



# FAMILY FIRST CREDIT UNION VENDOR MANAGEMENT POLICY



## Table of Contents

INTRODUCTION .....	4
PURPOSE .....	4
Specific Objectives.....	4
SCOPE .....	5
DEFINITIONS .....	6
Vendor .....	6
Contractor Agreement.....	6
Vendor Class .....	6
TDC Services Vendor Management.....	7
RESPONSIBILITY .....	7
Board Responsibility .....	7
Management Responsibility .....	7
POLICY .....	8
Pre-Contract Vendor Risk Assessment .....	9
Self-Assessment.....	10
Insurance Review.....	10
Review of Third Party Expertise and Past Performance .....	10
Legal Review .....	10
Financial Review .....	10
Controls .....	11
Limitation of Exposure.....	11
Sensitivity Analysis.....	11
Staff Oversight .....	11
Reporting .....	11
Contracts and Formal Agreements.....	11
Post-Contract Vendor Management .....	12
Vendor Classifications .....	13
Risk Re-assessment .....	14
Vendor List.....	14
Vendor Due Diligence .....	14
Contract Management .....	14
Contract Negotiation.....	15
Contract Language .....	16

## Family First Credit Union Vendor Management Policy

---

Contract Approval and Renewal .....	17
Contract Cancellation .....	17
Contract File Retention .....	17
Vendor Supervision.....	17
COMPLETING A PRE-CONTRACT VENDOR RISK ASSESSMENT .....	18
Completing a Due Diligence Analysis .....	19
REVISION HISTORY.....	<b>Error! Bookmark not defined.</b>
APPENDIX A: SAMPLE VENDOR LETTER.....	20
APPENDIX B: SAMPLE VENDOR QUESTIONNAIRE .....	21
APPENDIX C: SAMPLE CONFIDENTIALITY AGREEMENT .....	23
APPENDIX D: VENDOR RATING.....	25

## INTRODUCTION

In an effort to enhance the services provided to members, Family First Credit Union often partners with outside parties. We rely on these vendors to perform a range of services and provide products for Family First Credit Union and its 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. Vendor Due Diligence reviews are required prior to entering into any arrangement with a third party.

Some of the most important people we will ever work with at Family First 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.

## PURPOSE

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. In addition, this policy assists in maintaining appropriate and well-managed contractual relationships with a wide variety of external vendors who are critical to Family First Credit Union's success

### Specific Objectives

- ❖ Ensure that outsourced relationships are initiated based on a sound business case and comprehensive due diligence in the selection process
- ❖ Ensure that outsourced relationships are effectively managed by providing consistent, risk-focused controls and processes
- ❖ Ensure that Family First Credit Union is in compliance with regulatory guidance and requirements pertaining to outsourced relationships.

Family First Credit Union will achieve these objectives by maintaining an active vendor management oversight function. Specific practices and procedures will ensure that vendor performance is monitored, contractual requirements are in place, and regulatory requirements are met.

## SCOPE

This policy covers all of Family First Credit Union relationships with third party service providers and vendors that meet one or more of the following criteria:

- ❖ Provides outsourced technology services (e.g., data processing, web site hosting, application development and support)
- ❖ Provides outsourced operational support (e.g., credit card processing, debit/ATM card processing, etc.)
- ❖ Provides outsourced facilities support (e.g. maintenance, cleaning, etc.)
- ❖ Provides outsourced professional services (e.g., legal, advisory, consulting, accounting, etc.)

For administration of this policy, outsourced relationships that meet any of the following criteria may be considered an exception to this program:

- ❖ Non-critical services or items of a non-recurring and incidental nature (e.g., short-term maintenance service, lawn service, office supplies)
- ❖ Emergency purchases, as approved by an executive officer
- ❖ Routine expenses (e.g., utilities, travel expenses, memberships and dues, etc.)
- ❖ Payments to Government Agencies
- ❖ Other exceptions as determined by the Board of Directors

This policy applies to all Family First Credit Union business entities including individuals, departments, or subsidiaries who engage vendors defined in this document.

