IS-19 THIRD PARTY POLICY

19.1 Third Party Policy

<COMPANY NAME> makes every effort to assure all 3rd party organizations are compliant and do not compromise the integrity, security, and privacy of <COMPANY NAME> or <COMPANY NAME> Customer data. 3rd Parties include Customers, Partners, Subcontractors, and Contracted Developers.

19.2 Policies to Assure 3rd Parties Support Organizational Compliance

1. The following steps are required before 3rd parties are granted access to any <COMPANY NAME> systems:
    - Due diligence with the 3rd party;
    - Controls implemented to maintain compliance;
    - Written agreements, with appropriate security requirements, are executed.
2. All connections and data in transit between the <COMPANY NAME> Platform and 3rd parties are encrypted end to end.
3. Access granted to external parties is limited to the minimum necessary and granted only for the duration required.
4. A standard business associate agreement with Customers and Partners is defined and includes the required security controls in accordance with the organization's security policies. Additionally, responsibility is assigned in these agreements.
5. <COMPANY NAME> has Service Level Agreements (SLAs) with Subcontractors with an agreed service arrangement addressing liability, service definitions, security controls, and aspects of services management.
    - <COMPANY NAME> utilizes monitoring tools to regularly evaluate Subcontractors against relevant SLAs.
6. Third parties are unable to make changes to any <COMPANY NAME> infrastructure without explicit permission from <COMPANY NAME>. Additionally, no <COMPANY NAME> Customers or Partners have access outside of their own environment, meaning they cannot access, modify, or delete anything related to other 3rd parties.
7. Whenever outsourced development is utilized by <COMPANY NAME>, all changes to production systems will be approved and implemented by <COMPANY NAME> workforce members only. All outsourced development requires a formal contract with <COMPANY NAME>.
8. <COMPANY NAME> maintains and annually reviews a list all current Partners and Subcontractors.
9. <COMPANY NAME> assesses security requirements and compliance considerations with all Partners and Subcontracts.
10. Regular review is conducted as required by SLAs to assure security and compliance. These reviews include reports, audit trails, security events, operational issues, failures and disruptions, and identified issues are investigated and resolved in a reasonable and timely manner.
11. Any changes to Partner and Subcontractor services and systems are reviewed before implementation.
12. For all partners, <COMPANY NAME> reviews activity annually to assure partners are in line with SLAs in contracts with <COMPANY NAME>.

19.3 INVENTORY AND CLASSIFICATION OF OUTSOURCED PRODUCTS & SERVICES

If a product or service will be outsourced, both the due diligence during the selection process and the ongoing oversight of the selected vendor will be based on the bank's assessment of the importance or criticality of the outsourced product or service, but all vendors will have some level of ongoing oversight. An inventory of third party service providers shall be maintained, the inventory shall include:

- Vendor risk level;
- Types of data shared with the third party, including data classification;
- Brief description of services; and
- Significant controls in place.

Vendor risk level assessment will be based on the following considerations:

A product/service will be designated "critical" if:

- The vendor will be performing processing required for daily activities;
- The vendor has access to Restricted/Sensitive information;
- The service is significant to the bank's strategic - plans; and
- ***executive management designates it as such.***

A product/service will be designated "major'' if

- The vendor will perform any processing for the bank;
- The product is important to the bank's competitive posture; and
- ***Executive management designates it as such.***

A product/service will be designated "low" if

- The service is minimal to the bank's strategic - plans;
- The vendor's own reputation un-harms the Bank's reputation; and
- ***Executive management designates it as such.***

19.4 Third Party Contracts

Formal contracts that address relevant security and privacy requirements must be in place for all third parties that process, store, or transmit confidential data or provide critical services. The following must be included in all such contracts:

- Contracts will acknowledge that the third party is responsible for the security of the institution's confidential data that it possesses, stores, processes, or transmits;
- Contracts stipulate that the third-party security controls are regularly reviewed and validated by an independent party;
- Contracts identify the recourse available to <COMPANY NAME> should the third party fail to meet defined security requirements;
- Contracts establish responsibilities for responding to direct and indirect security incidents including timing as defined by service-level agreements (SLAs);
- Contracts specify the security requirements for the return or destruction of data upon contract termination;
- Responsibilities for managing devices (e.g., firewalls, routers) that secure connections with third parties are formally documented in the contract: and
- Contracts stipulate geographic limits on where data can be stored or transmitted.

19.5 Third-Party Review

In all cases where <COMPANY NAME>'s sensitive, critical services or data are provided to a third-party service provider, <COMPANY NAME> must review the service provider's internal control structure to ensure compatibility with <COMPANY NAME> Information Security requirements. The request and the results of the review should be provided to the Management Team. Once the relationship is established, an ongoing review of the service provider's internal controls structure is required on at least an annual basis. The evaluation of a third party may include the following items (if applicable):

- Audited financial statements, annual reports, SEC filings, and other available financial information;
- Significance of the proposed contract on the third-party's financial condition;
- Experience and ability in implementing and monitoring the proposed activity;
- Cost analysis comparing the Vendor's offering to other methods of performing the service, including the use of the other potential vendors and performing the service in-house.
- Business reputation of the Vendor (including reference checks with current customers);

- Qualifications and experience of Vendor's principals;
- Strategies and goals, including service philosophies, quality initiatives, efficiency improvements; and employment policies;
- Existence of any significant complaints or litigation, or regulatory actions against the Vendor;
- Ability to perform the proposed functions using current systems or the need to make additional investment;
- Use of other parties or subcontractors by the Vendor;
- Scope of internal controls, systems and data security, privacy protections and audit coverage;
- Business continuity and disaster recovery plans;
- Adequacy of management information systems;
- SSAE 18 documentation;
- Applicable Gramm-Leach-Bliley Act (GLBA) reviews; and,
- Insurance coverage.

Purpose

The purpose of this policy is to establish requirements for ensuring third-party service providers meet <COMPANY NAME> requirements for preserving and protecting <COMPANY NAME> Data.

Scope

This policy governs the processes used to determine the security posture and risk level of vendors with use of the company's data. The scope includes but may not be limited to the following:

• Information Technology & Security Operations.

• Finance Administration – Purchasing.

• Operations.

Applicable Standards

<u>Applicable Standards from the HITRUST Common Security Framework</u>

05.i - Identification of Risks Related to External Parties
05.k - Addressing Security in Third Party Agreements
09.e - Service Delivery
09.f - Monitoring and Review of Third Party Services
09.g - Managing Changes to Third Party Services
10.1 - Outsourced Software Development

<u>Applicable Standards from the HIPAA Security Rule</u>

164.314(a)(1)(i) - Business Associate Contracts or Other Arrangements

Revision History

Version	Date	Description of changes
		Initial creation