Apple Financial Holdings, Inc.

Bring Your Own Device(“BYOD”)Policy

June 24, 2020

Contents

REVIEW AND TRACKING CHART

Effective Date:	June 24, 2020
Version Number:	1.0
Policy Level:	Policy Level 2
Corresponding Board Review Frequency:	Biennial (Every 24 Months)
Board or Designated Board Committee:	Board Risk Committee
Last Board Review Date:	June 24, 2020
Next Board Review Date:	June 2022
Designated Management Committee:	Management Risk Committee
Last Management Review Date:	June 11, 2020
Next Management Review Date:	June 2021
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 Bring Your Own Device ("BYOD") Policy (the "Policy") applies to the implementation, management, monitoring, and compliance with information security requirements for non-Bank issued mobile devices 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 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

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

- **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.

- **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.

- **Policy Level 2:** A Regular Board Review Cycle level for a Policy, designated by Risk Management in consult with Legal. Level 2 policies require Biennial 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.

- **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 2.

- **Bank Data:** Information that belongs to the Bank which may be accessed by a Mobile Device through email and other authorized Bank systems and includes, without limitation, business and financial records, intellectual property assets, and personal data relating to customers, employees, or others.

- **BYOD User:** Employees who acknowledge and agree to the terms and conditions in the BYOD Use Agreement, which affords them the opportunity to use their own Mobile Devices for business purposes (in particular, access to the Gmail application).

- **Terms and Conditions:** Access and use is subject to the Minimum Security Requirements, which include obligations of the BYOD User such as maintaining the original Mobile Devices' operating system provided by the Mobile Device's manufacturer, by keeping the Mobile Device current with security patches and updates as released by the Mobile Devices' manufacturer, and also, signing of the relevant agreements before having access granted.

- **Minimum Security Requirements:** The technical and procedural requirements outlined that the BYOD User must comply with to maintain their device's enrollment in the mobile device management ("MDM") solution, which allows the BYOD User's Mobile Device to access Bank Data.

- **Mobile Device:** A personal portable, wireless computing device that is small enough to be used while held in the hand, such as smartphone, computer tablet, PDA, etc., which is authorized by the Information Technology ("IT") Department for business purposes to access and use Bank Data. The Mobile Device must be acquired voluntarily without payment by the Bank and be used without any expectation of reimbursement for any costs related to the purchase, activation, service or repairs, or other costs that may be incurred related to the device or its use.

- **Mobile Device Management ("MDM"):** A technology industry term for the administration of mobile devices (*e.g.*, smartphones, tablets). MDM solutions typically are implemented by the use of a third party application that has management features for mobile devices.

  A MDM solution typically has a combination of on-device applications and configurations, corporate policies and certificates, and backend infrastructure for the purpose of simplifying and enhancing the IT management of end user Mobile Devices. These solutions are typically cloud-based solutions with an emphasis on supporting and administering a BYOD Program in a consistent and scalable manner. Core functions of a MDM solution include: segregation of corporate data, securing emails and corporate documents on Mobile Devices, enforcing corporate policies, monitoring security configurations of end user's Mobile Devices and offering solutions for when a device is lost/stolen (*e.g.*, remote-wipe capabilities of Downloadable App and App Manager).

- **Downloadable App:** The Bank will provide you with access to an approved downloadable software application(s) (collectively and individually, referred to as the "Downloadable App") that will allow you to access your work-related emails, contacts, calendar and certain other Bank system applications made accessible by the Bank on your Device. The Bank has procured the Downloadable App from a third-party provider that may process some or all of the information described in the Program Terms. You are responsible for downloading and installing the Downloadable App on your Device.

- **App Manager:** Certain device-management programs (collectively and individually, referred to as the "App Manager") are included when you install the Downloadable App. By downloading the Downloadable App, you agree to it being installed on your Device and that you will be bound by the disclosures of terms and conditions presented to you.

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

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

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

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

- **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.

- **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

The acronym BYOD ("Bring Your Own Device") refers to the ability of AFH to allow its employees who acknowledge and agree to the terms and conditions below (collectively, "BYOD Users") the opportunity to use their own smart phones, tablets, and other mobile devices for business purposes to remotely access and use Bank Data via email and other Bank systems, as deemed appropriate by the BYOD Use Agreement. Access and use is subject to the below terms and conditions (collectively, "Terms and Conditions").

2. Objective

The objective of this Policy is to establish a standardized and consistent approach to secure both the Mobile Device and the Bank Data accessed, processed, used, stored, transferred, and handled via the Mobile Device.

3. Key Components of Policy

a. Permitted Users

Authorized employees may use personally owned Mobile Devices to connect to the Bank's systems provided they meet security standards and connectivity requirements established from time to time by the Bank's Information Technology ("IT") Department. Only those employees with a documented approval by their Department Manager will be permitted to use their Mobile Device to access the Bank's systems. Participation in the Bank's BYOD Program is voluntary; however, once approved to participate in the BYOD Program, the employee must abide by this Policy, the requirements set forth in the Bank's Bring Your Own Device Use Agreement ("BYOD Use Agreement"; see Appendix 1) and other policies referenced herein for as long as such employee is enrolled in the BYOD Program (as defined by the "BYOD Use Agreement").[1] Failure to comply with this BYOD Policy, the BYOD Use Agreement or any other applicable Bank policies may lead to corrective actions including, but not limited to, termination of an employee's participation in the BYOD Program, and additional disciplinary actions, up to and including termination of employment.

