**Policy**

It is the policy of \_\_\_ Federal Credit Union to ensure coordinated and consistent management of critical vendors as part of its overall risk management, maintain member privacy and confidentiality of member information and ensure full compliance with the requirements applicable law and regulations regarding risk management, vendor and contract management and management of third party service providers including the following:

* The Financial Services Modernization Act (Gramm Leach Bliley Act (GLBA));
* Title V, NCUA Regulations Part 748 and appendices
* NCUA Letter to Credit Unions 00-CU-11 “Risk Management of Outsourced technology Services;”
* NCUA Letter to Credit Unions 07-CU-13 “Vendor Review and Due Diligence;”
* NCUA Letter to Credit Unions 01-CU-20 “Due Diligence over Third Party Service Providers;”
* NCUA Letter to Credit Unions 02-CU-17 “E-Commerce Guide for Credit Unions;”
* FFIEC guidelines; and
* The credit union’s policies and procedures.

**Business Owner and Compliance**

The board of directors and management are accountable for policy development, implementation and guiding compliance. Each vendor relationship will have a member of management responsible for the vendor relationship and the manager for a contract (Business Owner) will play a key role in reviewing and deciding compliance related issues and will be responsible for reporting and documentation as defined by the vendor management program.

All managers directly responsible for or having the authority to engage external services, purchase new products or have signing authority for outsourcing contracts shall comply will the procedures set by this program.

Management is responsible for planning, directing, and controlling the credit union’s affairs. To fulfill these duties, management will require a risk assessment and a due diligence review prior to entering into any arrangement with a third party.

**Vendor Management Procedures**

This program establishes accountability, procedures and standards for selection and management of the credit union’s vendors.

**New Product or New Service**

The Business Owner will do the following for each new product or service:

1. Establish service or product need
2. The Business Owner will complete a preliminary risk assessment questionnaire for the service or product under consideration using the attached form and share the same with management.
3. The Business Owner will research and respond to questions and concerns posed by other managers or the board.
4. If high risk concerns are not mitigated by the Business Owner, the Business Owner will confirm acceptance of that risk through a memo to the file and document the decision in the due diligence file for such vendor(s). If the risk assessment results support further action, proceed to the next step.
5. Identify vendors who can provide service or product
6. Prepare a Request for Proposal (See **Request for Proposal** section below).
7. Perform due diligence review as required (See **Vendor Due Diligence** below).
8. If necessary, request vendor presentations for the finalists.
9. Execute the contract and forward copies to vendor and Maple Street to add to contract and vendor databases.
10. Conduct follow up meetings with all departments or areas affected by the new service or product.
11. Proceed with implementation that includes the following:
12. Timeline for implementation
13. Policies and procedure development, revision or deletion including communication of such changes
14. Training scheduled/completed as required.

**Request for Proposal**

* Requests for Proposals (RFPs) will be completed when considering adding or changing a service provider or product.
* Management will determine the necessity of following the RFP process for vendor contract renewals and the decision to outsource the negotiation and RFP process.
* The Business Owner will complete a RFP as outlined in the attached example RFP.
* The Business Owner will determine the number of vendors to send an RFP.
* The timeframe for completing and mailing of RFPs will be directed by the Business Owner.
* Once RFPs have been returned by the vendors, the Business Owner or assigned staff will schedule meetings to review proposals and select a vendor.
* The timeframe for review and selection of a vendor will be directed by the Business Owner.
* The vendor(s) selected will be subject to the required due diligence review.

**Vendor Due Diligence**

1. Business Owners will evaluate all vendor products and services, negotiate the prices and negotiate the contract terms before contracting with the vendor. The type of evaluation will vary and should be commensurate with risk, complexity and product or service cost. A formal due diligence analysis will be conducted for any relationship where the combined implementation and annual contract costs exceed $25,000.
2. The Business Owner will contact Maple Street and use the Maple Street vendor management database to determine what due diligence information is to be gathered from the vendor(s) by Maple Street or the credit union and added to the database.
3. A Business Owner has the discretion to alter this amount or waive this requirement up to his/her authorized signing limits. Any alteration of the amount or waiver of this requirement must be documented in the due diligence file of the 3rd party vendor.
4. Verbal product and service agreements are prohibited. All vendors must provide, depending upon the services and products engaged, a purchase invoice, legal contract and/or service agreement.
5. Purchasing authority thresholds for all executives and managers are documented in credit union’s other policies and procedures.
6. The Business Owner will appoint, as needed, appropriate staff members to perform a due diligence review prior to entering into any arrangement with a third party vendor and due diligence reviews for existing third party vendors.
7. The Business Owner will enter all new or existing vendors due diligence reviews into the Maple Street vendor management database. Business Owners will complete applicable sections in the Maple Street database as the information is obtained and/or the step is completed. The review will be conducted to detect unwarranted exposure to operations, reputation, compliance or strategic risk.
8. The Business Owner will review the contract(s) along with the supporting due diligence in order to determine if any outstanding issues exist.
9. If the credit union is then willing to contract with a vendor, the Business Owner will execute the contract and proceed with implementation of service or product as defined in Section I above (New Product or Service Provider).

