Apple Financial Holdings, Inc.

Information Security Policy

December 19, 2019

Table of Contents

POLICY NAME: Information Security Policy

REVIEW AND TRACKING CHART

Effective Date:	December 19, 2019
Version Number:	3.0
Policy Level:	Policy Level 1
Corresponding Board Review Frequency:	Annual (Every 12 Months)
Board or Designated Board Committee:	Board Risk Committee
Last Board Review Date:	December 19, 2019
Next Board Review Date:	December 2020
Designated Management Committee:	Management Risk Committee (MRC)
Last Management Review Date:	December 5, 2019
Next Management Review Date:	December 2020
Policy Owner:	Chief Information Security Officer

Terms not defined herein are defined on the Review and Tracking Chart on previous page.

I. POLICY PURPOSE STATEMENT AND SCOPE

The Information Security Policy (the "Policy") applies to the implementation, management and monitoring of information security at Apple Financial Holdings, Inc. ("AFH"), inclusive of Apple Bank for Savings and its subsidiaries (collectively, "ABS," "Apple," or the "Bank") in accordance with applicable state and federal statutes, rules and regulations.

The Chief Information Security Officer will provide effective oversight and governance to ensure that all Information Security policies, processes and procedures are being adhered to for the purposes of system acquisition, development, and maintenance. This includes, but is not limited to, roles and responsibilities, operations, monitoring, and/or other key components as set forth in the Information Security policy.

All Departments, at a minimum, must achieve the security level required by this Information Security Policy.

All AFH employees and third party resources engaged by the Bank must comply with the terms of this Policy to the degree applicable to them.

II. DEFINITIONS

- **Annual or Annually:** Every twelve (12) months.

- **Authentication:** A security method used to verify the identity of a user and authorize access to a system or network.

- **Biennial or Biennially:** Every twenty-four (24) months.

- **BYOD User:** Employees who acknowledge and agree to the terms and conditions in the BYOD Policy, the opportunity to use their own computers, smart phones, tablets, and other devices for business purposes (in particular, access to the Gmail application).

- **Effective Challenge:** An overarching, guiding business principle is that of "effective challenge" of all key business processes: that is, critical analysis by informed parties who can identify limitations to the process and produce appropriate changes. Personnel at all levels of the Bank are expected to execute effective challenge in their roles and responsibilities.

- **Encryption:** The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission (in-transit) or while stored (at-rest).

- **Firewall:** A security system that secures the network by enforcing boundaries between secure and unsecure areas. Firewalls are often implemented at the network perimeter as well as in high-security or high-risk areas.

- **Immaterial Change:** A change that does not alter the substance of the policy in any way, but rather is a change only to grammar, formatting, template, typos, and the like.

- **Incident:** An occurrence that actually or potentially jeopardize the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits that constitutes a violation or imminent threat of a violation of security policies, security procedures, or security manuals, or acceptable use policies.

- **Information Leakage:** Application weakness or information sharing where an application or the sharing of data reveals non-public information unintentionally.

- **Legal Contact:** The attorney from the Legal Department assigned to the group responsible for this Policy. The attorney does initial and ongoing reviews of the Policy; serves in an advisory capacity.

- **Malicious Code:** A term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors, and malicious active content.

- **Material Change:** A change that alters the substance of the policy in any way or how it is applied, such as a change to a definition, phrase, vendor name, threshold, or anything beyond an immaterial change as defined above.

- **Mobile Device:** A portable, wireless computing device that is small enough to be used while held in the hand, such as a smartphone, computer tablet, PDA, etc.

- **Mobile Storage Media:** A data storage device that utilizes flash memory to store data. They are often called a USB drive, a flash drive, or thumb drive.

- **Multi-Factor Authentication ("MFA"):** Authentication through verification of at least two of the following types of authentication factors:

  a. Knowledge factors, such as a password; or
  b. Possession factors, such as a token or text message on a mobile phone; or
  c. Inherence factors, such as a biometric characteristic.

- **Non-Public Information ("NPI"):** All electronic information that is not publically available information and is:

  a. Business related information of an organization that the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of an organization.
  b. Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: social security number, driver's license number or non-driver identification card number, account number, credit or debit card number, any security code, access code or password that would permit access to an individual's financial account, or biometric records;
  c. Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, the provision of health care to any individual, or payment for the provision of health care to any individual.

- **Password:** A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also can be known as a passphrase or passcode.

- **Policy Level 1:** A Regular Board Review Cycle level for a Policy, designated by Risk Management in consult with Legal. Level 1 policies require Annual approval by the Board or a Board level committee.

- **Policy Owner:** The person responsible for management and tracking of the Policy. This includes initiating the review of the Policy and recommending updates to the Policy, to the extent needed. Policy Owners are responsible for obtaining the appropriate level of approval and providing the approved documents to the Policies and Procedures Administrator ("PPA") (defined in this Section) for upload to AppleNet. Additionally, the Policy Owner is responsible for presenting revisions and Policy exception requests for consideration.

- **PPA (Policies and Procedures Administrator):** The PPA is a member of Risk Management. The PPA monitors the occurrence and timeliness of scheduled Policy and Procedure reviews, obtains the updated versions of Policies and Procedures, and ensures they are uploaded to AppleNet. The PPA shall review Policies and advise the Policy Owner if procedures have been errantly included in the Policy, and the Policy Owner shall revise accordingly. The PPA will also provide guidance regarding the use of this Policy to Bank personnel.

- **Private Information:** Any personal information concerning a natural person in combination with any one or more of the following data elements: social security number, driver's license number, account number, or credit or debit card number in combination with any required security code.

- **Publically Available Information:** Any information that an organization has a reasonable basis to believe is lawfully made available to the general public from federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law. An organization has a reasonable basis to believe that information is lawfully made available to the general public if the organization has taken steps to determine:

    a. That the information is of the type that is available to general public; and
    b. Whether an individual can direct that the information not be made available to the general public and, if so, that such individual has not done so.

- **Regular Board Review Cycle:** The required periodic Board or Board level committee approval process for a Policy, the frequency of which is determined by the designation of Level 1, Level 2, or Level 3.

- **Remote Access:** Communicating with a computer or network from an off-site location.

- **Router:** A network layer device that uses on or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information.

- **Sensitive Position:** An employee that engages in transactional business or has the ability to change the official records of the Bank and/or can influence or cause such activity to occur.

- **Triennial or Triennially:** Every thirty-six (36) months.

- **User Roles:** A group of users with particular meaning in a business model, such that the group of users share a business function.

III. KEY POLICY COMPONENTS

1. Executive Summary

This document outlines AFH's Policy with respect to the implementation, management, and monitoring of information security.

The information that AFH uses to conduct its business is a valuable asset that must be protected at all times ensuring the security and confidentiality of customer information. This information must be protected from anticipated threats or hazards to the security or integrity of the information such as unauthorized access, modification, disclosure or destruction. Information security is defined as the protection of:

- Confidentiality: Ensuring that information is accessible only to those persons authorized to have access;
- Integrity: Safeguarding the accuracy and completeness of information; and
- Availability: Ensuring that authorized users have access to information and information systems in a timely manner.

AFH has identified a set of core security principles to guide the creation of the Policy. The Policy is derived in principle from: NIST IT standards, COBIT 5 IT standards, NYSDFS cybersecurity regulations, FFIEC IT booklets and the ISO 27002 framework, Center for Internet Security controls and additionally reflects industry best practices.

AFH also operates under the three lines of defense model, in which management control acts as the first line of defense; risk, control and compliance over-sight (e.g., the Information Security Department) functions established by management are the second line of defense while independent assurance (e.g., Internal Audit reporting to the Board of Directors) acts as the third line. Details regarding the lines of defense model is located in Appendix A, in the Information Security & Information Technology Lines of Defense document.

Information can exist in many forms: on paper, in an electronic format or verbally on or off the bank premises. In whatever form, AFH information is shared or stored, the goal of this policy is to ensure AFH information is properly safeguarded.

AFH retains the right to observe, review or audit all information stored on Bank provided computers, storage media, and any other information assets used to support AFH business activity.

2. Objectives

The objective of this Policy is to protect the confidentiality, integrity and availability of AFH information and to establish a standardized and consistent approach to provide a security framework that will ensure the protection of Apple Bank Information from unauthorized access, loss or damage while supporting the open, information-sharing needs of the Bank.