Employees are expected to follow all other Bank policies while participating in the BYOD Program including, without limitation, the Bank's Code of Conduct and Acceptable Use Agreement.

BYOD Users will only be granted access to Bank Data if the following requirements are met:

a. BYOD User is in compliance with both the Acceptable Use Agreement and Code of Conduct;
b. BYOD User's Mobile Device must be compliant with the "Minimum Security Requirements"; and
c. BYOD User must complete and sign the "BYOD Use Agreement" and adhere to any requirements or instructions contained therein.

[1] Although an employee's use of a personally owned Mobile Device for connection to the Bank's systems is voluntary, a Department Head can require an employee to use their personally owned Mobile Device for Bank related phone calls. To the extent an employee is required to use of a personally owned Mobile Device for Bank related phone calls, the employee will be provided a monthly reimbursement supplement that will be determined at the sole discretion of the Bank.

See Appendix 2 for “Control Reference(s)”

b. End User - Minimum Security Requirements

Mobile Devices must meet the “Minimum Security Requirements” in order to be enrolled in the BYOD Program.

The “**Minimum Security Requirements**” for Mobile Devices are:

a. Password-Protected Access for the Downloadable App and App Manager using either a Personal Identification Number (PIN #), Password, Pattern or Biometrics-based authentication mechanism;
b. The BYOD User must maintain the original Mobile Devices’ operating system provided by the device’s manufacturer by keeping the Mobile Device current with security patches and updates as released by the Mobile Devices’ manufacturer;
c. The BYOD User will not “jail break” or “root” the Mobile Device (install software that allows the user to bypass the standard built-in security features and controls) or otherwise modify safeguards installed in the Mobile Device by the device’s manufacturer.

c. AFH Mobile Device Security Controls

Information Security will define the security controls to be implemented on Mobile Devices via the MDM platform. These will include, at a minimum, the following:

a. Segregation of AFH data from non-AFH data;
b. Remote wipe capabilities for AFH data;
c. Methods to detect and prevent connectivity from devices without strong authentication enforced;
d. Methods to detect and prevent connectivity from devices with operating systems not patched to the appropriate level; and,
e. Methods to detect and prevent connectivity from “jail broken” or “rooted” devices.

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

(A) Required Biennial (24 Month) Board Review and Approval Cycle

The Policy Owner is responsible for initiating a regular Board review of the Policy on a Biennial (every 24 months) basis prior to the Next Board Review Date ("Regular Board Review Cycle"). 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 Biennial review are as follows:

a) The Policy shall be reviewed biennially 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 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 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.

(B) Required Annual (12 Month) Management Review

The Policy Owner is responsible for initiating an Annual review of the Policy outside the Regular Board Review Cycle. The Policy Owner will track the 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 Policy, with a summary of all substantive changes. The 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) If the changes are **Immaterial Changes** (i.e., no change to any substance of the policy, but rather grammar, formatting, template, typos, etc.), or **Material Changes** that do not alter the **scope and purpose** of the Policy or do not **lessen a requirement** for transactions or actions governed under the Policy (e.g., lowering a loan review threshold from $5k to $3k), such changes shall be submitted to the Designated Management Committee for final 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 Regular Board Review Cycle (or the next time the Policy requires interim Board approval, whichever comes first).

c) If the changes are **Material Changes** that alter the **scope and purpose** of the Policy or **lessen a requirement** for transactions or actions governed under the Policy (e.g., lowering a loan review threshold from $5k to $3k), then:

   i. The Policy shall be submitted to the Designated Management Committee for review and approval. 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.

   ii. 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 the updated Policy has received final approval by either the Designated Management Committee or the Board or the 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 Board Review Date and Next Management Committee 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

If the Policy requires changes to be made outside the Required Board Review Cycle outlined in the previous section, review and approval shall follow the Required Annual (12 Month) Management Review process outlined in Section IV(B) above.

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 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.

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: 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.

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 policies. The CISO is to report on the effectiveness of the cybersecurity program and material cybersecurity risks, including: the confidentiality, integrity and availability of material data elements defined within the Data Classification Policy.

Chief Technology Officer ("CTO"): The CTO and his designated representatives are responsible for providing effective challenge of Information Security policies and the implementation of Information Technology solutions.

Information Security ("InfoSec"): Information Security will Consult ("C")[2] and Inform ("I")[2] Information Technology regarding the configuration and deployment of controls and overall implementation of the Mobile Device Management ("MDM") platform.

Information Technology ("IT"): Information Technology is Responsible ("R")[2] and Accountable ("A")[2] for all configuration and deployment of controls and overall implementation of the Mobile Device Management ("MDM") platform. In addition, IT is Responsible ("R")[2] and Accountable ("A")[2] for the collection and storage of the "signed and approved" BYOD Use Agreement.

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.

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 1

Bring Your Own Device ("BYOD") Use Agreement

[2] as per *Information Technology ("IT") / Information Security ("InfoSec") RACI (Responsible, Accountable, Consult & Inform) Matrix*

XII. APPENDIX 2

Control Reference(s)

Asset	Mobile Devices
Examples (not a complete list)	▪ BYOD User is in compliance with both the Acceptable Use Policy and Code of Conduct, ▪ BYOD User's Mobile Device must be compliant with the "Minimum Security Requirements" ▪ BYOD User must complete and sign the "BYOD Use Agreement" and adhere to any requirements or instructions contained therein.
Controls	▪ Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled Mobile Devices; and ▪ Authorizes the connection of Mobile Devices to organizational information systems.
Control Source	NIST SP 800-53 Rev. 4 AC-19