## 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 Family First Credit Union and also meets any of the following criteria:

- ❖ Performs services at Family First Credit Union facilities

#### Safety, insurance, or data security risk

Examples: Consultants who perform work onsite, auditors, equipment repair companies, gardeners, and deliveries past the key pad access doors. Deliveries to the lobby 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 Family First Credit Union

#### Financial or member service risk

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

### Contractor Agreement

A legal document, between Family First Credit Union and a vendor, in which the vendor agrees to provide services or products and, for which, the credit union agrees to render payment.

### Vendor Class

A Class assigned as a result of the “Vendor Risk Assessment” that indicates the relative risk this vendor represents to Family First Credit Union.

## TDC Services Vendor Management

The Family First Credit Union TDC Services vendor management site is in place for tracking and maintaining all vendor information. The service and site include:

- ❖ Existing contracts are input into the Vendor Management System by TDC Services. In the event a contract cannot be located, TDC Services contacts the vendor on Family First Credit Union's behalf to obtain the copy
- ❖ Confidentiality agreements, vendor questionnaires, and written references for each vendor are obtained and maintained, if applicable
- ❖ TDC Services obtains the annual SSAE16s, where applicable
- ❖ TDC Services manages each vendor's documentation in compliance with the vendor oversight requirements issued by Federal entities.
- ❖ Family First Credit Union forwards new contracts to TDC Services for input into the system or Family First Credit Union inputs the contract themselves
- ❖ All information is accessible via a secure site for reviewing terms, expiration dates, class assignment, all documentation and various vendor reports
- ❖ Automated alerts/notifications regarding vendor contracts are automatically generated at 1 year, 6 months, and 90 days prior to contract expiration to ensure there are no missed auto-renewal or expiration dates

## RESPONSIBILITY

### Board Responsibility

The Board of Directors are responsible for understanding the risks associated with outsourcing with third-party vendors and insuring that effective risk management practices are in place. The Board of Directors shall approve this Third Party Due Diligence Policy and any recommended changes.

### Management Responsibility

Family First Credit Union Management is also responsible for understanding the risks associated with outsourcing with third-party vendors and insuring that effective risk management practices are in place. Management is responsible for the development, implementation, and maintenance of Family First Credit Union's due diligence program.

As part of this responsibility, Management maintains a list of all third-party providers, along with the scope of services provided by each using the TDC Services Vendor Management site. Management may delegate due diligence to appropriate staff as warranted, but shall be responsible for reviewing the information gathered and making the final decisions. Management will provide the Board of Directors with an annual review of third-party providers and the scope of services they provide.

Management is responsible for implementing, maintaining, and enforcing this policy as well as the following:

- ❖ 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 report
- ❖ Maintaining Vendor files
- ❖ Effectively acting as Vendor liaison.

## POLICY

It is the policy of Family First 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:

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



## Pre-Contract Vendor Risk Assessment

As part of the due diligence process, the decision to outsource a material service or function is to be ultimately determined and/or approved by the Management or the Board of Directors. The decision is based upon the recommendations of Management and the Vendor Due Diligence Report. The recommendation to engage with a third party must include a written business case analysis that outlines the nature of the service or function and the rationale for an outsourced (versus internally supported) service. At a minimum, the written business case must address the following issues:

- ❖ The nature of services provided (e.g., bill payment, funds transfer or other electronic services) that might result in the vendor performing services that can increase the levels of credit, liquidity, transaction, reputation risk, threats to security, availability and integrity of systems, facilities and resources, confidentiality of information, reputation, and regulatory compliance
- ❖ Summary of the business case (justification for the service)
- ❖ Overview of the vendors considered
- ❖ Overview of the basic requirements for the service/function
- ❖ Estimated costs and pro-forma projections
- ❖ Estimated implementation timeframe
- ❖ Summary of the recommendation for the potential service provider
- ❖ Expectations of third party relationship (what needs will be met by the third-party? What are the desired results?)
- ❖ Staff expertise (Is Family First Credit Union qualified to manage and monitor the third-party relationship?)
- ❖ Criticality of the activity to be outsourced (How important is the outsourced activity? Do other alternatives exist?)
- ❖ Cost/benefit analysis (Does the potential benefit of the relationship out-weigh the potential risks or costs? Will this change over time?)
- ❖ Impact on membership (How will this relationship affect our members and their expectations?)
- ❖ Exit strategy (Is there a reasonable means to exit the relationship if it becomes necessary to change course in the future?)