Apple Bank Information may be verbal, digital, and/or hardcopy, individually controlled or shared, stand-alone or networked, used for administration or other purposes. Procedures related to this Information Security Policy will be developed and published separately.

3. Key Components of Policy

This Information Security Policy describes safeguards implemented by Apple Bank to protect covered data and information in compliance with the Safeguards Rule promulgated under the Gramm Leach Bliley Act (GLBA). These safeguards are provided to:

a. Ensure the security and confidentiality of covered data and information;
b. Protect against anticipated threats or hazards to the security or integrity of such information; and
c. Protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to any customer.

This Information Security Policy also identifies mechanisms to:

a. Identify and assess the risks that may threaten covered data and information maintained by Apple Bank;
b. Develop written policies and procedures to manage and control these risks;
c. Implement and review the policies; and
d. Adjust the Policies to reflect changes in technology, the sensitivity of covered data and information and internal or external threats to information security.

AFH ensures that information and information systems are protected in a manner that complies with all applicable banking laws and regulations, such as 15 USC 6801 and 6805(b): Gramm-Leach-Bliley Act (GLBA), 12CFR 364 Appendix B Interagency Guidelines Establishing Information Security Standards, FDIC FILs, New York State Department of Financial Services 23 NYCRR 500 (Cybersecurity Requirements for Financial Services Companies) and/or industry standards.

To achieve these objectives:

a. The Chief Information Security Officer has been designated to manage from the second line of defense to provide oversight of Information Security;
b. Perform risk assessments, including cyber related risks, to AFH information and information systems;
c. Monitor, evaluate and adjust the Information and Cyber Security policies and procedures at least annually;
d. The Information and Cybersecurity policies must be approved by the board of directors or an appropriate committee of the board annually; and
e. The overall status of AFH Information Security environment and the Bank's compliance with the Gramm Leach Bliley Act must be reported to the Board at least annually.

3.1 RISK ASSESSMENTS

The Bank must identify and prioritize risk, including cyber risk, using control objectives and to implement controls that provide a reasonable assurance that objectives will be met and that risk will be managed to an acceptable level.

The risk assessment performed must conform to the Risk Management Policies and Procedures.

Annual risk assessments must be performed and include the evaluation of risk by identifying the potential threats to the information and the information technology resource and the impact and likelihood of potential threats.

The Bank completes the annually the FDIC Cybersecurity Assessment Tool to determine their inherent risk profile, the targeted maturity level required for the inherent risk and the current cybersecurity maturity level for the Bank.

3.2 ASSET MANAGEMENT

Effective controls must be implemented to protect assets including a mechanism to maintain an accurate inventory of assets and establish ownership of assets and classification of assets based on business impact and privacy implications. A Data Classification Policy must be implemented to provide guidance in classifying assets and protecting this data.

3.2.1 Accountability

Hardware assets must be transferred reliably and any data they contain rendered unreadable prior to the transfer to another employee or other disposition. Management must be notified of any lost or misplaced assets. At least annually, an asset recertification must be completed.

3.2.2 Acceptable Use

An Acceptable Use Policy must be implemented to stipulate constraints and practices that a user must agree to for access to the AFH network.

3.2.3 Personal Assets

Security controls such as remote wipe capability and encryption, must be in place if devices are used to perform business transactions or to access AFH Technology resources.

3.2.4 End of Life

Documented replacement or risk mitigation strategies must be in place for operating systems, software applications and critical infrastructure components that are nearing end of life.

3.3 HUMAN RESOURCE SECURITY

Security responsibilities must be defined and addressed at the employee hiring stage, included in contracts with third parties, and monitored by the employee's direct supervisor during an individual's employment.

3.3.1 Job Responsibility

Security roles and responsibilities as defined in this policy must be documented where appropriate.

3.3.2 Screening

Background checks (screening) on all potential employees and third party users must be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements.

3.3.3 Training

At least annually, employees must receive cybersecurity and security awareness training and regular updates in Bank policies and procedures relevant to their job functions. Security awareness training must commence with the onboarding process.

3.3.4 Vacation

All Bank employees in sensitive positions must take at least two (2) consecutive weeks of vacation or other leave on an annual basis (within a twelve-month period incorporating the current year).

3.3.5 Disciplinary Process

For employees who have violated AFH Information Security policy, disciplinary actions may result in a warning up to and including termination.

3.3.6 Termination

A formal process must be implemented to ensure an employee’s or third party user’s exit from the AFH is managed, and that the return of all AFH assets and the removal of all access rights are completed upon termination.

3.3.7 Reporting Security Weakness

Users of AFH Information Technology resources are required to report any observed or suspected security weaknesses or threats to the appropriate manager/supervisor or the Chief Information Security Officer or members of the Information Technology Department immediately.

3.4 IDENTITY AND ACCESS CONTROL

Users must be required to authenticate themselves with a unique user account and an authentication mechanism such as password, token, biometric when accessing application/systems.

3.4.1 User Accounts

The user accounts are the responsibility of the individual for which it was assigned and will be accountable for all activity linked to their user account. In regards to user accounts, the following must be adhered to:

a. A standard format must be created for user accounts;
b. Users must not share their user account;
c. Group or service accounts are only permitted when a legitimate business or operational reasons require and the ownership of the account must be documented;
d. User accounts should be automatically disabled after a set period of inactivity; and
e. Deactivated accounts should be monitored through audit logging to determine if there are attempts to access such accounts.

3.4.2 Passwords

Passwords must conform to the requirements and guidelines stated in AFH's Password Policy, including the following:

a. No employee should request or require another employee to disclose their password;
b. Informal delegation of processing responsibility by sharing passwords is not permitted; and
c. A secure process must be implemented to reset passwords.

3.4.3 Logical Access Control

AFH must ensure authentication and authorization controls are appropriate for the risk that exists for the data and application, including the following:

a. Application and system access will not be granted to any user without approval;
b. Access controls must be used to limit user access to only those applications, network rights and systems functions, for which they have been authorized and the time periods that they need to access the network;
c. Users will only receive access to the minimum applications and privileges required to perform their job function; and
d. A role based access control model that grants access to IT resources based on a user role, such as job title or work responsibilities, should be implemented where practical.

3.4.4 User Registration and Management

A formal user management process which includes a sign-off by the authorized requestor and data owner must be implemented. This will ensure only authorized users have access to AFH resources required for their business needs. This process must include:

a. Creating new user accounts;
b. Removing user accounts;
c. Modifying user accounts;
d. Periodic reviewing user accounts and their access; and
e. Resetting Passwords.

3.4.5 Banners

Logon banners must be implemented on all systems where that feature is available to inform all users that the system is intended only for AFH business or other approved use consistent with AFH policies and that user activity may be monitored and the user should have no expectation of privacy.

3.4.6 Privileged Accounts

The issuance and use of privileged accounts must be controlled and restricted. Responsibility for creation of and access to privileged accounts should be limited to pre-authorized sets of users, such as administrators. The following items are also required:

a. Privileged accounts will only be setup when there is a legitimate business requirement;
b. Privileged users must complete annual training;
c. Based on a risk-based approach, users must be assigned a different privileged account from their user account used for non-privileged use;
d. Use of privileged user account activity must be logged and monitored;
e. Users must not be granted local administrator rights to the workstations;
f. User account must be recertified, at least, quarterly for all applications that are considered high risk (either according to the CISO or the official application inventory);
g. Remote control of workstations must be restricted to privileged accounts and remote control must not be permitted unless and until the user gives permission; and
h. Any privileged user account no longer needed must be removed.

3.4.7 Third Party Accounts

Third party users must not be granted a user account or otherwise be given privileges to the AFH network unless approval of the vendor owner has first been obtained and the business requirement documented.

Any access must be enabled only for the time period required to accomplish the contracted tasks and a non-disclosure agreement ("NDA") must be in place and an Acceptable Use Policy agreement must be completed by the third party user.

3.4.8 User Account Review

AFH Management must review access rights granted to users for all applications that contain non-public information. User access rights must be reviewed and evaluated when the user is transferred to another department or reassigned from one role to another role within the same department.

At least annually, existing entitlements for all applications that contain non-public information or identified as critical applications must recertified.

3.5 PHYSICAL SECURITY AND ENVIRONMENTAL CONTROLS

AFH's information technology resources must be physically protected in based on the criticality or importance of their function.

3.5.1 General Offices

Access to staff offices, telephone closets, computer rooms, network rooms, and other work areas containing non-public information must be physically restricted.

