1. INTRODUCTION
Some of the most important people we will ever work with at CREDIT UNION are those who are employed by our vendors. As such, it is our desire to treat our vendor relationships with utmost care and professionalism.

CREDIT UNION relies on vendors to perform a range of services and provide products for CREDIT UNION and CREDIT UNION members. Financial industry regulations and business best-practices require that we perform a risk assessment on our vendors and perform additional due diligence commensurate with the identified risk. Building and sustaining effective, positive vendor relationships directly correlates with how we are able to delight our members, make the most of limited resources, minimize risk, keep a true regulatory course, enhance our standing in our community, and protect the information and assets in our care.

2. PURPOSE
The purpose of this policy is to provide a framework for managing the lifecycle of vendor relationships and provide context for CREDIT UNION procedures that outline specific systems and guidelines for vendor management.

3. SCOPE
This policy applies to all CREDIT UNION business entities including individuals, departments, or subsidiaries who engage vendors as defined in this document.

4. REFERENCES
California Civil Code
Contract Negotiation and Amendment Tool
Document and Data Destruction Procedure
CREDIT UNION Confidentiality Agreement

5. DEFINITIONS
The following definitions are provided for the purposes of this policy.

Vendor
A company or individual that provides a product or performs a service for CREDIT UNION and also meets any of the following criteria:

• Performs services at CREDIT UNION facilities
  *(Safety, insurance, or data security risk.)*

  *Examples:* Consultants who perform work onsite, auditors, equipment repair companies, gardeners, and deliveries past the reception desk. Deliveries to the reception desk are excluded.

• Has access to member or other sensitive data
  *(Data security risk.)*
Examples: Some consultants, banking service providers, some software maintenance vendors, and auditors.

- Has a contractual commitment to CREDIT UNION

  *(Financial or member service risk.)*

  Examples: Contracted maintenance services, major software vendors, and contracted supply companies

**Contract or Agreement**
A legal document, between CREDIT UNION and a vendor, in which the vendor agrees to provide services or products and, for which, CREDIT UNION agrees to render payment.

**Vendor Risk Rating**
A Low, Medium, or High rating assigned as a result of the “Vendor Risk Assessment” that indicates the relative risk this vendor represents to CREDIT UNION.

6. **POLICY**

It is the policy of CREDIT UNION to effectively manage the lifecycle of all vendor relationships in order to responsibly steward resources and minimize the inherent risk associated with engaging third parties to perform services.

Vendor management, as addressed by this policy consists of:

- Vendor Risk Assessment
- Vendor Due Diligence
- Contract Management
- Vendor Supervision

*Appendix A Implementation Guidelines* provide best-practice activities for effectively implementing the Vendor Management Policy.

6.1 **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 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 that vendor. Exceptions to the assigned risk rating may be granted as noted by the Risk Rating Matrix.

The Rating is an indicator of the level of due diligence CREDIT UNION requires for each vendor.

- 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.
- High risk vendors require annual due diligence review.
## Vendor Risk Rating Matrix

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
<th>Exceptions Granted By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Impact</td>
<td>Nominal business impact</td>
<td>Significant, but non-critical business impact</td>
<td>Mission Critical</td>
<td>EVP</td>
</tr>
<tr>
<td>Member Contact</td>
<td>None</td>
<td>Indirect</td>
<td>Direct</td>
<td>EVP</td>
</tr>
<tr>
<td>Total Contract Amount (Full term for multi-year contracts)</td>
<td>&lt;$10,000</td>
<td>$10,000 -- $50,000</td>
<td>&gt;$50,000</td>
<td>EVP</td>
</tr>
<tr>
<td>Contract Term</td>
<td>One year or less</td>
<td>1 to 3 years</td>
<td>&gt; 3 years</td>
<td>EVP</td>
</tr>
<tr>
<td>Access to Non-Public Personal Information (NPPI) for either members or employees</td>
<td>No access, except for possible unintentional exposure.</td>
<td>N/A</td>
<td>Access expected</td>
<td>Information Security Systems Administrator or Director of Compliance and Internal Controls</td>
</tr>
<tr>
<td>Safety of CREDIT UNION Employees, Guests and Vendors</td>
<td>Injury or Illness – No Potential</td>
<td>Injury or Illness – Low Severity</td>
<td>Injury or Illness – High Severity</td>
<td>Safety Officer</td>
</tr>
</tbody>
</table>

### 6.1.1 Risk Re-assessment
Risk assessments should be revisited as part of contract renewal or anytime the relationship with the vendor changes in any significant way.

