**Policy 2185: Third-Party Vendor Due Diligence and Oversight**

**Model Policy Revised Date: 5/6/2025**

**General Policy Statement:**

The Board of Directors is responsible for planning, directing and controlling [[CUname]]'s (Credit Union) affairs. In an effort to enhance the services provided to members, the Credit Union often partners with outside parties. Due diligence reviews are required prior to entering into any arrangement with a third-party vendor. The purpose of this policy is to set forth the guidelines for management and staff to use in establishing and maintaining due diligence policies and procedures in order to minimize the risk of unanticipated costs, legal disputes and asset losses.

1. **POLICY AND PROGRAM RESPONSIBILITY.**  
   1. **Board Responsibility.** This policy and any recommended changes shall be approved by the Board of Directors ("Board").
   2. **Management Responsibility.** Credit Union management ("management") will be responsible for the development, implementation, and maintenance of the Credit Union's vendor due diligence program. As part of this responsibility, management will maintain a list of all third-party providers, along with the scope of services provided by each and the rationale for outsourcing the services provided. Management may delegate due diligence to appropriate staff members as warranted but shall be responsible for reviewing the information gathered and making the final decisions. All due diligence efforts will be documented and provided to the Board.
2. **PLANNING**  
   1. **Risk-Assessment.** Prior to engaging in a proposed activity, the Credit Union will perform a risk-assessment to determine whether the relationship complements the Credit Union’s overall mission and philosophy. Management will determine whether the proposed activities, related costs, product and services standards, and third-party involvement, are consistent with the credit union’s overall business strategy and risk tolerances. If the Board does not believe the proposed activity would complement the strategic vision for the Credit Union, the third-party vendor relationship will not be pursued. Risk assessments are part of the Credit Union’s broader risk management strategy and ongoing risk assessments will occur, as determined by the level of risk to the Credit Union. The risk assessment will document a risk rating based on the highest risk level the vendor may impose on the Credit Union. The higher the risk rating of the vendor, the more detailed and frequent the risk assessment and diligence the Credit Union will perform.  
      1. **Documentation.** Management will document how the relationship corresponds with the Credit Union’s strategic plan, considering long-term goals, objectives and resource allocation requirements. Consistent with the Credit Union’s Strategic Plan, management will design action plans to achieve objectives in support of strategic planning for new third-party vendor arrangements. Management will also clearly define the nature and scope of the Credit Union’s needs, which needs will be met by the third party, and to what extent the third party will be responsible for the desired results.
      2. **Categories of Risk.**The Credit Union will consider all seven risk areas (Credit, Interest Rate, Liquidity, Transaction, Compliance, Strategic, and Reputation). Some additional risks to be assessed include: loss of capital if the venture fails; loss of member confidence if the program, product or service fails to meet member expectations; costs associated with attracting or training personnel and investing in required infrastructure; and whether the potential benefit of the arrangement outweighs the potential risks or costs.
      3. **Periodic.**The risk assessment will take place in advance of the decision to offer new products and services and will be conducted periodically as long as the product or service is offered. The risk assessment will be shared with the Board.
   2. **Financial Projections.** In evaluating the cost-benefit or risk-reward of the third-party vendor relationship, the Credit Union will develop financial projections outlining the range of expected and possible financial outcomes. The Credit Union will project a return on its investment, considering expected revenues, direct costs and indirect costs. Financial projections will be in line with the context of the Credit Union’s strategic plan and asset-liability management (ALM) framework.
   3. **Insurance Review.**Third-party vendor relationships can result in increased liabilities. Therefore, Credit Union will maintain an adequate review of the Credit Union’s insurance coverage, including the fidelity bond and policies covering such matters as errors and omissions, property and casualty losses, and fraud and dishonesty. When appropriate, the Credit Union will ensure that it is the beneficiary on all insurance policies and will review all insurance contracts to ensure full coverage.