3.5.2 Mobile Storage Media

The ability for users to use mobile storage media along with ‘auto-run’ features upon the insertion of mobile storage media must be blocked by default and only Apple Bank issued encrypted mobile storage media must be used. Any requests for mobile storage media capabilities must be authorized by the Information Security Department.

3.5.3 Mobile Devices

Non-public information must not be stored on mobile devices, unless absolutely necessary and if so, it must always be encrypted.

3.5.4 Clean Desk

Sensitive or confidential information, e.g. on paper or on electronic storage media, must be secured when not required, especially when the office is vacated at the end of the workday.

3.5.5 Clear Screen

Whenever unattended or not in use, all computing devices must be logged off or protected with a screen or keyboard locking mechanism controlled by a password or similar user authentication mechanism (this includes laptops, tablets, smartphones and desktops).

When viewing sensitive information on a screen, users should be aware of their surroundings and must ensure that third parties are not permitted to view the sensitive information.

3.5.6 Printers/Faxes

Paper containing sensitive or classified information must be removed from printers and faxes immediately. Faxes and printers used to print sensitive information should not be in public areas. Printers and fax machines must be kept within a secure area.

3.5.7 Servers and Network Devices

Servers and network devices must be secured in locked cabinets, locked closets, locked computer rooms or in a secure location based on risk and feasibility.

3.5.8 Data Center

The data center must be physically separate from all other AFH offices. The data center must be protected with physical security measures that prevent unauthorized persons from gaining access.

3.5.9 Power

Standard electrical power surge protectors must be installed to protect all application or network systems. Equipment used for critical production business applications must employ uninterruptible power systems (UPS). Additional controls must be implemented to protect supporting infrastructure such as power supply and cabling infrastructure from interception or damage.

3.5.10 Environmental Controls

To protect the critical computer systems, a combination of fire suppression, smoke alarms, raised flooring, water detectors, and heat and moisture sensors must address risks from environmental threats (e.g., fire, flood, and excessive heat). Environmental threat monitoring should be continuous, and responses should occur when alarms activate.

3.5.11 Document Disposal

Employees must not discard paper based information (documents) containing non-public information in the regular garbage. All documents being discarded which contains non-public information must be destroyed by shredding or disposed in locked shredding bins.

The disposal of the documents must be consistent with established regulatory and AFH retention guidelines.

When shred bins are emptied, the process must be logged, secured until disposal and an adequate audit trail must be maintained.

3.5.12 Media Disposal

Electronic files containing non-public information must have their drives sanitized or the drives physically incinerated, shredded, or destroyed in a timely manner. The following guidance is also required:

a. Management should log the disposal of the media.
b. All media must be logged, secured until disposal and an adequate audit trail must be maintained.
c. The disposal of the data must be consistent with established regulatory and AFH retention guidelines.

3.5.13 Delivery and Loading Areas

Delivery and loading areas where unauthorized persons may enter AFH must be secured and, if possible, isolated from information processing areas to avoid unauthorized access. This area should be configured so delivery personnel can unload without entering processing areas or other parts of the facility.

3.6 SOFTWARE AND HARDWARE

Hardware or software must be secured from unauthorized access. Hardware and software must not be taken off-site without prior authorization.

3.6.1 Software

Users must understand and abide by the terms of the licensing agreements of the software they use. User must not use, copy or distribute software in violation of the license agreement, copyrights or law. The following is also required:

a. All software must be installed by a designated system administrator
b. Only install licensed and authorized software is to be installed.

3.6.2 Hardware

AFH computer hardware purchasing must be centralized within the MIS Department to ensure that all equipment conforms to hardware standards. All such hardware must be used in compliance to applicable licenses, notices, contracts and agreements.

No outside computer equipment may be connected to the AFH network without the MIS Department approval and hardware must be sited or protected to reduce the risks from environmental threats and unauthorized access.

3.7 INFORMATION AND DATA SECURITY

Information contained in AFH's system must be complete and accurate. Controls must be implemented to ensure that inaccurate or incomplete information is deleted, corrected, supplemented or updated. Customer or consumer information, especially non-public information must be protected to ensure only authorized individuals have access.

3.7.1 Privacy

Employees must protect the individual's non-public information throughout the data lifecycle (see the Apple Bank Privacy Policy).

3.7.2 Employee Responsibilities

Department Managers have the responsibility to authorize access to application or systems containing non-public information including information about customers, consumers, employees and third parties, collected and maintained by AFH.

AFH data must be:

a. Used only for the stated purpose for which it was gathered;
b. Gathered in lawful and fair circumstances;
c. Retained for the amount of time required by law or regulations or as long as it remains relevant for its primary purpose;
d. Not be disclosed without specific consent or as authorized by law;
e. Available for review by authorized individuals;
f. Corrected, if errors are found or are reported;
g. Deleted where appropriate if the individual requests are consistent with applicable laws;
h. Be protected using system access controls, or be stored in a locked cabinet or office;
i. Be destroyed in a manner consistent with established AFH retention requirements and by law or regulations;
j. For systems that store, process, transmit or otherwise come into contact with sensitive information which are accessed in an ad-hoc and/or irregular manner should be classified further as a ‘stand-alone system’ and should be removed from the network and only accessed when needed (alternatively, the system can be fully virtualized and powered off until needed);
k. Automated tools must be deployed on all network perimeters to monitor for the unauthorized transfer of sensitive information and block such transfers while alerting information security professionals;
l. The network should be segmented based on the classification level of the information stored on systems and systems containing sensitive information should reside on a separate virtual local area network (VLAN); and
m. Third parties must be contractually obligated to abide by these rules.

3.7.3 Electronic Files at Rest

Based on risks, the Bank must implement controls, including encryption, to protect electronic files containing non-public information at rest. All electronic files containing non-public information at rest must be secured by encryption. If encryption is not feasible, compensating controls must be approved by the Chief Information Security Officer.

3.7.4 Electronic Files in Transit

Based on risks, electronic files containing non-public information that are in transit or transmitted over a public or untrusted network (e.g., Internet) must be encrypted or use an encrypted connection to protect the confidentiality of the communication. If encryption is not feasible, compensating controls must be approved by the Chief Information Security Officer.

Traffic leaving the organization must be monitored to detect the unauthorized transfer of non-public information.

3.7.5 Cloud Storage

Files containing non-public information must be encrypted when transmitted or stored using a cloud storage provider and must never be stored on an unauthorized cloud storage provider.

3.7.6 Social Media

Non-public information must not be posted to social media sites in any form.

3.7.7 Third Party

Non-public information must not be released to a third party without a confidentiality/non-disclosure agreement and the assurance of proper controls over data that is transmitted and at rest. The third party controls must demonstrate to AFH, the third party's diligence in protecting such data and its subsequent destruction.

The third party controls must be evaluated annually to ensure they are maintaining a level of control that adequately protects such data. At a minimum, the third party's safeguards for protecting non-public information must include:

a. Limiting access of non-public information to authorized persons;
b. Granting access based on least privileged requirements;
c. Securing facilities, data centers, paper files, servers, back-up systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability;
d. Implementing network, device, application, databases and platform security.
e. Backing up data and a recovery strategy;
f. Ensuring anti-malware software installed and regularly updated;
g. Multi-factor or strong authentication for accessing the internal network remotely;
h. Implementing access and authentication controls;
i. Logging and monitoring of unauthorized and malicious activity;
j. Encrypting non-public information at rest and stored on any mobile media, including backup media; If encryption is not feasible, compensating controls must be approved by the CISO;
k. Provide appropriate security awareness training to its employees;
l. Encrypting non-public information transmitted over public or wireless networks;
m. Conduct appropriate due diligence in selecting and monitoring third-party service providers;
n. Implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law;
o. The actual physical location of the data and/or the system (databases, cloud storage, etc.) the data is stored therein, which has been classified as either Sensitive or Non-Public, must be in the United States of America.

At a minimum, the contract must have provisions that the Third Party will:

a. Return or destroy Bank information upon termination or expiration of the contract;
b. Provide notice to the Bank of any actual or suspected unauthorized disclosure of, access to or other breach of data;
c. Not copy, cause to be copied, use or disclose data received from or on behalf of the Bank except as permitted or required by the agreement, as required by law, or as otherwise authorized by the bank in writing; and
d. Provide the geographical location of where the Apple Bank data resides if the third party is storing such data;
e. Audit records, logs and log files that are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Bank shall be maintain at least five years; and
f. Audit records, logs and log files that are designed to detect and respond to cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operations of the Bank must be maintained for at least three years.
g. AFH will retain data based on business requirements and applicable rules, regulations, laws and standards.