Family First Credit Union evaluates the costs (e.g., staffing, capital expenditures, communications, and technological investment) of monitoring and providing support to the third-party program. Family First Credit Union also performs and documents a cost-benefit analysis to determine if it is receiving sufficient reward for the risk associated with any potential relationship.

Categories of risk to be assessed also include loss of capital if the venture fails, loss of member confidence if the program, product or service fails to meet member expectations, and costs associated with attracting or training personnel and investing in required infrastructure.

### Self-Assessment

Management determines whether the proposed activities, related costs, product and services standards, and third-party involvement, are consistent with Family First Credit Union's overall business strategy and risk tolerances.

### Insurance Review

Third party relationships can result in increased liabilities. Therefore, this financial institution maintains an adequate review of Family First 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, Family First Credit Union ensures that it is the beneficiary on all insurance policies and reviews all insurance contracts to ensure full coverage.

### Review of Third Party Expertise and Past Performance

The amount of due diligence performed is relative to the magnitude and impact of the product and the reputation of the third party. An unfamiliar third party that offers a new and unfamiliar product or service requires the most due diligence.

Family First Credit Union researches and/or interviews several prospective organizations to determine which is best qualified to meet credit union needs. It is also important to understand how the third party has performed in other relationships. Management contacts other financial institutions or clients of the third party. Other sources for information, such as the Better Business Bureau, Federal Trade Commission, credit reporting agencies, state member affairs offices, state attorney general offices, and state and federal courts, are consulted to determine complaint histories on businesses.

### Legal Review

When appropriate based on the service and/or risk, all contracts may be reviewed by Family First Credit Union's legal counsel to ensure the credit union has a clear understanding of the rights and responsibilities of both parties; the term of the agreement and its termination provisions, along with any consequences associated with early termination; and what actions Family First Credit Union may take if the contract is breached, or the services are not performed. The credit union will exercise its right to modify contracts if necessary.

### Financial Review

Financial statements of the third party are reviewed to determine the strength of the institution. In evaluating the overall financial health of the third party, Family First Credit Union may also use other available sources (e. g., Nationally Recognized Statistical Rating Organizations, SSAFE16 reports, etc.).

### Controls

Once Family First 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 is meeting its responsibilities.

### Limitation of Exposure

Depending on the nature of the relationship, Family First 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.

### Sensitivity Analysis

Management routinely conducts sensitivity analysis, projects its expected revenue, expenses, and net income on its investment, and recognizes 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 Family First Credit Union, and compared with our own data. Services that are not directly income generating, such as infrastructure, will be subjected to a cost-benefit analysis.

### Staff Oversight

Management designates 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.

### Reporting

Reports are submitted to Family First Credit Union's Management and the Board of Directors to keep them abreast of significant findings, especially areas of non-compliance. Management and/or the Board are notified when targets are met or exceeded as well as when they are not. In any case, the reports will consist of appropriate information so that Management and/or the Board can make informed decisions and take timely corrective action.

### Contracts and Formal Agreements

Once a service provider has been selected and approved, contract negotiations may commence. Generally, negotiations are led by Management. Depending on the risk rating assigned to the proposed relationship and recommended provisions to address controls, service levels, etc., the contract is drafted. If the service provider requires a "standard contract," such is reviewed to ensure that it addresses the needs and requirements for Family First Credit Union.

Management will review all contracts for "critical" vendors. Specific attention is given to provisions for privacy and security over member information. Dependent on the financial significance, criticality of service, and complexity of the contract, it may also be submitted to legal counsel for review.

Once contracts have been reviewed for Family First Credit Union's requirements and any legal concerns, they are submitted for appropriate signature. Contracts, maintenance agreements, service agreements, and purchase contracts with third party vendors must be approved by Management. All original contracts will be centrally filed.

## Post-Contract Vendor Management

An initial risk analysis is conducted for each potential vendor. At a minimum, the risk analysis utilizes the Vendor Classifications Matrix to assign a vendor class of 1, 2, 3, and 4. A vendor is assigned a class based on the highest risk level attributable to the contract, or sum of all contracts, with that vendor. Exceptions to the assigned class may be granted by Management as needed and appropriate.

The Class is an indicator of the level of due diligence Family First Credit Union requires for each vendor.