### 6.1.2 Department Vendor List
Each department will retain a complete vendor list, including low risk vendors, with the risk rating noted for each vendor. This list shall be available for the Compliance Officer to include in the annual report to the Supervisory Committee.

### 6.2 Vendor Due Diligence
Due diligence requires a reasonable inquiry into a vendor's ability to meet the requirements for the proposed service. The degree of due diligence required in selecting a vendor will depend on the results of the initial Vendor Risk Assessment. Due diligence for a low risk vendor may be nominal, while high risk vendors require more thorough due diligence. Appendix A contains additional information about completing a due diligence
analysis. All due diligence records performed in establishing the vendor relationship, including the Risk Rating, should be kept by the Vendor Relationship Manager.

6.3 **Contract Management**

While acknowledging that even the most comprehensive agreement cannot replace the effectiveness of a relationship built on trust, a clearly drafted and equitable contract will protect CREDIT UNION and provide a structure for expectations and issue resolution. The level of detail and relative importance of contract provisions varies with the scope and risks of the services and products provided.

6.3.1 **Contract Negotiation**

Vendor negotiations should be delegated only to qualified staff with proven skills appropriate to the level of risk represented by the vendor relationship.

Medium or High risk, complex, or unusual contracts should be considered for review by the following designees, as appropriate to the scope and type of contract:

- **Legal Counsel.** *Review by legal counsel typically only addresses the legal perspective and does not relieve management of the responsibility to review it from all perspectives.*
- **VP Information Systems.** *Required for all contract negotiations related to software, hardware, and Information Systems.*
- **Director of Compliance and Internal Controls**
- **Director of Insurance and Risk Management**

6.3.2 **Contract Language**

Contract language should be reviewed to ensure that the agreement or contract meets regulatory requirements and does not expose CREDIT UNION to unnecessary risk.

6.3.3 **Contract Approval and Renewal**

Vice Presidents are responsible for the contracts executed by their staff. Medium and High Risk vendor contracts, including renewals, are to be executed by a VP or above.

6.3.4 **Contract Cancellation**

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.

6.3.5 **Contract File Retention**

Vendor contract files will be stored for four years after contract expiration in compliance with California Civil Code that identifies the statute of limitations for California contracts as four years.
6.4 Vendor Supervision
Each vendor will be assigned a Vendor Relationship Manager who will complete the vendor risk analysis, vendor due diligence review, maintain vendor files, and act as vendor liaison.

The Compliance Officer, as part of the Security Program Report, will provide an annual status report of Medium and High risk vendors to the Supervisory Committee.

7. RESPONSIBILITY
• Senior Management is responsible for implementing, maintaining, and enforcing this policy.
• The department Vice President is responsible for:
  – Approving Medium and High Risk vendor contracts
  – Appointing Vendor Relationship Managers for all department vendors.
  – Ensuring Vendor Relationship Managers comply with this policy.
• Vendor Relationship Managers are responsible for:
  – Completing a Vendor Risk Assessment
  – Completing a Vendor due diligence review
  – Maintaining vendor files
  – Effectively acting as vendor liaison.

8. REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending</td>
<td>Original Issue</td>
</tr>
</tbody>
</table>

9. APPROVAL

9.1 Approve
COO

9.2 Review
VP IS
Compliance
Risk

10. APPENDIX A IMPLEMENTATION GUIDELINES
Appendix A provides guidelines for effectively implementing the Vendor Management Policy and is employed as directed by the department Vice President.
## 10.1 Completing a Vendor Risk Assessment