3.7.8 Data Retention

Non-public information which is no longer necessary for business operations or other legitimate business reasons must be securely disposed unless required to be retained by law or regulation or where disposal is not feasible due to the manner in which the information is maintained.

3.8 SYSTEMS AND NETWORK SECURITY

Managers must implement controls to ensure the security of information in systems and networks and the protection of connected services from unauthorized access. The following is required:

a. User must only be granted the least privileges to perform their tasks;
b. The network perimeter must be configured to deny all activity that is not expressly permitted;
c. Operational responsibilities for the network must be separated from computer operations, where appropriate
d. Network Intrusion Prevention System (IPS) sensors must be deployed at the network’s boundaries to block malicious traffic at each of the organization’s network boundaries;
e. DHCP (Dynamic Host Configuration Protocol) logging is to be used on all DHCP servers and the respective logs need to fed into the SIEM (Security Incident & Event Manager); and
f. Management must maintain accurate network diagrams and store them securely, providing access only to authorized personnel.

3.8.1 E-Mail

Access to non-bank/personal e-mail solutions must be restricted. Preventive and detective measures must be established to safeguard AFH's e-mail system from unauthorized access, modification or denial of service, spam and phishing emails, malicious e-mails, attachments and the leaking of non-public information.

Authorized e-mails containing non-public information must be masked or encrypted if leaving the AFH network and unauthorized use of non-public information must be blocked. E-mail records must be archived to a central storage location. The minimum retention period for theses archived records should be, at a minimum, sixty (60) months.

3.8.2 Messaging and Conference

When using commercial messaging solutions, methods of authorization and encryption must be employed, when appropriate, to ensure that information is not disclosed to unauthorized individuals.

3.8.3 Internet

Global Internet access is granted based on job function title. Web content filtering must be in place to restrict non-bank external webmail, instant messaging, file sharing and other prohibited sites.

Customer access to Internet-based products or services must require authentication controls such as multi-factor or layered controls that are commensurate with the risk.

All networking traffic flowing either to or from the Internet must be configured to filter unauthorized connections.

3.8.4 Personal Usage

Personal usage of the Internet is permitted as long as such usage follows does not have a detrimental effect on AFH’s operations or reputation or on the user’s job performance.

3.8.5 Remote Access

All remote access users are expected to comply with AFH policies, may not perform illegal activities and may not use the access for outside personal or business interests. The following controls must be implemented to ensure protection against unauthorized access or introduction of malicious code to hardware or software:

a. Remote users must authenticate using strong or multifactor authentication and must authenticate to the Windows Active Directory;
b. Any and all devices must be in compliance to Bank's security policies in the same manner as it is for local users;
c. Third party users that are required to access the Bank's internal network remotely must have the application owner get IT Department approval;
d. Third party user accounts, used to perform maintenance, must be disabled outside of the maintenance period; and
e. Employees, in sensitive positions, on vacation are prohibited from accessing the AFH network remotely and any exceptions must be formally authorized by the Chief Technology Officer.

3.8.6 Modern Usage

Connecting dial-up modems to workstations that are stand-alone or connected to AFH network is prohibited.

3.8.7 Wireless Connections

The installation of wireless access points and gateways without Management approval is prohibited. Management must use an industry-accepted level of encryption with strength commensurate with the risk profile on the Bank's wireless network. In regards to wireless connections, the following guidance must be followed:

a. Someone must be appointed responsible and have the authority over the network;
b. A risk assessment must be performed prior to installation to determine the threats and vulnerabilities of the wireless network to the Bank;
c. The network must be separate and distinct from the production network; and
d. The Bank may provide guests with access to a wireless network and must be configured to prevent access to any portion of the production network.

The Bank must scan the network regularly to detect rogue access points and consider implementing NAC systems to prevent the successful connection of unauthorized devices.

3.8.8 External Connections

Access granted for external connections must be restricted and carefully controlled to ensure security concerns are addressed and the proper use of AFH information technology resources, such as:

a. Any new external connection must not interfere with the current production work environment and requires the CISO’s approval;
b. An external connection involving non-public information being transmitted over public or untrusted networks, must be secured by encrypting the information or using an encrypted connection;
c. Web Application Firewalls (WAFs) must be deployed in front of any web application servers to verify and validate the traffic going both to and from the server; and
d. Any unauthorized traffic detected should be blocked and logged accordingly.

3.8.9 Standard Builds

Information systems must be deployed with appropriate security configurations that are hardened and tested, at a minimum, monthly for compliance with industry standards or baselines approved by Information Security. The following actions must also be followed:

a. Documented baselines must be established and when configurations change, baselines must be updated;
b. Baselines must be based on industry standards and any deviation must be supported by business justification and information Technology Operations Security and Information Security approval; and
c. A configuration monitoring tool is to be deployed and used to verify all security configuration elements, with a catalog of approved exceptions/deviations.

3.8.10 Host Intrusion Prevention

AFH computers connected to the internal network must have a host-based firewall implemented to monitor suspicious activity by analyzing events. Host-based firewalls or port-filtering tools on end systems are enabled (with a default-deny rule) to drop all traffic except those services and ports are specifically allowed.

3.8.11 Malicious Code

Management must implement defense-in-depth to protect, detect, and respond to malicious code. The Bank must implement tools to block malicious code before it enters the environment and to detect it and respond if it is not blocked. The following controls must also be implemented:

a. Workstations connected to the internal network must have an endpoint protection solution installed;
b. Daily automatic local scans must be scheduled;
c. Software and definition files must be set to automatically receive the latest updates;
d. All files retrieved through a network connection, e-mail or mobile storage media must be scanned; and
e. Controls must be in place to restrict the ability to disable or remove anti-malware programs must be restricted.

3.8.12 Network Segmentation

When the AFH network is connected to an external network, controls must be in place to prevent unauthorized users and third party users from accessing restricted areas of AFH's internal network. These types of connections must be secured with firewalls or external security devices that filters both incoming and outgoing network traffic against access restrictions, common threats. The Information Security Department also requires that:

a. Each firewall or external security device must have their rules formally documented, at the minimum, indicating the business case for the rules;
b. Firewall changes are risk rated and high risk changes must be approved by Information Security; and
c. Rules must be independently reviewed quarterly to ensure unauthorized changes were not implemented.

3.9 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

Security has to be considered at all stages of the development in order to ensure adherence with all appropriate security requirements, protect non-public information, facilitate efficient implementation of security controls, prevent new risks when the system is modified, and ensure proper removal of data when the system is retired.

AFH must develop written procedures and/or guidelines and standards designed to ensure the use of secure development practices for in-house developed applications.

Without specific written exceptions, all programs and documentation generated by or provided by employees or third parties for the benefit of AFH are the property of AFH.

3.9.1 Operational Software

Policy and procedures must be implemented to control the installation of only authorized software on operational systems.

The software version acquired must still be supported by the developer or third party or appropriately hardened based upon the developer or third party's security recommendations.

3.9.2 Test Data

Testing must not be done using live data due to the threat to its confidentiality and/or integrity. Testing of information systems must be done with test data that mimics the characteristics of the real data, or on copies of real data with any non-public or confidential data appropriately sanitized or protected with at least equivalent protection measures as production.

3.9.3 Source Code

Access to program source code and associated documents specifications, documentation must be controlled to limit the unauthorized functionality and avoid unintentional changes.

3.9.4 Change Management

All critical computer and communications systems must employ a process to authorize changes to software, hardware, communications networks, system configuration, applications and security tools. Configuration of these devices over the network must be managed using both encrypted sessions and multi-factor authentication (MFA). The following items are also required:

a. All critical changes must flow through the established change management oversight function, requiring CISO approval(s);
b. Any unauthorized changes need to be identified and investigated and if confirmed, the unauthorized change must be reported to management; and
c. Only documented, approved and tested changes, when feasible, are installed into the production environment.

3.9.5 Test Environment

Development, testing, and production environments must be sufficiently separated and any non-public information stored in these environments must have at least equivalent protection measures as production.

Procedures for the transfer of software from development to production must be defined and documented.

3.9.6 Operating System Changes

When operating systems and processes are changed, critical business processes must be documented, authorized, reviewed and tested to ensure that there is no adverse impact.

All critical changes must flow through the established change management oversight function, requiring the CISO's approval.