- ❖ Class 1 (High Risk) require annual due diligence review
- ❖ Class 2 (Medium Risk) require annual due diligence review
- ❖ Class 3 (Low Risk) vendors typically require little analysis and due diligence.
- ❖ Class 4 (Low or No Risk) vendors typically require no analysis or due diligence.

## Vendor Classifications

Class	Type	Reason	Docs Required
1	Critical	<ul style="list-style-type: none"> <li>The services or function performed by the third party involve high levels of strategic operational, credit and reputation risk to the credit union.</li> <li>The services will be provided for an extended period of time.</li> <li>The vendor has access to a significant amount of highly sensitive nonpublic information (NPPI).</li> <li>There is no immediate replacement or backup for the service.</li> <li>The vendor provides customer service or interacts directly with current or prospective customers.</li> <li>The vendor collects and remits payments on behalf of the credit union.</li> <li>The activities conducted by the vendor account for a significant level of income for the credit union.</li> </ul>	Confidentiality Agreement Insurance Verification Financial Statement Financial Condition System Schematic SSAE 16
2	Material	<ul style="list-style-type: none"> <li>The vendor has access to highly sensitive levels of confidential customer information or has low volume of the information or the vendor is subject to the Information Safeguarding Guidelines under section 501(b) of the GLBA.</li> </ul>	Confidentiality Agreement Financial Statement Insurance Verification System Schematic
3	Minor	<ul style="list-style-type: none"> <li>Services of function performed by the vendor involve low levels of strategic, operational, credit, compliance and reputation risk to the credit union.</li> <li>Acceptable alternative services are readily available that ensure the continuity of the credit union's operations.</li> <li>Minor vendors have no access to, or possession of, nonpublic personal information (NPPI).</li> </ul>	Confidentiality Agreement Insurance Verification
4	No Due Diligence	<ul style="list-style-type: none"> <li>No Risk</li> </ul>	None

### Risk Re-assessment

Risk assessments are revisited as part of contract renewal or anytime the relationship with the vendor changes in any significant way. Through TDC Services Vendor Management, each vendor is reassessed no less than annually and updated documents, if applicable are acquired either annually or semi-annually dependent upon the assigned vendor class.

### Vendor List

Through TDC Services Vendor Management, a complete vendor list is retained, including low risk vendors, with the class noted for each vendor. This list is available 24/7 via the Family First Credit Union TDC Services vendor management site. Reporting is available via the site for the Compliance Management to include in the annual report to the Supervisory Committee.

### 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 depends on the results of the initial Vendor Risk Assessment and resulting class assigned. Due diligence for a low risk vendor may be nominal, while high risk vendors require more thorough due diligence. All due diligence records performed in establishing the vendor relationship, including the class, are maintained on the vendor management site.

### 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 Family First 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.

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

- ❖ Contract Negotiation
- ❖ Contract Language
- ❖ Contract Approval and Renewal
- ❖ Contract Cancellation
- ❖ Retaining Contract Files

## Contract Negotiation

Vendor negotiations are only delegated 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 are 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
- ❖ Information Systems. Required for all contract negotiations related to software, hardware, and Information Systems
- ❖ Management
- ❖ Board of Directors

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:

Perspective	Consideration
Legal	Are Family First Credit Union's interests adequately protected if a problem arises with this vendor?
Financial	Does the agreement reasonably assure that Family First Credit Union's investment in this relationship will deliver the desired benefits without exposing the credit union to unacceptable financial risks?
Operational	Are the terms of the agreement operationally feasible for Family First Credit Union? <ul style="list-style-type: none"><li>❖ Timing considerations</li><li>❖ Service Levels</li><li>❖ Family First Credit Union performance commitments</li><li>❖ Technology compatibility</li><li>❖ Human Safety</li></ul>
Risk Management	Are the terms of the agreement acceptable in light of regulatory, financial, operational, and reputation risks?

2. Maintain multiple vendor candidates for as long as possible to enter the negotiation stage with important leverage. The possibility that Family First Credit Union could select an alternate vendor may prove invaluable to obtaining the vendor's agreement to important contract provisions.
3. Document negotiations and contact between a potential vendor and Family First Credit Union.
4. Retain the negotiation records with the contract record for the life of the contract.