2. Review the substantive risk exposure to CREDIT UNION if the product or service fails or is inadequately performed.

<table>
<thead>
<tr>
<th>Risk Exposure Category</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulatory</td>
<td>• Can the vendor create regulatory risk for CREDIT UNION?</td>
</tr>
<tr>
<td>Reputation</td>
<td>• Can the vendor impact CREDIT UNION’s reputation?</td>
</tr>
<tr>
<td>Financial</td>
<td>• Can the vendor impact CREDIT UNION or its members financially?</td>
</tr>
<tr>
<td></td>
<td>• Does CREDIT UNION or the vendor have insurance that will allow CREDIT UNION to transfer some of the risk?</td>
</tr>
<tr>
<td>Member or other Sensitive</td>
<td>• To what extent will the vendor handle sensitive CREDIT UNION data?</td>
</tr>
<tr>
<td>Data Access</td>
<td></td>
</tr>
<tr>
<td>Operational Effectiveness</td>
<td></td>
</tr>
<tr>
<td>Process Risk</td>
<td>• How would the vendor’s failure impact CREDIT UNION’s business needs and strategic objectives?</td>
</tr>
<tr>
<td>People Risk</td>
<td>• Could CREDIT UNION step in and perform the critical functions provided by the vendor if the vendor failed to perform?</td>
</tr>
<tr>
<td>System Risk</td>
<td>• Are there other potential vendors that could readily assume service should the current provider fail?</td>
</tr>
<tr>
<td></td>
<td>• Can CREDIT UNION provide adequate oversight of the vendor’s function?</td>
</tr>
<tr>
<td></td>
<td>• Can the vendor create risk to CREDIT UNION’s processes, people, or systems?</td>
</tr>
<tr>
<td></td>
<td>• Would CREDIT UNION be considered the “Controlling Employer” for this vendor?</td>
</tr>
<tr>
<td></td>
<td>• Would CREDIT UNION be placed in a position of “Joint Employer’s Liability” for this vendor?</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>The terms “Controlling Employer” and “Joint Employer’s Liability” usually apply to staff employed by an outside company, such as a staffing agency, but whose work place activities are directed by CREDIT UNION. Direct questions regarding these designations to the</td>
</tr>
</tbody>
</table>
10.2 Completing a Due Diligence Analysis

1. Review the following, as appropriate, based upon the Vendor Risk Rating and the type of risk exposure created by this vendor relationship:
   • SAS -70’s or audit reports
   • Industry expertise
   • Return on Investment
   • Background Check, including client references and independent sources
   • Staffing experience and expertise
   • Internal controls
   • Financial condition and annual reports
   • Insurance coverage
   • Privacy policy review
   • On-site visits

2. Record and retain the analysis with the Relationship Manager Records.

10.3 Managing the Contract

Vendor relationship documentation varies with the scope and risks of the services and products provided. The process includes:

• Negotiating the Contract
• Reviewing the Contract Language
• Approving and Renewing the Contract
• Canceling the Contract
• Retaining Contract Files

10.3.1 Negotiating Contracts

This process is completed by qualified staff with proven skills appropriate to the level of risk represented by the vendor relationship.

1. Review each contract from four perspectives:

<table>
<thead>
<tr>
<th>Perspective</th>
<th>Consideration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal</td>
<td>• Are CREDIT UNION’s interests adequately protected if a problem arises with this vendor?</td>
</tr>
<tr>
<td>Financial</td>
<td>• Does the agreement reasonably assure that CREDIT UNION’s</td>
</tr>
</tbody>
</table>
### Operational
- Are the terms of the agreement operationally feasible for CREDIT UNION?, including:
  - Timing considerations
  - Service levels
  - CREDIT UNION performance commitments
  - Technology compatibility
  - Human safety

### Risk Management
- Are the terms of the agreement acceptable in light of regulatory, financial, operational, and reputation risks?

2. Complete the levels of review as directed in 6.3.1 of the Vendor Management Policy.

3. Maintain multiple vendor candidates for as long as possible to enter the negotiation stage with important leverage. The possibility that CREDIT UNION could select an alternate vendor may prove invaluable to obtaining the vendor’s agreement to important contract provisions.

4. Record negotiations and contact between a potential vendor and the CREDIT UNION using the *Contract Negotiation and Amendment Tool*, Microsoft Word's *Track Changes*, or other tools.