3.9.7 Patch Management

A patch management program must be implemented to ensure that all software and firmware patches across all Bank platforms and third Party applications are applied in a timely manner. The Information Security Department also requires that:

a. A patch schedule must define a based on industry standards or approved by Information Security that prioritized the testing and implementation of critical patches, with the highest priority to zero day patches and/or critical assets;
b. Appropriate patch and/update windows (maintenance window) must be defined to implement patches to minimize business impact or potential down time;
c. Regular assessments must be performed to gauge the success of the patch management efforts ensuring the systems that are supposed to be updated are actually patched; and
d. Any vulnerability deemed not patchable must be assessed, compensating controls identified and remediated through a risk acceptance process.

3.9.8 Outsourced Software Development

Outsourced software development must be appropriately supervised and monitored by AFH personnel and must be evaluated, assessed and/or tested to ensure security concerns were addressed, including, but not limited to:

a. All security related guidelines and standards must be periodically reviewed, assessed and updated as necessary by the Chief Information Security Officer; and
b. Outsourced developers must adhere to, at least the same level, as the AFH's Software Development Lifecycle (SDLC) policy;
c. Outsourced developers must use secure coding practices, appropriate to both the language and development environment being used;
d. Only up-to-date and trusted third party components will be used by the outsourced developers;
e. Upon completion of development activities by a third party, a static and/or dynamic analysis scan of the codebase must be completed to ensure secure development practices were adhered to and that the code will be delivered from the third party developer to AFH, free from any issues or vulnerabilities.

3.9.9 Encryption

Encryption of non-public information at rest or in transit must be achieved via commercially available products that incorporates Federal Information Processing Standard (FIPS) approved algorithms for data encryption at a minimum of 128-bit strength. Minimum key length for digital signatures and public key encryption is 2048. Hashing functions must have a minimum key length of 256.

3.9.10 Encryption Key Management

Keys used for encrypting AFH information must be classified as non-public information. Key owners need to ensure keys will be generated, stored, and managed in a secure and approved manner.

Keys must be changed periodically based on industry standards and the keys must be physically secured with at least two upper-level personnel assigned access and key management related activities must be logged.

3.9.11 Software Packages

Modifications to software packages should be discouraged, limited to necessary changes, and all changes shall be strictly controlled and approved by Management.

3.9.12 Information Leakage

Opportunities for information leakage must be mitigated or prevented. Perimeter controls must identify, quarantine and report unauthorized information leakage.

3.10 OPERATIONS MANAGEMENT

Responsibilities, processes and procedures should be established and documented for the management and operation of all information processing facilities. This includes the development of appropriate operating instructions and incident response procedures.

Operating procedures, including housekeeping activities must be formally documented and controlled with a formal change management process.

3.10.1 Segregation of Duties

Segregation of duties must be implemented to ensures that there is oversight and a review process to catch errors and help to prevent fraud and theft.

3.10.2 Capacity Management

Information Technology capacity must be planned and managed to provide the Bank's environment capable of sustaining the workload of it entire production systems while providing acceptable response time for al supported systems.

Requirements for new systems must be established, documented and tested prior to their acceptance and implementation and capacity demands must be monitored and projections for future capacity requirements must be made to ensure that adequate processing capability and storage are available for normal and peak times.

3.10.3 Acceptance Testing

Acceptance criteria based on best practices for new information systems, upgrades and new versions of existing systems must be established. Tests must be performed to ensure requirements have been met prior to formal system acceptance.

3.10.4 System Utilities

The use of utility programs that are capable of overriding systems and application controls must be restricted and controlled by Management.

Unnecessary software utilities and system software must be removed/disabled and system utilities must not be available to users that have access to the system applications.

3.10.5 Software and Data Backup

A backup process and strategy must be developed and documented to ensure all software and critical data can be recovered following hardware or media failure or a cybersecurity incident. The following controls are required by the Information Security Department:

a. Backup media that contains non-public information must be encrypted;
b. All current versions of software must be backed up;
c. Critical data stored on the AFH file server(s) and network servers, which may include web servers, database servers, domain controllers, firewalls, network devices, security appliances and remote access servers must be backed up;
d. Backup media must be retained according to documented retention schedule;
e. Backup media must be regularly tested for recoverability and documented;
f. Backup media containing critical software and data must have at least one destination which is either offline or inaccessible with a network connection; and
g. Geographic separation from the backups must be maintained to protect the media from fire, flood, or other regional or large-scale disasters.

3.10.6 Equipment Maintenance

All computers and communication equipment used must be maintained in accordance with the manufacturers' recommended service intervals and specifications, with only qualified and authorized maintenance personnel permitted to repair and service such equipment.

Documented records must be kept of suspected or actual faults and corrective or maintenance activities.

3.11 SYSTEMS AND NETWORK MONITORING

Systems must be configured to log exceptions, security related events and user activities. Operator logs and fault logging must be used to ensure information system problems are identified. Business defined security events must generate alarms and notifications to appropriate personnel. The Bank must comply with all relevant legal and regulatory requirements applicable to its monitoring and logging activities.

3.11.1 Logging

Logs recording exceptions, user activities, security violations, system alerts or failures and changes to or attempts to change system settings must be maintained by completing the following:

a. Logging systems and log data must be protected against tampering and unauthorized access;
b. Infrastructure devices must have their internal clocks set accurately and synchronized regularly from an AFH accurate time source; and
c. Logging must be enabled on all devices that allows for the following attributes to be captured inside the log files: event source, date, user, timestamp, source addresses, destination addresses, and any other useful elements deemed necessary.

3.11.2 Log Retention

Audit records, logs and log files are to be kept available to assist in the reconstruction of material financial transactions and to detect and respond to cybersecurity events. In addition, the following controls are required:

a. Audit records that are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Bank shall be maintain at least five years; and
b. Audit records that are designed to detect and respond to cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operations of the Bank must be maintained for at least three years.

3.11.3 Unauthorized Use Monitoring

Processes for monitoring use of information technology resources must be established to detect unauthorized access or use of, or tampering with non-public information. The level of monitoring required can be continuous and/or periodic depending on the event severity or the results of a risk assessment.

3.11.4 Network Monitoring

Network traffic traversing AFH network must be inspected for active attacks against AFH information technology resources. Interdiction capabilities must be maintained to effectively block attacks that present appreciable risks to AFH. The following requirements must also be considered:

a. Event logs such as system logs, network logs, application logs and logs generated by commercial tools, such as malware protection, intrusion detection systems (IDS) and intrusion prevention systems (IPS) must be analyzed, prioritized and selected for monitoring based on the data and services critical to the Bank business operations and their value from a security monitoring perspective;
b. Suspicious activity must be investigated, documented and remediated in the approved SLAs;
c. Critical alerts must be reported real-time; and
d. Management summary reports must be distributed to the Chief Technology Officer and Chief Information Security Officer.

3.11.5 Unauthorized Device Monitoring

A formal processes to identify unauthorized devices, including wireless devices or modems, connected to the internal network must be implemented. Any unauthorized device must be immediately investigated and remediated.

3.11.6 Penetration Testing

To reduce the risk that a malicious actor can gain unauthorized access to the AFH network or exploit vulnerabilities within the network, an external penetration test of all external access points and an internal penetration test of the internal network must be completed annually. All penetration tests conducted by AFH personnel or third parties must ensure:

a. All penetration testing of Apple Bank systems must be coordinated through the Chief Information Security Officer.
b. Identified vulnerabilities that could lead to penetration or exploitation must be retested after remediation; and
c. Penetration test summary reports must be distributed to the Chief Technology Officer and Chief Information Security Officer.

3.12 CUSTOMER REMOTE ACCESS TO FINANCIAL SERVICES

AFH offers remote banking services, and must implement appropriate authentication techniques commensurate with the risk from remote banking activities. Based on risk, AFH must implement additional layered security controls including a combination of the following:

a. Application time-outs with mandatory re-authentication;
b. Fraud detection and monitoring systems that include consideration of customer history, geographic locations and behavior to alert management, and enable a timely and effective Bank response;
c. Positive pay, debit blocks, and other techniques to appropriately limit the transactional use of the account;
d. Supplementary controls over certain account activities, such as transaction value limits, restrictions on devices for adding payment recipients, limits on the number of transactions and allowable payment windows (e.g., days and times);
e. Reputation-based tools to block connections to the institution's servers based on device or network indicators known or suspected to be associated with fraudulent activities;
f. Device authentication with appropriate enrollment and de-enrollment processes;
g. Policies for addressing customer devices identified as potentially compromised and identifying customers who may be facilitating fraud;
h. Controls over changes to account maintenance activities (e.g., address or password changes) performed by customers either online or through customer service channels;
i. Supplementary controls for system administrators who are granted privileges to set up or change system configurations of business accounts; and
j. Customer education to increase awareness of the fraud risk and effective techniques customers can use to mitigate the risk.