   4. **Exit Strategy.** The Credit Union will investigate and determine whether there is a reasonable way out of the relationship if it becomes necessary to change course in the future, along with whether there are any other providers that can perform critical services.
   5. **Accounting.** The Credit Union will ensure that it has a sufficient accounting infrastructure to appropriately track, identify and classify transactions in accordance with generally accepted accounting principles (GAAP). When necessary, the Credit Union will obtain guidance from a certified public accountant (CPA) to ensure proper accounting treatment.
3. **BACKGROUND CHECK.**The Credit Union will research and/or interview several prospective organizations to determine which is best qualified to meet the Credit Union’s needs. If the relationship will require a significant investment of resources and capital, the Credit Union will consider hiring a consultant or industry expert to assist in its evaluation, upon approval of the Board. It is also important to understand how the third party has performed in other relationships. Management will contact other credit unions or clients of the third party. Other sources such as the Better Business Bureau and the Federal Trade Commission will be consulted to determine complaint histories on businesses. The Credit Union will review and consider any lawsuits or legal proceedings involving the third party and/or its principals. The Credit Union will also ensure that the third party and/or its agent(s) have all of the required licenses or certifications, and that they remain current for the duration of the relationship.
4. **BUSINESS MODEL REVIEW.**Before entering into a third-party vendor relationship, the Credit Union will investigate and understand the third party’s business model – the conceptual architecture or business logic employed to provide services to its clients. If the third party’s business and marketing plans are available, the Credit Union will review them. Management will 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 will also 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 the revenue stream is tied to loan origination volume rather than loan quality). The Credit Union will also identify any vendor-related parties (subsidiaries, affiliates or sub-contractors) involved with the proposed arrangement, understanding the purpose and function of each. When these parties are to play a critical role in the relationship, the Credit Union will perform its due diligence on these vendor-related parties.
5. **CASH FLOWS.** The Credit Union will understand how cash flows move between all of the parties in the third-party relationship. Management will be able to explain how cash flows (both incoming and outgoing) move between the Credit Union, the third party and the Credit Union’s members. The Credit Union will also independently verify the source of these cash flows and match them to related individual accounts.
6. **LEGAL REVIEW.**All contracts will be reviewed by the Credit Union’s legal counsel. At a minimum, third-party contracts should address the following:  
   1. Scope of arrangement, services offered and activities authorized;
   2. Responsibilities of all parties (including subcontractor oversight);
   3. Service level agreements addressing performance standards and measures;
   4. Performance reports and frequency of reporting;
   5. Penalties for lack of performance;
   6. Ownership, control, maintenance and access to financial and operating records;
   7. Ownership of servicing rights;
   8. Audit rights and requirements (including responsibility for payment);
   9. Data security and member confidentiality (including testing and audit);
   10. Business resumption or contingency planning;
   11. Insurance;
   12. Member complaints and member service;
   13. Compliance with regulatory requirements (i.e., Privacy, BSA, etc.);
   14. Dispute resolution; and
   15. Default, termination and escape clauses.
7. **FINANCIAL REVIEW.** Financial statements of the third-party vendor and its closely-related affiliates will be reviewed to determine the strength of the institution. These financial statements should demonstrate an ability to fulfill the contractual commitments proposed, and will be considered with regard to outstanding commitments, capital strength, liquidity and operating results. Undercapitalized companies or those exhibiting weak earnings may not be able to continue as ongoing concerns. This could lead to disruptions in member service, uncollected payments, and potential losses if the third party fails to remit funds due to the Credit Union. A licensed CPA will be consulted when necessary.
