Apple Financial Holdings, Inc.

Cybersecurity Policy

December 19, 2019

Table of Contents

POLICY NAME: Cybersecurity 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

I. POLICY PURPOSE STATEMENT AND SCOPE

The Cybersecurity Policy (the "Policy") applies to the development, 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.

All Departments, at a minimum, must achieve the security level required by this Cybersecurity 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

- **Affiliate:** Any Person that controls, is controlled by or is under common control with another Person. For purposes of this subsection, control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of stock of such Person or otherwise.

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

- **Authorized User:** Any employee, contractor, agent or other Person that participates in the business operations of a Covered Entity and is authorized to access and use any Information Systems and data of the Covered Entity.

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

- **Covered Entity:** Any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law.

- **Cybersecurity Event:** Any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.

- **Effective Challenge:** An over-arching, guiding business principle is that of "effective challenge" of all key business processes: that is, critical analysis performed 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.

- **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.

- **Information System:** A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

- **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.

- **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.

- **Multi-Factor Authentication:** 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 Publicly Available Information and is:

  a. Business related information of a Covered Entity 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 the Covered Entity;
  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:

     i. Social Security number,
     ii. Drivers' license number or non-driver identification card number,
     iii. Account number, credit or debit card number,
     iv. Any security code, access code or password that would permit access to an individual's financial account, or
     v. 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:

     i. The past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family,
     ii. The provision of health care to any individual, or
     iii. Payment for the provision of health care to any individual.

- **Penetration Testing:** A test methodology in which assessors attempt to circumvent or defeat the security features of an Information System by attempting penetration of databases or controls from outside or inside the Covered Entity's Information Systems.

- **Person:** Any individual or any non-governmental entity, including but not limited to any nongovernmental partnership, corporation, branch, agency or association.

- **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.

- **Publicly Available Information:** Any information that a Covered Entity 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.

    a. For the purposes of this subsection, a Covered Entity has a reasonable basis to believe that information is lawfully made available to the general public if the Covered Entity has taken steps to determine:

        i. That the information is of the type that is available to the general public; and
        ii. 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.

- **Risk Assessment:** Refers specifically to the risk assessment that each Covered Entity is required to conduct under NYCRR 500.09.

- **Risk-Based Authentication:** any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a Person and requires additional verification of the Person's identity when such deviations or changes are detected, such as through the use of challenge questions.

- **Senior Officer(s):** Senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of a Covered Entity, including a branch or agency of a foreign banking organization subject to this Part.

- **Third Party Service Provider(s):** A Person that:

    a. Is not an Affiliate of the Covered Entity,
    b. Provides services to the Covered Entity, and
    c. Maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity.

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

III. KEY POLICY COMPONENTS

1. EXECUTIVE SUMMARY

The Cybersecurity Policy (the “Policy”) applies to the development, 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 Policy represents the Board of Directors and Senior Management’s recognition of the risks and importance of establishing a Cybersecurity policy that adequately protects the information assets at all times ensuring the security and confidentiality of customer and Bank information.

Cybersecurity is the process of protecting customer and Bank information by preventing, detecting, and responding to attacks. AFH manages internal and external threats and vulnerabilities to protect information assets and the supporting infrastructure from technology-based attacks. In light of the increasing volume and sophistication of cybersecurity threats, AFH focuses on cybersecurity preparedness in assessing the effectiveness of the overall information security program. AFH implements a defense-in-depth program to protect, detect, and respond to cyber threats.

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 and additionally reflects industry best practices.

2. OBJECTIVES

The goal of this Policy is to protect the confidentiality, integrity and availability of the Bank’s information systems, identify, and assess internal and external cybersecurity risks that may threaten the security or integrity of Non-Public Information stored on the Bank’s Information Systems;

AFH’s utilizes defensive infrastructure and implements policies and procedures to protect the Bank’s Information Systems and the Non-Public Information stored on those Information Systems:

a. From unauthorized access, use or other malicious acts;
b. Detect security events;
c. Respond to identified or detected security events to mitigate any negative effects;
d. Recover from security events and restore normal operations and services; and
e. Fulfill applicable regulatory reporting obligations.