3.12.1 Third Party Controls

AFH must develop policies and procedures to identify, measure, mitigate, monitor, and report on significant security incidents to ensure the resilience of remote financial services. AFH must plan and coordinate with its third-party to improve the resilience of services in the face of cyber attacks. To prevent or minimize exposure to these incidents, AFH management must implement, when feasible, the following controls:

a. Monitoring threat alerts;
b. Monitor service availability and diagnose causes of reduced availability;
c. Monitor applications and network traffic for indicators of nefarious activity;
d. Design and implement applications to withstand application-level DOS;
e. Utilize distributed architecture;
f. Limit traffic (e.g., allow valid traffic and block known bad traffic by port or IP address);
g. Add bandwidth; and
h. Enable access to services through alternative channels.

3.13 CLOUD COMPUTING

Cloud Service Providers (CSP) used by Apple Bank must have the configuration, deployment, and management structures than can meet the Bank's security, privacy, and other requirements wherever possible in order to access or store AFH non-public information.

3.13.1 Preliminary Requirements

All cloud providers utilized by the Bank's systems that will access non-public information as defined in the AFH Information Security Policies must meet the minimum requirements outlined below:

a. Cloud providers must be able to comply with requirements as established within the relevant AFH Information Security Policy, including this document;
b. A security review of the cloud service must be conducted by AFH prior to the procurement of the service;
c. AFH must exercise due care and due diligence and conduct a thorough analysis of the provider's capabilities and security measures;
d. At a minimum, AFH must include (where possible), the contractual language identified in Information Security Policy (Subsection 3.7.7 *Third Party*);
e. Contracts should be re-evaluated upon any significant change to the CSP as a third-party entity (e.g., bought by another company, bankruptcy);
f. Where possible, AFH must negotiate with CSPs to allow for ongoing evaluation by the AFH to ensure that security measures are properly implemented and enforced;
g. Any violation of security measures affecting the security of AFH information or resources that is discovered by AFH must be communicated with the CSP as soon as possible after discovery so the CSP can address the concern; and
h. CSPs must be able to demonstrate compliance with applicable regulatory requirements such as Section 501(b) of the Gramm-Leach-Bliley Act of 1999, NYSDFS 23 NYCRR 500, PCI DSS, HIPAA, SOC1-Financial, SOC2-IT Controls and SOC3-Attestation).

3.13.2 Privacy and Security Controls for Cloud Hosting

AFH will assess a potential cloud service provider that will be accessing AFH managed non-public information to ensure the CSP can operate with any applicable capabilities and functionalities outlined below:

a. Ensure that cloud provider’s electronic discovery capabilities, processes, and policies do not compromise the privacy and security of accessing AFH managed non-public information hosted by the CSP;
b. Where possible, ensure hosted systems or services will allow AFH to monitor the services for uptime, availability and security functionality;
c. Ensure relevant safeguards are in place to secure authentication, authorization, and other identity and access-management functions in accordance with the requirements outlined in the Information Security Policy;
d. CSPs should certify that in multi-tenant offerings the structure or architecture of their systems are capable of isolating hosted data and operations from other tenants where possible;
e. Establish an SLA with the CSP for notification of service disruption as well as resumption of critical operations within an agreed upon time; and
f. Ensure that the cloud provider informs AFH within a reasonable time after a breach has been discovered that directly impacts the bank resources or information.

3.14 SUPPLY CHAIN SECURITY

AFH purchases a wide variety of hardware and software, which often is manufactured or developed internationally. AFH must identify factors that may increase risk from supply chain attacks and responds with appropriate risk mitigations. Security within the supply chain must be considered to limit the potential for harm through techniques tailored to specific acquisitions and services. The following must be considered and implemented when feasible:

a. Only making purchases through reputable sellers who demonstrate an ability to control their own supply chains;
b. Purchasing hardware and software through third parties to shield the Bank's identity;
c. Reviewing hardware for anomalies;
d. Using automated software testing and code reviews for software; and
e. Regularly reviewing the reliability of software and hardware items purchased through activity monitoring and evaluations by user groups.

3.15 EVENT AND INCIDENT MANAGEMENT

An incident management plan must be maintained to addresses security incidents and malfunctions. Event reporting and escalation procedures must be formalized. Incident scoring and prioritization schema must be developed based on the known or potential impact to the organization.

3.15.1 Incident Response Plan

The Bank must have an established, written Incident Response Plan (“IRP”) designed to promptly respond to, and recover from, any cybersecurity event materially affecting the confidentiality, integrity or availability of the Bank’s Information Systems or the continuing functionality of any aspect the Bank’s business or operations. The Incident Response Plan must address the following areas:

a. The internal processes for responding to a cybersecurity event;
b. The goals of the incident response plan;
c. The definition of clear roles, responsibilities and levels of decision-making authority;
d. External and internal communications and information sharing;
e. A detailed and current playbook for addressing specific scenarios and incidents;
f. The identification of requirements for the remediation of any identified weakness in Information Systems and associated controls;
g. Documentation and reporting regarding cybersecurity events and related incident response activities;
h. The evaluation and revision as necessary of the incident response plan following a cybersecurity event; and
i. The Incident Response Plan must be tested, at a minimum, annually.

3.15.2 Responsibility

Incident management responsibilities and procedures must be identified and documented. Individuals responsible for Event and Incident Management must be identified along with their respective back-ups and/or delegates.

Users of AFH systems must be made aware of the procedure for reporting breaches, threats or weaknesses that may have an impact on the security of AFH information systems and employees and third party users are required to report any observed or suspected security incidents to management as quickly as possible.

3.15.3 Reporting

Information security events/incidents will be reported through an approved channel and reviewed promptly by authorized employees. Response actions related to security incidents will adhere to a documented set of procedures, including appropriate communication and coordination of the following efforts:

a. The Chief Technology Officer and Chief Information Security Officer must be alerted as promptly as possible but not later than 24 hours for significant security incidents such as a breach of non-public information and/or disruption of services;
b. The IRP Team Leader will oversee these investigations and implement corrective actions, where needed, to reduce the risk of reoccurrence;
c. The IT Security Operations Team must complete a Root Cause Analysis (“RCA”) to be delivered to the Chief Technology Officer and Chief Information Security Officer and interim reporting throughout the duration of the incident; and
d. Weekly and monthly summary reports must be provided to the Chief Technology Officer and Chief Information Security Officer and interim reporting throughout the duration of the incident.

3.15.4 Suspicious Activity Reporting (SAR)

Information Security will submit egregious, significant, or damaging cyber events and cyber enabled crimes and cyber incidents to the Apple Bank Financial Crimes to determine if a Suspicious Activity Report (SAR) needs to be filed. To the extent available, involving cyber-incidents/events/crimes, the following should be include when submitted:

- Description and magnitude of the event
- Known or suspected time, location, and characteristics or signatures of the event
- Indicators of compromise
- Relevant IP addresses and their timestamps
- Device identifiers
- Methodologies used
- Other information the institution believes is relevant

3.15.5 Regulatory Incident Reporting

The Bank must notify the NYSDFS superintendent as promptly as possible but in no event later than 72 hours from a determination that a cybersecurity event has occurred as defined in NYSDFS 23 NYCRR.

The Bank must notify the FDIC as soon as possible when the Bank becomes aware of an incident involving unauthorized access to or use of non-public customer information.

The NYS Attorney General, the NYS Department of State's Division of Consumer Protection and the NYS Division of State Police must be notified in the most expedient time possible and without unreasonable delay. This delay must be consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system when New York residents’ private information is exposed.

3.15.6 Post Incident

Knowledge gained during the analysis of cybersecurity incidents must be captured, reviewed, and reported to the Chief Technology Officer and Chief Information Security Officer in order to identify corrective actions or control measures that may help address similar events in the future.

An “Incident Report” must be completed and provided to Information Security within three days of the investigation’s completion.

3.15.7 Collection of Evidence

When a follow-up action against a person or organization after an information security incident (either civil or criminal) is required, evidence must be collected, retained, and presented to conform to the rules for evidence prescribed by the appropriate authority in the relevant jurisdiction.

