

WRITTEN INFORMATION SECURITY PROGRAM (WISP)

VENDOR MANAGEMENT PROGRAM

<<Legal Entity>> (TEMPLATE – Smaller Entity)

Responsible Office: <<TBD>>

Effective Date: << INSERT DATE >>

REVISION HISTORY

Date of Change	Responsible	Summary of Change
September 2018	TTG SAS	TTG template revision v4

I. OBJECTIVE:

To vendor due diligence policy governs an on-going process whereby vendors are evaluated on a periodic basis. Vendor evaluations take place at the time of initial contractual engagement and periodically thereafter based on the type of relationship.

Any vendor or third-party service provider the Company enters into contractual obligations with must pass through an initial risk assessment and contract review process prior to execution of the contract. This assessment process is intended to ensure the proper structure of each business relationship, and to identify those vendors that need to be tracked for regulatory (GLBA) purposes.

II. APPLICABILITY

This vendor due diligence policy applies to all the Company customers, employees and individuals associated with the Company, whether full-time or part-time, paid or unpaid, temporary or permanent, as well as all agents and representatives of the Company, including any Third Party Provider providing services to the Company, who create, use or otherwise access or interact with any Company Information or Company Information Resource.

This Program applies to all Company sensitive, non-public Information, including all information collected, stored or used by or on behalf of any operational unit, department and person in connection with Company operations. In the event that any particular sensitive, non-public information is governed by more specific requirements under other Company policies or procedures, the more specific requirements shall take precedence over this Program to the extent there is any conflict.

WRITTEN INFORMATION SECURITY PROGRAM (WISP)

VENDOR MANAGEMENT PROGRAM

<<Legal Entity>> (TEMPLATE – Smaller Entity)

Responsible Office: <<TBD>>

Effective Date: << INSERT DATE >>

III. VENDOR DUE DILIGENCE POLICY

A “third-party relationship” is broadly defined to include all entities that have entered into a business relationship with the Company, whether the third-party is affiliated or not affiliated, regulated or non-regulated, or domestic or foreign.

A. DUE DILIGENCE REVIEW

Company management is responsible for planning, directing, and controlling business affairs. To fulfill these duties, the officials should require a due diligence review prior to entering into any arrangement with a third party. The following identifies minimum procedures the Company should follow. However, information gathered from the review may lead to further inquiries or fact-finding.

B. PLANNING

The officials should determine whether the proposed activities are consistent with the Company's overall business strategy and risk tolerances. These risks include the potential loss of capital invested if the venture fails, the loss of member confidence if the program does not meet their expectations, and the costs associated with attracting and retaining qualified personnel and investing in the required infrastructure (e.g., technology, space, communications). If the officials do not believe the activities would complement their strategic vision for the Company, the third-party lending relationship should not be pursued.

C. BACKGROUND CHECK

It always is important to understand how the third-party has performed in other relationships. Contacting companies or other clients of the third-party is essential. Inquire how satisfied these companies or third parties are with the prospective partner, and what pitfalls they may have encountered. Sources such as the Better Business Bureau, and Federal Trade Commission also maintain complaint histories on businesses.

D. LEGAL REVIEW

The Company's attorneys should review all contracts to ensure that the officials clearly understand the rights and responsibilities of each party. For example, the review should indicate which party bears the costs of collateral disposition, and whether or not there are recourse arrangements. The Company should exercise its right to modify contracts to make them fair and equitable. Further, a Company should understand what actions it may take if the contract is breached or services are not performed as expected.

WRITTEN INFORMATION SECURITY PROGRAM (WISP)

VENDOR MANAGEMENT PROGRAM

<<Legal Entity>> (TEMPLATE – Smaller Entity)

Responsible Office: <<TBD>>

Effective Date: << INSERT DATE >>

E. FINANCIAL REVIEW

Financial statements of the company should be reviewed to determine the strength of the institution. Weakly capitalized 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 on loans and leases, and potential losses if the third party fails to remit funds due to the Company. Preferably, a licensed CPA will have audited the financial statements to attest to their accuracy.

F. RETURN ON INVESTMENT

The Company should project its expected revenue, expenses, and net income on its investment, and recognize how each of these factors may change under different economic conditions. For example, expected losses, collection costs, or the volume of activity would fluctuate depending upon the economy or the members' employment stability. Profit projections generated by the prospective third-party should be scrutinized and the underlying assumptions fully understood by the Company.

G. INSURANCE REQUIREMENTS

Third party relationships can result in increased liabilities. Therefore they necessitate a thorough review of the Company's insurance coverage, including the fidelity bond and policies covering such matters as errors and omissions, property and casualty losses, and fraud and dishonesty.

H. CONTROLS

Once a third-party arrangement is entered into, it is important for a Company to establish controls (e.g. Service Level Agreements) to ensure the relationship is meeting its expectations and the third-party is meeting its responsibilities. As part of these controls, a Company should adopt monitoring and reporting practices that are completed annually, at minimum. Failing to do so constitutes an unsafe and unsound practice.

I. POLICIES AND PROCEDURES

The Company should develop detailed policy guidance that sets forth responsibilities, authorities, and reporting requirements. Limits should be established so that the program grows at a controlled pace and reflects the risk tolerance of the officials. For example, a Company may limit the number of leases initially granted so it can assess performance or identify problems before the leasing volume becomes significant.

WRITTEN INFORMATION SECURITY PROGRAM (WISP)

VENDOR MANAGEMENT PROGRAM

<<Legal Entity>> (TEMPLATE – Smaller Entity)

Responsible Office: <<TBD>>

Effective Date: << INSERT DATE >>

J. STAFF OVERSIGHT

A Company staff member should be responsible for monitoring the performance of the program. Actual results should be compared to projections and the third-party's performance should be reviewed to determine compliance with expectations and contracts.

K. REPORTING

Reports should be submitted to the Company's senior management to keep them abreast of significant findings, especially areas of noncompliance. The officials should be informed when targets are met or exceeded, or limits breached. Reports should also consist of appropriate information so that the officials can make informed decisions and take timely corrective action.

L. SOC REQUESTS

A vital piece of that program is understanding the risks posed by vendors. To understand these risks, Service Organization Controls (SOC) reports are a key component in the process. On an annual basis, an organization should request a SOC report from each of its vendors that house any of the organization's sensitive or proprietary data. These reports should be reviewed in detail to ensure the vendor is taking the necessary precautions in protecting the organization's data. Pay special attention to the 'User Control Considerations' section that the vendor has outlined, as this maps them back to your own policies and procedures to ensure that you have controls in place that properly align with your vendor's expectations.