5. Retain the negotiation records in the Vendor Relationship Manager’s files for the life of the contract.

#### 10.3.2 Evaluating Contract Language

1. Verify that the language in the agreement or contract meets regulatory requirements and does not expose CREDIT UNION to unnecessary risk.

2. Verify that the essential components of the agreement include:
   - Performance standards, expectations, and responsibilities
   - Fees and payment terms
   - Term length
   - Termination provisions
   - Insurance Requirements

3. Evaluate the agreement for what it *does not state*, as well as for what it does state.

4. Verify that the vendor’s standard agreement includes all the necessary clauses.

5. Consider the appropriateness of the following clauses.
• Definitions
• Scope of work
• Process for changing scope of work
• Installation and training requirements
• Ownership of any work product or intellectual property
• Acknowledgement that the vendor is subject to regulatory review
• Privacy and information security
• Confidentiality Agreement
• Limitations of liability
• Indemnity
• Warranties
• Standard CREDIT UNION dispute resolution provisions
• Choice of law
• Choice of venue
• Service Level Agreement, including:
  – Acceptable range of service quality and applicable timeframes
  – Definition of what is being measured
  – Formula for calculating the measurement
  – Mechanism for ongoing monitoring, and supervision
  – Type and timing of reporting on the status of performance
  – Penalties or credits for meeting, exceeding, or failing to meet targets

10.3.3 Approving Contracts

1. Execute the contract with the appropriate level of approval as outlined in section 6.3.3 of the Vendor Management Policy.

2. When a contract is due for renewal, complete the following:
   a. Review and update the Vendor Risk Rating.
   b. Review and update the Vendor Due Diligence Report.
   c. Review contract terms.

10.3.4 Canceling Contracts

When canceling a contract:

1. Follow agreed upon contract language.
2. Execute at the same or higher level of the organization as the original contract execution.

10.3.5 Retaining Contract Files
Complete the following based upon file type:

<table>
<thead>
<tr>
<th>File Type</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department Vendor List</td>
<td>Maintain a complete list of department vendors with the risk rating noted for each vendor.</td>
</tr>
<tr>
<td>Original Vendor Contract File</td>
<td>Retain the originals of all contracts, agreements, and other essential documentation of the vendor relationship in the centralized Enterprise file location for four years after contract expiration.</td>
</tr>
<tr>
<td>Working Vendor Contract File</td>
<td>Retain copies of all contracts, agreements, and other essential documentation in the Vendor Relationship Manager’s work files along with the negotiation records.</td>
</tr>
</tbody>
</table>

10.4 Supervising Vendors
The Vendor Relationship Manager completes the following:
1. Assigns Vendor Risk Rating using the Vendor Risk Rating Matrix.
2. Completes Vendor Due Diligence Analysis, as appropriate for the risk rating.
3. Completes periodic due diligence review (at least annually for High risk vendors).
4. Coordinates and documents ongoing vendor communication.
5. Maintains vendor files.
6. Compiles and maintains vendor information, including:
   - Vendor name and contact information
   - Service or product provided
   - Risk rating
   - Contract expiration
   - Renewal dates and terms
   - Regulatory requirements
   - Insurance Requirements
   - Required vendor reports
   - Date of last review and next review
   - Triggers for annual and interim reviews
   - Contract amount
   - Number of licenses, if applicable
7. Monitors vendor compliance to contract terms.
8. Coordinates contract renewal with appropriate contract approver.

11. **RESPONSIBILITY**

   - Each Vice President is responsible for implementing these guidelines as appropriate to the department.
   - The Vendor Relationship Manager is responsible for following the implementation guidelines as directed by the department Vice President.

12. **REVISION HISTORY**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending</td>
<td>Original Issue</td>
</tr>
</tbody>
</table>

13. **APPROVAL**

13.1 Approve  
   VP IS

13.2 Review  
   Compliance

14. **RELATED DOCUMENTS**

<table>
<thead>
<tr>
<th>Type of Document</th>
<th>Document Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>Vendor Management Policy</td>
</tr>
<tr>
<td>Form</td>
<td>Contract Negotiation and Amendment Tool</td>
</tr>
<tr>
<td></td>
<td>CREDIT UNION Confidentiality Agreement</td>
</tr>
</tbody>
</table>