The Bank must ensure that their procedures comply with any published standard, or code of practice for the production of admissible evidence.

3.16 BUISNESS CONTINUITY AND RECOVERY PLANNING

Business continuity and disaster recovery plans must be implemented to guide recovery from cyber events or other major disruptions to business processes in a manner that maintains the security of AFH operations and ensures timely restoration. All affected staff must be made aware of the plans and their own roles within the plans.

3.16.1 Business Continuity Plan

The business continuity plan ("BCP") must include controls to identify and reduce risks, limit the consequences of cybersecurity incidents, and ensure the timely resumption of essential business processes. In addition, the following must be performed:

a. An annual business impact analysis must be completed to determine the critical AFH processes, legal and regulatory requirements, recovery time and recovery point objectives and the required resources; and
b. An annual risk assessment must be included to determine the impact of the threats on the business, the likelihood of occurrence, and the recovery time necessary for critical AFH systems.

3.16.2 Disaster Recovery Plan

A disaster recovery plan must be maintained for the recovery of critical information technology systems and data communications. It is also to guide recovery from security/cyber events or other major disruptions to business processes in a manner that maintains the cybersecurity/security of AFH operations and ensures timely restoration. All affected staff must be made aware of the plans and their own roles within the plans.

3.16.3 Testing

At least annually, critical components of the business continuity plan and disaster recovery plans must be tested. General objectives for the tests need to include determining the overall feasibility of the recovery strategies, verifying compatibility of hardware backup, identifying deficiencies in the plans and providing training for employees involved in the plans.

Both the Business Continuity and Disaster Recovery plans must be tested annually and a formal report must be issued to both the Chief Technology Officer ("CTO") and the Chief Information Security Officer ("CISO") documenting details and summarizing the success of the of the stated objectives for the tests.

3.16.4 Review and Update

Management must review and update the business continuity and disaster recovery plans annually and whenever there is a material change to the operations, structure, business or locations.

3.17 COMPLIANCE WITH INFORMATION SECURITY POLICY

AFH Management must ensure the implementation of the information Security Policy, Procedures and Manuals within their areas or responsibility. In addition, all departments within AFH will be subject to regular reviews to ensure compliance with security policies, procedures and standards.

4. Escalation Procedures

The Policy Owner will monitor this Policy. Any non-compliance with the Policy will be escalated to the Designated Management Committee for resolution. If the Designated Management Committee cannot resolve the issue, it will be escalated to the Executive Management Steering Committee ("EMSC") for further consideration. If the issue cannot be resolved by the EMSC the issue will be escalated to Board or Designated Board Committee for further consideration.

IV. REQUIRED PERIODIC REVIEW AND APPROVAL CYCLE

Required Annual (12 Month) Board Review and Approval Cycle (Policy Level 1)

The Policy Owner is responsible for initiating the Board review of the Policy on an Annual basis prior to the Next Board Review Date. The Policy Owner will track the Next Board Review Date for the Policy and begin the review process early enough to provide ample time for all necessary approvals to occur in a timely manner. All submissions for approvals should include a redline and clean copy of the updated Policy, with a summary of all substantive changes. The updated Policy does not go into effect until all steps listed below are complete. Steps for required Annual review are as follows:

a) The Policy shall be reviewed annually by the Policy Owner, in consult with the Legal Contact, and updated (if necessary).

b) The [updated] Policy shall be submitted to the Designated Management Committee for review.

c) If the Designated Management Committee cannot agree on an issue or a change to the Policy, it shall be submitted to the EMSC for consideration.

d) The Designated Management Committee shall review all revisions and recommend an updated Policy document to the Designated Board Committee (or the Board, as the case may be) for review and final approval. To the extent the Designated Management Committee is a sub-committee, prior to review by the Board or Designated Board Committee the updated Policy shall be reviewed by the primary management committee with oversight of the Designated Management Committee.

Once the steps above are complete and an updated Policy has been approved by the Designated Board Committee (or the Board, as the case may be), the updated Policy shall go into effect and the Policy Owner shall be responsible for delivering the approved Policy document to the Policies and Procedures Administrator ("PPA") within seven days of the approval date so that it can be loaded in a timely manner to AppleNet or such other intranet site where Policies are stored and made available to the employees of the Bank. The Next Board Review Date shall be adjusted accordingly.

If there are any questions about the above process contact Corporate Governance at corpsec@applebank.com.

V. OFF-CYCLE REVIEW AND APPROVAL PROCESS

Off-Cycle Policy Changes – Review and Approval Process (Policy Level 1)

If the Policy requires changes to be made outside the required Annual Board cycle noted in the previous section, review and approval shall follow the following steps:

a) The Policy shall be updated by the Policy Owner, in consult with the Legal Contact.

b) If the changes are **Immaterial Changes** (i.e., no change to any substance of the policy, but rather grammar, formatting, template, typos, etc.), such changes shall be submitted to the Designated Management Committee for approval and no further approval is required. A record of all such changes shall be kept and submitted for reference to the Designated Board Committee (or the Board, as the case may be) during the required Annual approval cycle (or the next time the Policy requires interim Board approval, whichever comes first).

c) If the changes are **Material Changes** (i.e., changes that would materially alter the substance of the Policy in any way), the revised Policy shall be submitted to the Designated Management Committee for approval and recommendation to the Designated Board Committee (or the Board, as the case may be) for final approval. Final approval by the Designated Board Committee in this instance shall be required. To the extent the Designated Management Committee is a sub-committee, prior to review by the Board or Designated Board Committee the updated Policy shall be reviewed by the primary management committee with oversight of the Designated Management Committee.

d) If the Designated Management Committee cannot agree on an issue or a change to the Policy, it shall be submitted to the EMSC for consideration.

Once the steps above are complete and the Policy has received final approval by either the Designated Management Committee or the Board or Designated Board Committee, as the case may be, the updated Policy shall go into effect and the Policy Owner shall be responsible for delivering the approved Policy document to the PPA within seven days of the approval date so that it can be loaded in a timely manner to AppleNet or such other intranet site where Policies are stored and made available to the employees of the Bank. The Next Management Review Date and Next Board Review Date shall be adjusted accordingly.

If there are any questions about the above process contact Corporate Governance at corpsec@applebank.com.

VI. DESIGNATED COMMITTEES AND POLICY LEVEL REVIEW

Risk Management, in conjunction with Legal, identifies the Designated Management Committee, Designated Board Committee (or the Board, as appropriate), and Policy Level for this Policy, and re-evaluates the same at least annually. Changes, if any, will be communicated to the Policy Owner, who shall update the Policy accordingly, as well as the PPA.

VII. EXCEPTIONS TO THE POLICY

Requests for exceptions to this Policy must be specific and may only be granted on specific items, rather than to entire sections. AFH staff will communicate their exception requests in writing to the Policy Owner, who will then present the request to the Designated Management Committee for consideration.

VIII. ROLES AND RESPONSIBILITIES

The key roles and responsibilities for this Policy are summarized below:

Designated Board Committee: The Designated Board Committee provides general oversight over management's administration of the Policy. The Designated Board Committee is responsible for initially approving this Policy and reviewing the Policy on an annual basis according to the Policy Level (*refer to the Review and Tracking Chart*).

Designated Management Committee: The Designated Management Committee is responsible for reviewing and approving changes to the Policy as set forth herein on an annual basis (except in the year designated for Board approval) and submitting material changes to the Designated Board Committee, or Board, as appropriate.

Executive Management Steering Committee ("EMSC"): The EMSC is the primary management team of the Bank and is responsible for reviewing the Policy, as needed per the relevant sections of this Policy.

Chief Executive Officer ("CEO"): The CEO is ultimately responsible for and assumes ownership and leadership of the strategic planning process and ongoing reporting to the board of directors. The CEO establishes the "direction at the top" that affects integrity, ethics and other factors of the internal AFH environment. The CEO coordinates the process of aligning strategic planning with AFH's risk appetite and risk strategy and monitors the way senior management manages the businesses.

Chief Technology Officer ("CTO"): The CTO and his designated representatives are responsible for creating and reviewing new and updated policies and to provide effective challenge of Management policies and procedures.

Chief Information Security Officer ("CISO"): The CISO is a qualified individual responsible for overseeing and implementing the organization's cybersecurity program and enforcing its cybersecurity policy. The CISO is to report on the cybersecurity program and material cybersecurity risks, including: the confidentiality of Non-Public Information and the integrity and security of the Bank's Information Systems, the cybersecurity policies and procedures, material cybersecurity risks to the Bank, overall effectiveness of the cybersecurity program and material Cybersecurity Events.