**On-going Oversight of Third Party Vendors**

1. Business Owners will have the responsibility for the management of the vendor relationship.
2. The Business Owner, either directly or through the assistance of staff will conduct oversight reviews for third party services in accordance the appropriate laws, regulations and policies/procedures.
3. The Business Owner will record the results of the oversight review for the third party services in the Maple Street vendor database and will determine the appropriate action for the credit union. This will include reporting the results to management or the board, if necessary, who will then determine the appropriate action.
4. The Business Owner will document the results of the due diligence in the Maple Street vendor due diligence database.
5. Appropriate action is defined as one of the following actions:
6. approval to continue service with vendor;
7. approval to continue service with the vendor, but on conditions of additional information and/or more frequent review;
8. begin a process to review other vendors; or
9. terminate the service/product for the credit union.
10. The Business Owner will document the appropriate action in the Maple Street vendor management database.

**Legal Review Standards**

Vendor reviews may require external legal review. The Business Owner or the Senior Executives can request external legal counsel. Legal review *may be* required *when one or more* of the following conditions exist:

* + The contract exceeds $25,000 in cumulative fees or annual recurring cost;
	+ The relationship and/or the contract is unusually complex in terms of operational matters, legal terms and provisions, fee structures, third party involvement and/or the potential for excessive liability to the credit union;
	+ The vendor is critical to operations and its reputation is not known or it has limited market presence;
	+ Vendor is unwilling to amend or include critical contract changes requested by the credit union.

**Contract Standards Checklist**

Per Federal Financial Institutions Examination Council (FFIEC) guidelines, legal contracts and service agreements shall define for both parties, as applicable:

* Service or product definitions and service level expectations (performance and reliability standards);
* Technology specifications and operational responsibility;
* Confidential Information privacy and security;
* Vendor reporting and documentation standards;
* Audit rights;
* Business continuity and disaster recovery reporting and standards
* Subcontract and third party responsibility and liability;
* Detailed fee structure and billing terms; and
* General terms: liability limitations, recourse, warranties, arbitration, termination, contract expiration, assignment and indemnification.

**Reporting and Documentation Standards**

Business Owners will ensure that all vendor and contract information is provided to Maple Street.

* 1. Vendor contracts, regardless of criticality, are entered by Maple Street into the Maple Street vendor/contract database and assigned a risk rating by the Business Owner.
	2. The Business Owner will file the signed original in the credit union’s files and will send a copy to Maple Street.
	3. The Business Owner will work with Maple Street to make sure the completed due diligence information is loaded into the vendor database. The information should include:
		1. Fully signed contract with all service level agreements and addenda, non-disclosure agreements, confidentiality agreements or invoices, together with a completed contract checklist;
		2. Vendor due diligence documentation such as most recent audited financials/annual report and independent internal control reviews (SAS-70, type 2);
		3. Material communications such as disputes, contract changes, fee changes, service or performance issues;
		4. Due diligence checklist; and
		5. Completed risk assessment (as required).

**Relationship Monitoring Standards**

Per FFIEC requirements and GLBA critical vendors shall receive annual financial and internal control reviews.

The Business Owner assigns a vendor risk rating at the time of engagement and is reviewed periodically through the term of the contract. The Business Owner should base criticality on the following elements:

1. **Criticality:** Impact to operations if the service or product was suddenly not available and/or excessive liability to the credit union.
2. **Dependence:** Degree of difficulty involved in finding and implementing a service or product replacement.
3. **Financial Commitment:** Higher financial commitment equates to higher risk of financial loss if relationship were to fail.
4. **Performance:** Vendors with substandard or unproven performance require a higher degree of monitoring by the Business Owner.
5. **Regulatory Impact**: Vendor’s ability to impact the credit union’s level of regulatory compliance.
6. **Business Impact**: Vendor’s ability to impact business reputation or strategy.

The following monitoring frequency is required. Notwithstanding the chart below, periodic review is required if deterioration in performance or financial performance is observed.

|  |  |
| --- | --- |
| **Vendor Classification** | **Monitoring Requirement** |
| 1 Critical  | At time of contract, at renewal and every year |
| 2 Important  | At time of contract and at renewal |
| 3 Non-essential  | At time of contract |

**Vendor Monitoring Standards**

Business Owners will schedule their vendor review dates.

Review dates are flexible and may be set to coincide with the vendor’s fiscal or calendar financial reporting dates, annual contract renewals, service issues or receipt of internal control reports.

Business Owners will use the Maple Street vendor database to record annual vendor reviews. Material adverse issues should be clearly documented and brought to the attention of management. Review standards include:

|  |  |  |
| --- | --- | --- |
| **Performance** | **Internal Controls** | **Financial** |
| * Service levels
* Uptime statistics
* Support response
* Member satisfaction
* Fee increase
 | * Type of Report
* Unfavorable Items
* Certifications
 | * Key financial ratios
* Type of Audit or Report
* Unfavorable trends
 |

**Attachment A**

**Critical Vendors**

**Vendors Subject To Initial Due Diligence**

* Any vendor providing critical or essential support, services or products to the credit union whose non-performance could cause a disruption to member service
* Any vendor who has or has access to non-public personal member information
* Data processing system
* Online banking provider
* Bill payer provider
* Loan system provider
* Statement processor
* Insurance/bond providers
* Security systems provider
* Check provider/processor
* Traveler's check & money order provider
* Forms printer/provider
* Hardware provider

**Vendors Subject To Ongoing Due Diligence**

* Data processing system provider
* Online banking provider
* Bill payer provider
* Loan system provider
* Insurance/bond providers
* Check provider
* ACH/Check processor
* Disaster Recovery provider
* Plastics provider
* ATMs
* Any other vendor as determined by the Business Owner

**NOTE -** *The list of vendors above is not meant to be represent all vendors subject to due diligence.*