8. **CONTROLS.** Once the Credit Union has entered into a third-party arrangement, the Credit Union will employ controls to ensure that the relationship is meeting expectations and the third-party vendor is meeting its responsibilities.  
   1. **Limitation of Exposure.**Depending on the nature of the relationship, the Credit Union will establish limitations on the risk of exposure (i.e., the number of leases initially granted, etc.) until the third-party’s performance is measured, or the level of the respective risk(s) becomes significant.
   2. **Sensitivity Analysis.** Credit Union management will routinely conduct sensitivity analyses; project its expected revenue, expenses, and net income on its investment; and recognize how each of these factors may change under different economic conditions. This analysis will be conducted internally by someone with the requisite knowledge, or through the use of an outside consultant. Data and other benchmarks, including yield and profit projections generated by the third party will be verified with the underlying assumptions fully understood by the Credit Union, and compared with Credit Union’s own data. Services that are not directly income generating, such as infrastructure, will be subjected to a cost-benefit analysis.
   3. **Staff Oversight.** Management will designate the staff that is to be responsible for monitoring the performance of each outsourced program. Duties will include comparing the actual results of each program to projections, and reviewing each of the third party’s performance to determine compliance with expectations and contracts.
   4. **Reporting.** Staff responsible for third-party relationship monitoring will submit regular reports to the Credit Union’s senior officials and the Board. The reports will include appropriate information in order to provide the officials and the Board the opportunity to make informed decisions and take timely corrective action.
9. **Due Diligence Documents to be Collected for Each Risk Rating**
10. **High Risk**
11. Financials from the Previous Year – Acceptable documents include 10-K, Annual Report, Audited Financials, Balance Sheet, Profit & Loss Statement (P&L), Income Statement, Statement of Financial Condition, and Unaudited Financials.
12. Business Continuity/Disaster Recovery Plan - Acceptable documents include Business Continuity Plan, Disaster Recovery Plan, Incident Response Plan, and Pandemic Response Plan.
13. SSAE16/SSAE18/SOC Report – Acceptable documents include SOC 1 Type 1, SOC 1 Type 2, SOC 2 Type 1, SOC 2 Type 2, and SOC 3 Bridge Letters DO NOT fulfill the SOC requirements; they are merely a supplement to the Report itself.
14. Privacy Policy
15. Proof of Liability Insurance – Acceptable documents include a Certificate of Insurance (COI) or a Declaration page.
16. Business License/Certificate – Acceptable documents include a PDF or screencap of a Business Entity Summary (located on the business’s state Secretary of State website), a PDF or screencap of their Taxable Entity Search, a Certificate of Good Standing.
17. Fully Executed Agreement (and any corresponding Amendments and Addendums).
18. **Medium Risk**
19. Financials from the Previous Year- Acceptable documents include 10-K, Annual Report, Audited Financials, Balance Sheet, Profit & Loss Statement (P&L), Income Statement, Statement of Financial Condition, and Unaudited Financials.
20. SSAE16/SSAE18/SOC Report – Acceptable documents include SOC 1 Type 1, SOC 1 Type 2, SOC 2 Type 1, SOC 2 Type 2, and SOC 3.
21. Privacy Policy
22. Proof of Liability Insurance – Acceptable documents include a Certificate of Insurance (COI) or a Declaration page.
23. Business License/Certificate - Acceptable documents include a PDF or screencap of a Business Entity Summary (located on the business’s state Secretary of State website), a PDF or screencap of their Taxable Entity Search, a Certificate of Good Standing.
24. Fully Executed Agreement (and any corresponding Amendments and Addendums). Alternatively, if there is not a written agreement, acceptable documents include a Quote, SOW, an invoice, or a document that provides there is a relationship between the CU and the Third party vendor.
25. **Low Risk**
26. Proof of Liability Insurance - Acceptable documents include a Certificate of Insurance (COI) or a Declaration page.
27. Business License/Certificate - Acceptable documents include a PDF or screencap of a Business Entity Summary (located on the business’s state Secretary of State website), a PDF or screencap of their Taxable Entity Search, a Certificate of Good Standing.
28. Fully Executed Agreement (and any corresponding Amendments and Addendums). Alternatively, if there is not a written agreement, acceptable documents include a Quote, SOW, an invoice, or a document that provides there is a relationship between the CU and the Third party vendor.
29. **No Risk**
    * 1. No Documents are required at this Risk Level