### Contract Language

Contract language should be reviewed to ensure that the agreement or contract meets regulatory requirements and does not expose Family First Credit Union to unnecessary risk.

1. Verify that the language in the agreement or contract meets regulatory requirements and does not expose Family First 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 and 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 and Indemnity
  - ◆ Warranties
  - ◆ Standard Family First Credit Union dispute resolution provisions
  - ◆ Choice of law and 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



### Contract Approval and Renewal

Management is responsible for the contracts executed by their staff. Medium and High-Risk vendor contracts, including renewals, are to be executed by Management.

1. Execute the contract with the appropriate level of Management and/or Board of Directors approval
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. Complete the Vendor Re-Assessment Questionnaire
  - d. Review contract terms

### 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.

### Contract File Retention

Vendor contract files are stored for five years after contract expiration.

### Vendor Supervision

Each vendor is assigned a Vendor Relationship Manager who completes the act as vendor liaison. Management will provide an annual status report of Medium and High-risk vendors to the Supervisory Committee.

The Vendor Relationship Manager completes the following:

1. Review the vendor class assigned by TDC Services
2. Reviews vendor due diligence analysis, as appropriate for the risk rating
3. Reviews periodic due diligence review (at least annually for high-risk vendors)
4. Coordinates and documents ongoing vendor communication
5. Reviews vendor files
6. Reviews 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
9. Coordinates contract cancellation

## COMPLETING A PRE-CONTRACT VENDOR RISK ASSESSMENT

1. Assign a vendor class using the vendor classification matrix
2. Review the substantive risk exposure to Family First Credit Union if the product or service fails or is inadequately performed.

Regulatory	Can the vendor create regulatory risk for Family First Credit Union?
Reputation	Can the vendor impact Family First Credit Union's reputation?
Financial	Can the vendor impact Family First Credit Union or its members financially?  Does Family First Credit Union or the vendor have insurance that will allow the credit union to transfer some of the risk?
Member or other Sensitive Data Access	To what extent will the vendor handle sensitive Family First Credit Union data?
Operational Effectiveness  Process Risk  People Risk  System Risk	How would the vendor's failure impact Family First Credit Union's business needs and strategic objectives?  Could Family First Credit Union step in and perform the critical functions provided by the vendor if the vendor failed to perform?  Are there other potential vendors that could readily assume service should the current provider fail?  Can Family First Credit Union provide adequate oversight of the vendor's function?  Can the vendor create risk to Family First Credit Union's processes, people, or systems?  Would Family First Credit Union be considered the "Controlling Employer" for this vendor?  Would Family First Credit Union be placed in a position of "Joint Employer's Liability" for this vendor?  Note: 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 Family First Credit Union.

### Completing a Due Diligence Analysis

Review the following, as appropriate, based upon the vendor class and the type of risk exposure created by this vendor relationship:

- ❖ SSAE16s 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 (as appropriate)

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

## APPENDIX A: SAMPLE VENDOR LETTER

[inquiries@tdcservices.org](mailto:inquiries@tdcservices.org)  
phone 864.476.2258 Fax 888.535.1910  
PO Box 365  
Woodruff, SC 29388-0365



**RE: VENDOR DUE DILIGENCE**

Dear

As part of federal requirements for due diligence, \_\_\_\_\_ is required to obtain the items requested below, as applicable, from each of their vendors. Failure to provide the information could result in the client not meeting compliance requirements which could result in unsatisfactory audits. Therefore, on behalf of \_\_\_\_\_, we need the following to be returned to us within 30 days of receipt of this request.

1. Completed Questionnaire (*enclosed*)
2. Signed Confidentiality Agreement (*enclosed*)
3. Copy of the original Contract/Agreement
4. Copy of the most recent Contract/Agreement
5. Copy of your most recent Financial Statement (*if available*)
6. Copy of your most recent Financial Condition Review (*if available*)
7. Copy of your Insurance Coverage/Verification
8. Copy of your most recent Reference List
9. Copy of your System Schematic
10. Copy of your most recent SSAE16 (*if applicable*)
11. Copy of any other Regulatory Examination Reports (*if applicable*)


When completing the enclosed questionnaire, please answer all that apply to your organization and answer N/A to all that does not. We appreciate your cooperation in keeping our mutual client's vendor information current.

