or an executive summary of any other third party vulnerability or risk assessment, and/or penetration test.[22]
- Documentation on application security if appropriate.[23]
- Copies of any relevant correspondence with the third party service provider. This includes any correspondence sent regarding bringing an existing contract/agreement into compliance.
- Documentation of all oversight activities including a summary of findings and follow-up activities.

21 Please see Appendix M for a sample letter requesting this and the most recent risk assessment.

22 Please refer to Appendix O for a sample letter.

23 Please refer to Appendix N for a sample letter requesting application security assurance.

Historical Record of Policy Changes

This policy is a complete rewrite.

Date Rewritten: July 2013
Date Ratified: July 2013