Senior Management: The management and business units are responsible for implementing this Policy, ensuring compliance and understanding of this Policy as well as developing procedures for his/her unit, to the extent needed, that align with the requirements of this Policy. Management is also responsible for running the day-to-day operations of the Bank in compliance with applicable laws, rules, regulations and the principles of safety and soundness. This responsibility includes implementing appropriate policies and business objectives. Senior management will anticipate changes in the internal and external environment and proactively respond to changing circumstances. Senior management will be results-oriented but not at the expense of sound banking practices.

Policy Owner: *See Section II – Definitions*.

Risk Management: Risk Management, in conjunction with Legal, determines the initial Designated Management Committee, Designated Board Committee (or Board, as appropriate), and Policy Level of the Policy, and re-evaluates the same at least Annually.

Policies and Procedures Administrator ("PPA"): *See Section II – Definitions*.

Legal Contact: *See Section II – Definitions*.

Internal Audit ("IA"): The internal audit team is responsible for the periodic audit of this Policy. Internal Audit will review the processes and any related gaps will be identified as findings to be monitored and remediated.

Risk Management ("RM"): The CRO and the Risk Management team are responsible for the ongoing review of this policy and for conformance with AFH Risk Tolerance, Risk Appetite and mitigation of Risk Exposure.

Information Security: The Information Security management team leads or participates in the development, enforcement, and maintenance of policies, procedures, measures, and mechanisms to protect the confidentiality, integrity and availability of information and to prevent, detect, contain, and correct information security breaches by aligning information security policy and compliance with statutory, industry published security standards and regulatory requirements.

Management and Business Units: The management and business units are responsible for ensuring compliance and understanding of this Bank policy as well as developing procedures that align with the requirements of this Policy. Management decisions must not be inconsistent with this or any other approved Bank policy and/or procedures.

Bank Personnel: All Bank personnel are responsible for executing their duties so that they are aligned with the Bank's overall goals and objectives and that they comply with this and all Bank policies and procedures.

IX. RECORD RETENTION

Any records created as a result of this Policy should be held for a period of 7 years pursuant to the Bank’s Record Retention Policy. Should records created as a result of this Policy require a different retention period (either a shorter or longer time period), the Policy Owner (in conjunction with the relevant business area leader) must describe the rationale for a different retention period and share the rationale with the Designated Management Committee.

X. QUESTIONS AND CONTACT INFORMATION

Questions regarding compliance with this Policy may be addressed to the Policy Owner listed in the tracking chart on the first page.

XI. APPENDIX A

Information Security & Information Technology

Lines of Defense

August 2019

Contents

1. Introduction

The Bank conducted the required analysis to determine the Information Security Department's structure, required staffing levels, and job descriptions that include duties and responsibilities.

2. Implementation of Three Lines of Defense

First Line: Management owns and manages the data, processes, risks, and controls. Business units need to develop processes, procedures, and controls with guidance from risk management designed to mitigate the risks associated with their activities.

Second Line: The Bank's Information Security Department and Risk Management is responsible for overseeing the Bank's risk-taking activities and working with business units to create a security management program. The program must include frameworks, developing policies and procedures, defining KRIs and metrics, creating risk assessments, providing information security training, monitoring business unit activities, and reporting to management and the Board.

Third Line: Internal Audit ensures that the bank's security framework and internal controls are appropriate and effective. The function also evaluates security standards within the business units and reports findings to the Board or audit committee.

3. Information Security Policies

The Information Security Role is defined in each of the IT Polices and is scheduled to be approved in September 2019 as follows:

CISO and Information Security: The CISO and the Information Security Department as required by the New York State Department of Financial Services 23 NYCRR 500 Cybersecurity will provide effective oversight and governance to ensure that all Information Security policies, processes and procedures are being adhered to for the purposes of system acquisition, development, and maintenance. This includes, but is not limited to, roles and responsibilities, operations, monitoring and/or other key components as set forth in the Information Security policy.

4. Information Technology Security Effective Challenge Framework

Information Technology Policies and Procedures have been enhanced to include Information Technology and Information Security implementation of an Effective Challenge framework for providing critical analysis. Effective challenge involves utilizing objective, informed parties who can identify limitations and assumptions and who can produce appropriate changes.

5. Information Technology Security

The Information Technology Security (IT Security) Team is the first line of defense and has responsibility for effectively challenging operational staff in all aspects of IT Security which includes the maintenance and configuration of infrastructure and software; and the deployment, approval, development, security monitoring and operations of the Information Security Program.

The IT Security Team is responsible for implementing and remediating security issues identified through assessment and reviews conducted by Regulators, Internal/External Auditors, RM, and Information Security.

6. Chief Information Security Officer (CISO)

The Chief Information Security Officer (CISO) is responsible for overseeing and reporting on the management and mitigation of information security risks across the enterprise

This responsibility includes establishing policy and overseeing information technology's security environment. Satisfying the Interagency Guidelines Establishing Information Security Standards, which were issued pursuant to the Gramm-Leach-Bliley Act (GLBA).

The CISO will assist Information Technology in remediating security issues identified by Regulators, Internal/External Auditors, RM and Information Security.

7. Information Security Roles and Responsibilities

Information Security and Monitoring Plan, RACI (Responsible, Accountable, Consult, Inform)

Key Activities based	Information Technology	Information Security
Oversight		
1. Present Information Security information at Board meetings, advise senior management and conduct staff oversight	C, I	R, A
Monitoring		
2. Data Leakage Program (DLP) monitoring	R, A	C, I
3. Intrusion Detection and Prevention System (IDS/IPS) monitoring	R, A	C, I
4. System Information and Event (SIEM) monitoring	R, A	C, I
Vulnerability Management		
5. IT vulnerability patches assessed, tested, implemented and reported	R, A	C, I
Access Management		
6. IT User access reviews	R, A	C, I
7. Third Party Account reviews	R, A	C, I
8. Privileged access reviews	R, A	C, I
9. Privileged User training (Annually)	C, I	R, A
Security Policy and Training		
10. User Security training (Annually)	C, I	R, A
11. External Security training	C, I	R, A
12. Security Awareness development	C, I	R, A
13. Internal Security Awareness training	C, I	R, A
System and Network Security		
14. Network Diagram refresh review	R, A	C, I
15. Network Security Scanning	R, A	C, I
16. Firewall Rule Request review	R, A	C, I
17. Network Segregation review	R, A	C, I
18. System Logging review	R, A	C, I
19. Log Retention review	R, A	C, I
20. File Share monitoring	R, A	C, I
21. Network Penetration testing	R, A	C, I
22. Hardware and Software inventory review (Criticality/Sensitivity)	R, A	C, I
Service Provider Security		
23. IT Service Provider Security review	C, I	R, A
24. Issue Identification	C, I	R, A
25. Issue Mitigation review	C, I	R, A

Key Activities based	Information Technology	Information Security
KPI/KRI		
26. Review and challenge of IT Key Security Performance Indicators	C, I	R, A
Assessments		
27. Data Center Physical/IT Security assessment	C, I	R, A
28. Cyber Security Risk assessments	C, I	R, A
29. Infrastructure Security Risk assessments	C, I	R, A
30. Application Security Risk assessments	C, I	R, A
31. Vendor Security Risk assessments	C, I	R, A
32. IT Secure Media Handling review	R, A	C, I
33. Cloud Application and Infrastructure Security Risk assessment	C, I	R, A
34. Legal & Compliance Privacy (GLBA & Red Flag) review	R, A	C, I
35. Remote Access review	R, A	C, I
36. Secure Change management review	R, A	C, I
37. Business Continuity plan review	R, A	C, I
38. Disaster Recovery plan review	R, A	C, I
39. Back-up and recovery status	R, A	C, I
40. Data Security compliance (Clean Desk/Electronic Retention)	C, I	R, A
Incident Management		
41. IT Security Incident management	R, A	C, I
42. Cyber Incident response	R, A	C, I
43. Cyber Incident recovery plan	R, A	C, I

Board Presentation		
44. Board presentation on Cybersecurity Risk appetite/Insurance review	C, I	R, A
45. Board presentation on Threat, Risk, Vulnerability Assessment and IT Security project status	C, I	R, A
Information Security Program Testing		
46. Perform Information Security Program Testing	C, I	R, A