Thank you,  
TDC Services

Enclosures: Questionnaire  
Confidentiality Agreement(s)

## APPENDIX B: SAMPLE VENDOR QUESTIONNAIRE

[inquiries@tdcservices.org](mailto:inquiries@tdcservices.org)  
 phone 864.476.2258 Fax 888.535.1910  
 PO Box 365  
 Woodruff, SC 29388-0365



TDC Services Vendor Questionnaire for \_\_\_\_\_

Audits/Regulations (if applicable)	
1. Have you ever completed a SAS70/SSAE16 audit?	
2. Have you ever completed a SAS70 Type II audit?	
3. Have you ever completed an ISO 17799 audit?	
4. Have you ever completed a Systrust audit?	
5. Have you ever completed a CUISPA audit?	
6. What is the frequency for which you schedule these audits?	
7. What was the date of your last audit?	
Business Continuity	
8. Do you have a Business Continuity/Disaster Recovery Plan?	
9. If yes, how often is this plan tested?	
10. If yes, what was the date of the last test?	
11. Will any of our information be stored outside of a secured area?	
12. If you will store applicable Client data (or records) in any form, do you have policies for disposal of such data/records that are compliant with applicable legal and regulatory requirements?	
13. What are the qualifications of your staff that are responsible for your overall security?	
14. Do you outsource any of your processing?	
15. If yes, please describe.	
16. Does your contract include a privacy clause?	
17. Do you provide references?	
18. Are you bonded?	

[inquiries@tdcservices.org](mailto:inquiries@tdcservices.org)  
phone 864.476.2258 Fax 888.535.1910

PO Box 365  
Woodruff, SC 29388-0365



TDC Services Vendor Questionnaire for \_\_\_\_\_

### System Security

31. Describe the physical controls you have in place to secure your building and data center.	
32. Are industry-standard firewalls deployed?	
33. Do you keep the software for the firewalls current?	
34. Do you use an intrusion prevention system?	
35. Are you continually monitored for intrusion detection?	

### Third Parties

36. What is your due diligence process for contracting with third parties?	
37. Do you require your vendors to conduct pre-employment background checks on their employees?	

### General

38. What is your company registered name?	
39. What is the name of your parent company?	
40. Where is your company located?	
41. How long has your company been in business?	
42. How many employees does your company have?	
43. How long has your product/solution been in use?	
44. How many clients do you have?	
45. What is your standard or required contract term?	

Name: \_\_\_\_\_ Street: \_\_\_\_\_  
Title: \_\_\_\_\_ City: \_\_\_\_\_  
Email: \_\_\_\_\_ State: \_\_\_\_\_  
Phone: \_\_\_\_\_ Zip: \_\_\_\_\_  
Fax: \_\_\_\_\_ Website: \_\_\_\_\_

## APPENDIX C: SAMPLE CONFIDENTIALITY AGREEMENT

[inquiries@tdcservices.org](mailto:inquiries@tdcservices.org)  
phone 864.476.2258 Fax 888.535.1910  
PO Box 365  
Woodruff, SC 29388-0365



---

### CONFIDENTIALITY AGREEMENT

The nature of the business between \_\_\_\_\_ and \_\_\_\_\_ necessitates that a limited amount of non-public personal information be disclosed concerning our consumers and their relationship with \_\_\_\_\_. Legally and philosophically \_\_\_\_\_ is committed to the protection and confidentiality of the personal and financial information our consumers entrust with us.

\_\_\_\_\_ agrees to maintain the confidentiality of the information we receive from \_\_\_\_\_. We understand that this information is given to us as a requirement of our joint business effort. This information will be used only for the business purpose for which it is intended. We agree that we will not disclose this confidential information to any third party except as it is necessary in the performance of our obligations or duties under this agreement.

We confirm that all “personally identifiable financial information” will be maintained in a safe and secure manner pursuant to the requirements of applicable laws. In addition, \_\_\_\_\_ shall only dispose of the information in a safe and secure fashion that meets or exceeds the requirements of applicable laws, rules and regulations.

