Lawdesk

Vendor Management Policy

REVISION CONTROL

Version Number	Change Description	Author	Date
1.0	Created Policy	Allan Shutt	09/03/2017

TABLE OF CONTENTS

Vendor Management Policy

1.0 INTRODUCTION

The provisions of the Vendor Management Policy are in scope with adherence to the *Gramm Leach Bliley Act* ("GLBA") regulation section (b) protecting personal information and the *Credit Card Associations Payment Card Industry Data Security Standards* ("PCI DSS") as directed in sections 12.8.2 through 12.8.4, and OCC Bulletin 2013-29.

Any vendor that processes or stores Company account information and social security number must adhere to all GLBA requirements and PCI DSS standards.

Given the specialized expertise or proprietary processes within the lending industry needed to design, implement, and service new technologies and products, vendors may provide a valuable means to acquire expertise and resources that Company cannot, or chooses not to, provide on its own. In planning whether and how to contract for these needs, Company will assess how it will manage the risks associated with these new relationships.

Company management shall establish written procedures that contain adequate controls to limit the risks associated with the use of vendors to perform critical operational functions. Vendors may be used to support new Company technologies, systems, and products. While a bank or company can outsource many functions, management remains responsible for the performance and actions of its vendors while the vendors are performing the work.

Managers are required to handle requests to do business with vendors, through a vendor management review process. The process assigns a risk level based on the amount of risk presented to Company by employing the vendor's services. All vendor contracts are reviewed for compliance with the regulatory requirements outlined in OCC Bulletin 2013-29; this bulletin rescinds OCC Bulletin 2001-47 and OCC Advisory Letter 2000-9.

It is management's responsibility to review and approve all vendor activities and performance and to know their competencies. If a vendor cannot meet contractual commitments, Company must be able to exercise a contingency plan and secure those services elsewhere. The risks associated with non-compliance, credit risk, operational risk, reputation risk, compliance risk, and strategic risk – will be borne by Company, not the vendor.

2.1 MANAGEMENT WHITE PAPER PLANNING

Outsourcing can be used to accomplish a great number of services needed by Company. The types of services can vary in complexity and risk to the institution.

Management shall maintain processes to determine the level of risk a particular service may have on Company and prescribe a required amount of analysis prior to engagement. Whether it's outsourcing high risk or critical processes, upgrading existing systems or creating a new system internally, management will undertake a pragmatic planning process that will assess risk and performance gains within the context of Company's overall strategic goals and existing competencies. An assessment document should be included in the vendor management approval file. This document should be maintained within the executive contract file and may include:

- A cost/benefit analysis;
- An overview of the vendors operation including a critique of the proposed process;
- A written overview outlining the vendor operations to identify and determine the specific risk exposure to Company as well as the adequacy of the vendors internal controls to ensure limitation of that risk;
- The ability to initiate a COB ("Continuity of Business") plan to resume operations swiftly and with data intact in the event of vendor system failure or inability to process;
- Service Level Agreements designed to monitor vendor performance;
- A review and evaluation of vendor information systems and MIS necessary to monitor adherence to the established objectives and properly supervise the relationship;
- A review and evaluation of their security controls in place necessary to protect the sensitive information of Company and adhere to GLBA regulations and PCI DSS compliancy; and
- A comparative analysis of similar vendors and or products to ensure competitive product and pricing.

Contracts and/or agreements should ensure that the expectations and obligations of each party are clearly defined, understood and otherwise enforceable.

It is the policy of Company to comply with all regulations for any transactions and dealings with outside vendors. Company's Executive Management shall ensure that vendors serve the Company's best interests and perform the services in a safe and sound manner.

3.1 CONTRACTS AND AGREEMENTS

Contracts and agreements with vendors must:

- Be in writing
- Be fair and equitable to Company

- Be in compliance with regulation and policy standards governing vendor relationships
- Be approved by Legal Counsel; and
- Be approved by Executive Management.

Contracts will be reviewed by management and the Chief legal and Compliance Officer, as appropriate, to ensure the following subject matter is incorporated in the agreement:

- Scope
- Responsibilities of both parties, and description of product or services to be provided including subcontractors, if applicable
- Performance Measurements or Benchmarks that can be used to ensure performance of the product or service
- Default and Termination
- Cost and Compensation
- Ownership and Licensing
- Confidentiality
- Notification of Network Compromise
- Consumer Complaint Handling
- Contingency Plans
- Indemnification
- Insurance certifications
- Training and Dispute Resolution
- Limits of Liability
- Right to Audit by Bank and OCC
- Subject to Regulatory Examination and Oversight

4.0 POLICY STANDARDS

4.1. OVERSIGHT

All vendor relationships must be documented and approved by the appropriate Executive Officer. Management shall ensure that Company does not relinquish strategic control of any functions or activities outsourced to a vendor, and that vendor management approval and ongoing review procedures are followed.

4.2 FEES

The vendor's fees should be representative of and have a direct relationship to the service provided.

4.3 INFORMATION SHARING

Executive Management shall ensure that sharing of customer information with vendors is restricted to sharing permitted by law, written agreement to maintain the confidentiality and adequate security procedures are maintained. Executive Management approval is required prior to the commencement of an information sharing relationship.

5.0 MAINTENANCE DUE DILIGENCE

5.1. VENDOR SELECTION

Management shall ensure that proper due diligence is performed in selecting a vendor, including, but not limited to, consideration of business reputation, financial condition, and qualifications. Written procedures shall address the steps to be taken to determine the amount of due diligence needed based on the level and complexity of services performed.

5.2 CRITICAL VENDORS

A list of vendors critical to Company will be maintained and updated as defined in the Vendor Management procedures.

5.3 ANNUAL REVIEWS

Management shall ensure that each vendor that is considered critical to Company's operation and/or processes and stores any Company account number or social security number will have an annual review performed to validate compliance and be subjected to an annual due diligence review, including financials, audits and security assessment and other areas as deemed necessary based on the level of risk associated with that vendor, as well as an optional on-site (at management's discretion) review of the vendors operations.

6.0 BOARD REVIEW

6.1 REVIEWS

An Executive Summary report will be prepared on the annual vendor management review of critical service providers and presented to the Executive Committee, Board of Directors for review. Quarterly updates will be provided if there are status updates from vendor management.