This Cybersecurity Policy is a high-level policy in regards to cybersecurity specifically, which compliments the AFH Information Security Policy. The Information Security Policy provides more granularity and addresses the aspects of non-digital information (e.g., disposal of printed documents containing Sensitive or Non-Public Information).

3. KEY COMPONENTS OF POLICY

The Cybersecurity Policy must be based on the Bank's Risk Assessments and address the following areas in the Bank's day-to-day operations:

f. Information Security;
g. Risk Assessments;
h. Data Governance & Classification;
i. Asset Inventory and Device Management;
j. Access Controls and Identity Management;
k. Systems Operations and Availability Concerns;
l. Systems and Network Security;
m. System and Network Monitoring;
n. Systems and Application Development and Quality Assurance;
o. Physical Security and Environmental Controls;
p. Customer Data Privacy;
q. Vendor and Third Party Provider Management;
r. Incident Response; and
s. Business Continuity/Disaster Recovery Planning and Resources.

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.

3.1 THREATS, VULNERABILITIES AND RISKS

The Bank identifies cyber related threats, risks and vulnerabilities. Cyber risk identification produces groupings of threats. A classification for categorizing threats, sources, and vulnerabilities can help support the risk identification process.

Risk is the potential that events, expected or unanticipated, may adversely affect the Bank's earnings, capital, or reputation. Risk is considered in terms of categories, one of which is operational risk. Operational risk is the risk of failure or loss resulting from inadequate or failed processes, people, or systems;

A threat can be a natural occurrence, technology or physical failure, a person with intent to harm, or a person who unintentionally causes harm. Information about threats is available from public and private sources

A technical vulnerability can be a flaw in hardware, firmware, or software that leaves an information system open to potential exploitation. These flaws provide opportunities for hackers to gain access to a computer system.

These threats, vulnerabilities and risks are mitigated via Cybersecurity, Business Continuity/Disaster Recovery and Pandemic Plans, Data Security and Network Security, a clean desk policy and proper disposal of information.

3.2 CHIEF INFORMATION SECURITY OFFICER

The Bank designated the Chief Information Security Officer ("CISO"), a qualified individual responsible for overseeing the cybersecurity program and enforcing its cybersecurity policy and designated the Chief Technology Officer for implementing the cybersecurity program and the cybersecurity policy.

The CISO must report in writing at least annually to the board of directors or equivalent governing body. The CISO must report on the cybersecurity program and material cybersecurity risks. The CISO must consider to the extent applicable:

a. The confidentiality of Non-Public Information and the integrity and security of the information systems;
b. The cybersecurity policies and procedures;
c. Material cybersecurity risks to the Bank;
d. Overall effectiveness of the cybersecurity program; and
e. Material cybersecurity events involving the Bank during the time period addressed by the report.

3.3 INFORMATION SECURITY POLICY

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:

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

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 the Information Security Policy needs to ensure AFH information is properly safeguarded. The policy would apply to all AFH staff, vendors, and contractors who have access to AFH information.

In addition, the Information Security policy must ensure that information and information systems comply with all applicable banking laws and regulations such as Gramm-Leach-Bliley Act (GLBA), New York State Department of Financial Services 23 NYCRR 500 (Cybersecurity Requirements For Financial Services Companies) and/or industry standards.

3.4 RISK MANAGEMENT

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.

Annually, the Bank completes 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.

3.5 DATA CLASSIFICATION

Data is a critical asset of AFH. All personnel have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored or used by AFH, irrespective of the medium on which the data resides and regardless of format. A Data Classification Policy must be implemented to provide guidance in classifying and protecting this data.

3.6 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.

3.7 CYBERSECURITY PERSONNEL & INTELLIGENCE

The Bank must utilize qualified cybersecurity personnel (including Third Party Providers) to manage the Bank’s cybersecurity risks to perform or to oversee the performance of core cybersecurity functions.