- a. **Confidential Information and Exclusions.** “Confidential Information” means any information disclosed by one Party (the “Disclosing Party”) to the other (the “Receiving Party”), which, if in tangible form is marked as “Confidential” or “Proprietary,” or which, if disclosed orally or by demonstration, is identified at the time of initial disclosure as confidential in a writing within thirty (30) days of such disclosure or which is otherwise deemed confidential. Confidential Information shall exclude information that the Receiving Party can demonstrate: (i) was independently developed by the Receiving Party without any use of the Disclosing Party’s Confidential Information or by the Receiving Party’s employees or agents who have not been exposed to the Disclosing Party’s Confidential Information; (ii) becomes known to the Receiving Party, without restriction, from a source other than the Disclosing Party and that had a right to disclose it; (iii) was or becomes in the public domain through no act or omission of the Receiving Party; or (iv) was rightfully known to the Receiving Party, without restriction, at the time of disclosure. Without limiting the foregoing, if a Receiving Party believes that it is or will be compelled by a court or other authority to disclose Confidential Information of the Disclosing Party, it shall give the Disclosing Party prompt notice so that the Disclosing Party may take steps to oppose such disclosure.

[inquiries@tdcservices.org](mailto:inquiries@tdcservices.org)  
phone 864.476.2258 Fax 888.535.1910  
PO Box 365  
Woodruff, SC 29388-0365



- b. Confidentiality Obligation. The Receiving Party shall treat as confidential all of the Disclosing Party's Confidential Information and shall not use such Confidential Information except as expressly permitted under this Agreement. The Receiving Party shall use at least the same degree of care that is uses to prevent the disclosure of its own confidential information, but in no event with less than reasonable care, to prevent the disclosure of the Disclosing Party's Confidential Information.
- c. Remedies. In the event of an actual or threatened breach or violation or infringement of a party's intellectual property rights, the non-breaching party shall, in addition to other available legal or equitable remedies, be entitled to seek an injunction against such breach without the necessity of posting bond.

Because of our commitment to the privacy of our member's information, we require that your company sign this confidentiality agreement.

This agreement shall survive the termination of any business arrangement between \_\_\_\_\_ and \_\_\_\_\_.

\_\_\_\_\_  
SIGNATURE

\_\_\_\_\_  
PRINTED NAME

\_\_\_\_\_  
TITLE

\_\_\_\_\_  
DATE



## APPENDIX D: VENDOR RATING

### Vendor Rating

Consideration	Response	Class 1	Class 2	Class 3
Are you Bonded?	Y	2	4	7
Do you conduct pre-employment background criminal checks on your employees?	Y	4	5	10
Does your contract include a privacy clause?	Y	5	5	5
Do you provide references?	Y	2	3	10
Are you a foreign subsidiary of U.S. Companies or foreign companies?	N	1	1	1
Do you outsource any of your processing?	N	4	5	5
Do you have a formal due diligence process for contracting with third parties?	Y	4	5	7
Are any of your third parties foreign subsidiaries of U.S. Companies or foreign companies?	N	1	3	1
Do you require your vendors to conduct pre-employment background checks on their employees?	Y	2	5	7
Have you ever completed an audit?	Y	10	10	10
Do you have a "need to know" policy that restricts access to resources and information?	Y	3	3	3
If you will store applicable consumer data in any form, do you have policies for disposal of such data?	Y	4	4	0
Do you require appropriate qualifications for the staff that is responsible for your overall security?	Y	1	3	0
Do you have an Information Security Officer?	Y	3	3	0
Does the Information Security Officer's Credentials meet industry standards?	Y	2	1	0
Will any of our information be stored outside of a secured area?	N	3	3	3
Do you have standard physical controls in place to secure your building and data center?	Y	5	5	5
Do you have your system tested for penetration?	Y	6	3	0
Do you perform a penetration test annually?	Y	1	1	1
Are you continually monitored for intrusion detection?	Y	5	3	0
Do you use an intrusion prevention system?	Y	5	4	0
Are industry-standard firewalls deployed?	Y	5	3	1
Do you keep the software for the firewall current?	Y	5	3	0
Are formal incident-response procedures in place?	Y	5	4	10
Are they tested regularly?	Y	3	2	4
Do you have a Business Continuity/Disaster Recovery plan?	Y	5	5	5
Is the plan tested annually?	Y	1	1	2
Financial Analysis Score	score	3	3	3
<b>Total</b>	<b>0</b>	<b>100</b>	<b>100</b>	<b>100</b>