**10. Frequency of Document Collection per Document (Working Title)**All of these documents will be requested from vendors on an *annual* basis:

1. **Financials**
   1. These are good for 17 months of the listed Fiscal Year. (e.g., if the fiscal year ends on December 31st, 2023, the document is considered the current version until May 31st, 2025).
2. **Business Continuity/Disaster Recovery Plan**
   1. If an updated version of this document is not provided by the vendor upon the annual request, the current version is still valid.
3. **SSAE16/SSAE18/SOC Report**
   1. These are good for 18 months following the last date in the report (e.g., if a SOC Report is covering a period between January 1st, 2024, to September 30th, 2024, that SOC Report is considered the current version until March 31st, 2026).
4. **Privacy Policy**
   1. If an updated version of this document is not provided by the vendor upon the annual request, the current version is still valid.
5. **Proof of Liability Insurance**
   1. These are only valid until the end date listed on the Certificate of Insurance. CU or 3rd Party Vendor Management Service will wait 2 weeks after the expiration date listed on the COI to request the document, to ensure that the vendor will provide the new version instead of the expired version.
6. **Business License/Certificate**
   1. If an updated version of this document is not provided by the vendor upon the annual request, the current version is still valid.

**11. Credit Union Reviews**

The Credit Union will review:

1. High/Critical Risk vendors every [\_\_\_] months
2. Medium/Moderate Risk vendors every [\_\_] months
3. Low Risk vendors every [\_\_] months
4. No Risk vendors every [\_\_] years

**12. Depth of Review Per Risk Level**

1. **High Risk – Factors to Consider**

*Strategic Risk* is the risk associated with the financial institution’s present or future business plans and strategies. This risk category includes plans for entering new business lines, expanding existing services through mergers and acquisitions, outsourcing and enhancing infrastructure. Strategic risk can impact earnings or capital arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes.

*Interest Rate and Liquidity Risk* is the risk associated with any vendor service that affects the credit union’s interest rate and or liquidity via funds transfer or investing on behalf of the Credit Union.

*Compliance Risk* is the risk associated with non-adherence to regulatory controls and or internal policies that directly affect Credit Union operations. Compliance risk can impact areas ranging from earnings to CU reputation. Compliance risk can arise from violations of, or non-conformance with laws, regulations, accepted standards, and/or ethical practices.

*Operational Risk* is the risk associated with loss resulting from inadequate or failed internal processes, people and systems provided by a specific vendor and the direct implication to the Credit Union. Operational risk factors consider the adequacy of the vendor’s standards, policies, procedures, hiring practices, facilities management, and Disaster Recovery and or Business Continuance.

*Reputation Risk* is the risk associated with negative publicity regarding an institution’s business practices which could lead to a loss of revenue or litigation. A Credit Union’s reputation, particularly the trust afforded it by its members can be irrevocably tarnished due to perceived or real breaches in its ability to conduct business securely and responsibly.

*Information Security Risk* is the risk associated with shared use of electronic systems, security, controls and information.

*Credit Union Action Plans:* The Credit Union must notate whether they intend to change vendors or if they will be renewing with the vendor and include their signature.

1. **Medium Risk – Factors to Consider**

*Interest Rate and Liquidity Risk* is the risk associated with any vendor service that affects the credit union’s interest rate and or liquidity via funds transfer or investing on behalf of the Credit Union.

*Compliance Risk* is the risk associated with non-adherence to regulatory controls and or internal policies that directly affect Credit Union operations. Compliance risk can impact areas ranging from earnings to CU reputation. Compliance risk can arise from violations of, or non-conformance with laws, regulations, accepted standards, and/or ethical practices.

*Operational Risk* is the risk associated with loss resulting from inadequate or failed internal processes, people and systems provided by a specific vendor and the direct implication to the Credit Union. Operational risk factors consider the adequacy of the vendor’s standards, policies, procedures, hiring practices, facilities management, and Disaster Recovery and or Business Continuance.

*Reputation Risk* is the risk associated with negative publicity regarding an institution’s business practices which could lead to a loss of revenue or litigation. A Credit Union’s reputation, particularly the trust afforded it by its members can be irrevocably tarnished due to perceived or real breaches in its ability to conduct business securely and responsibly.

*Information Security Risk* is the risk associated with shared use of electronic systems, security, controls and information.

*Credit Union Action Plans:* The Credit Union must notate whether they intend to change vendors or if they will be renewing with the vendor and include their signature.

1. **Low Risk – Factors to Consider**

*Compliance Risk* is the risk associated with non-adherence to regulatory controls and or internal policies that directly affect Credit Union operations. Compliance risk can impact areas ranging from earnings to CU reputation. Compliance risk can arise from violations of, or non-conformance with laws, regulations, accepted standards, and/or ethical practices.

*Operational Risk* is the risk associated with loss resulting from inadequate or failed internal processes, people and systems provided by a specific vendor and the direct implication to the Credit Union. Operational risk factors consider the adequacy of the vendor’s standards, policies, procedures, hiring practices, facilities management, and Disaster Recovery and or Business Continuance.

*Reputation Risk* is the risk associated with negative publicity regarding an institution’s business practices which could lead to a loss of revenue or litigation. A Credit Union’s reputation, particularly the trust afforded it by its members can be irrevocably tarnished due to perceived or real breaches in its ability to conduct business securely and responsibly.

*Credit Union Action Plans:* The Credit Union must notate whether they intend to change vendors or if they will be renewing with the vendor and include their signature.