The Bank must provide cybersecurity personnel with training and updates in order to address relevant cybersecurity risks and verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

3.8 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 and to reflect risks identified by the Bank’s Risk Assessment.

3.9 IDENTITY MANAGEMENT

For all applications and systems, users must be required to authenticate themselves with a unique user account and an authentication mechanism such as password, token, biometric, etc.

3.10 ACCESS CONTROLS

AFH must ensure authentication and authorization controls are appropriately for the risk that exists for the data and application. Application and system access will not be granted to any user without the appropriate approval.

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.

A formal user management process, which includes a sign-off by an authorized requestor, must be implemented.

3.10.1 Access Privileges

Users will only receive access to the minimum applications and privileges required to perform their job function and the Bank must limit user access privileges to Information Systems that provide access to Non-Public Information and must review such access privileges on a quarterly basis.

3.10.2 Multi-Factor Authentication

Based on its risk assessments, the Bank must use effective controls, which may include Multi-Factor Authentication or risk-based authentication to protect against unauthorized access to Nonpublic Information or Information Systems.

Multi-Factor Authentication ("MFA") must be utilized for any individual accessing the Bank's internal network from an external network.

3.11 PHYSICAL SECURITY AND ENVIRONMENTAL CONTROLS

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

3.11.1 Mobile Storage Media

The ability for users to use mobile storage media along with auto run features 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.

3.11.2 Mobile Devices

Non-Public Information must not be stored on mobile devices, unless necessary and if so, it must always be encrypted.

3.11.3 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.

3.11.4 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.

3.11.5 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.

3.11.6 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.

3.11.7 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.

3.11.8 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.

3.11.9 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.

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

3.12 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.

3.12.1 Privacy

Employees must protect the individual's Non-Public Information throughout the data lifecycle (see the Apple Bank Privacy Policy).

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.

3.13 LIMITATIONS ON 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.

3.14 ENCRYPTION OF NON-PUBLIC INFORMATION

3.14.1 Electronic Files at Rest

Based on risks, the Bank must implement controls, including encryption, to protect electronic files containing Non-Public Information at rest. As of September 1, 2018, All electronic files containing Non-Public Information at rest must be be secured by encryption. If encryption is not feasible, the Chief Information Security Officer must approve compensating controls.

3.14.2 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, the Chief Information Security Officer must approve compensating controls.

To the extent that the Bank is utilizing the above compensating controls, it must be reviewed by the CISO annually, at a minimum.

3.15 THIRD PARTY SERVICE PROVIDER POLICY

The Bank must implement written policies and procedures designed to ensure the security of Information System and Non-Public Information that are accessible, or held by the Third Party Service Providers. The policies and procedures should be based on a Risk Assessment, which must evaluate:

a) The identification and risk assessment of Third Party Service Providers;
b) Minimum cybersecurity practices required to be met by such Third Party Service Provider in order to them to do business with the Bank;
c) Due diligence processes must be used to evaluate the adequacy of cybersecurity of such Third Party Service Provider; and
d) Periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.

Policies and procedures must include relevant guidelines for due diligence and contractual protections relating to the Third Party Service Provider including the extent of applicable guidelines addressing:

a) The Third Party Service Provider's policies and procedures for access control, including its use of multi-factor authentication, to limit access to relevant Information Systems and Non-Public Information;
b) The Third Party Service Provider's policies and procedures cover the use of encryption to protect Non-Public Information in transit and at rest;
c) A notice is to be provided to the Bank in the event of a cybersecurity event directly impacting the Bank's Information Systems or the Bank's Non-Public Information being held at the Third Party Service Provider; and
d) Representations and warranties addressing the Third Party Service Provider's cybersecurity policies and procedures that relate to the security of the Bank's Information Systems or Non-Public Information.

3.16 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.

3.17 APPLICATION SECURITY

The Bank must include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Bank and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Bank within the context of the Bank's technology environment.

3.18 OPERATIONS AND AVAILABIILITY

Responsibilities, processes and procedures must 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 must be treated as formal documents with changes authorized by the management.

3.19 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. User must only be granted the least privileges to perform their tasks. The network perimeter must be configured to deny all activity that is not expressly permitted. Operational responsibilities for the AFH network must be separated from computer operations, where appropriate.

To ensure appropriate network security, management must maintain accurate network diagrams and store them securely, providing access only to authorized personnel. These diagrams must identify hardware, software, and network components, internal and external connections, and types of information passed between systems to facilitate the development of a defense-in-depth security architecture.

3.20 MONITORING

The Bank must implement risk-based controls designed to monitor the activity of authorized users and detect unauthorized access, or use of, or tampering with, Non-Public Information by such authorized users.

3.21 PENETRATION TESTING AND VULNERABILITY ASSESSMENTS

Monitoring and testing must be developed in accordance with the Bank's risk assessment, designed to assess the effectiveness of the Bank's cybersecurity program. The monitoring and testing must include continuous monitoring or periodic penetration testing and vulnerability assessments.

Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, the Bank must:

Annual Penetration Testing of the Information Systems determined each given year based on relevant identified risk in accordance with the risk assessment; and

At least, monthly vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publically known cybersecurity vulnerabilities in the Bank's information system based on the risk assessment.

3.22 LOGGING

Logs recording exceptions, user activities, security violations, system alerts or failures and changes to or attempts to change system settings must be maintained.

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.

3.23 AUDIT TRAILS

Audit records must be kept available to assist in the reconstruction of material financial transactions and to detect and respond to cybersecurity events.

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.

3.24 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.

3.25 NOTICES TO SUPERINTENDENT

The Bank must notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a cybersecurity event has occurred that is either of the following:

a) Cybersecurity event impacting the Bank in which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or
b) Cybersecurity event that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Bank.

The Bank must submit a written statement to the superintendent covering the prior calendar year. The statement must be submitted by February 15th, in such form set forth as Appendix A, certifying that the Bank is in compliance with the requirements set forth in NYDFS 23 NYCRR 500.

The Bank must maintain for examination by NYDFS all records, schedules and data supporting this certificate for a period of five years. To the extent that a Bank has identified areas, systems or processes that require material improvement, updating or redesign, the Bank must document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be made available to the Superintendent.

3.26 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

3.27 BUSINESS CONTINUITY AND RECOVERY PLANNING

Business continuity and disaster recovery plans ("BCP/DR") 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.

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.

3.28 COMPLIANCE WITH CYBERSECURITY POLICY

AFH Management must ensure the implementation of the Cybersecurity 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, standards and manuals.

IV. 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.

V. 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 must be reviewed Annually by the Policy Owner, in consult with the Legal Contact, and updated (if necessary).

b) The [updated] Policy must 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 must be submitted to the EMSC for consideration.

The Designated Management Committee must 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 must 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 must go into effect and the Policy Owner must 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 must be adjusted accordingly.

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

VI. 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 must follow the following steps:

The Policy must be updated by the Policy Owner, in consult with the Legal Contact.

a) 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 must be submitted to the Designated Management Committee for approval and no further approval is required. A record of all such changes must 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).

b) If the changes are **Material Changes** (i.e., changes that would materially alter the substance of the Policy in any way), the revised Policy must 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 must 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 must be reviewed by the primary management committee with oversight of the Designated Management Committee.

c) If the Designated Management Committee cannot agree on an issue or a change to the Policy, it must 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 must go into effect and the Policy Owner must 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 must be adjusted accordingly.

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

VII. 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 must update the Policy accordingly, as well as the PPA.

VIII. 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.

IX. 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.

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 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.

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's policies and procedures.

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.

Risk Management ("RM"): Risk Management ("RM"), 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.

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 Unit: 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.

Policy Owner: *See Section II – Definitions*.

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

Legal Contact: *See Section II – Definitions*.

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.

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.

X. 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.

XI. 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.