Apple Financial Holdings, Inc.

Vulnerability Management Policy

October 28, 2020

Contents

POLICY NAME: Vulnerability Management Policy

REVIEW AND TRACKING CHART

Effective Date*:	October 28, 2020
Version Number:	2.0
Policy Level:	Level 2
Corresponding Board Review Frequency:	Biennial (Every 24 Months)
Board or Designated Board Committee:	Board Risk Committee
Last Board Review Date*:	October 28, 2020
Next Board Review Date*:	October 2021
Designated Management Committee:	Information Security Subcommittee/ Management Risk Committee (“MRC”)
Last Management Review Date*:	October 15, 2020
Next Management Review Date*:	October 2021
Policy Owner:	Max Tumarinson

*The review and effective dates above should only be updated after the appropriate meeting where the review or approval occurs. Prior to such meeting the dates should reflect the “old” dates of review. For clarity, do not use anticipated/prospective dates for Last Review or Effective dates.

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

I. POLICY PURPOSE STATEMENT AND SCOPE

The Vulnerability Management Policy (the "Policy") applies to the identification, management, monitoring, and remediation of security vulnerabilities in compliance with the Information Security Policy 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

- **Automated Teller Machine ("ATM"):** A machine that dispenses cash or performs other banking services when an account holder inserts a bank card.

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

- **Common Vulnerability Scoring System ("CVSS"):** is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat. Scores are calculated based on a formula that depends on several metrics that approximate ease of exploit and impact of exploit. Scores range from 0 to 10, with 10 being the most severe. While many utilize only the CVSS Base Score for determining severity, temporal and environmental scores also exist, to factor in availability of mitigations and how widespread vulnerable systems are within an organization, respectively. The Bank uses the final CVSS score as described within this Policy (*see Section B*).

- **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.

- **Computing Devices:** Computing Devices consists of physical and virtual desktop OS and server OS, *etc*.

- **IT Infrastructure:** IT Infrastructure consists of IT Infrastructure consists of Hypervisor OS, Storage Arrays, *etc*.

- **IT Network Infrastructure:** IT Network Infrastructure consists of OS of network-related IT Infrastructure such as routers, switches, firewalls, virtual infrastructure, VoIP technology, *etc*.

- **Applications:** Applications are managed by both vendors and by Technology (on-premises systems).

- **IT Service Management ("ITSM"):** The implementation and management of quality IT services that meet the needs of the business. IT service providers perform ITSM through an appropriate mix of people, processes, and information technology. See also "Service Management."

- **End-of-Life ("EoL"):** The point in time when the support vendor indicates that an asset has reached the end of its useful life [according to the vendor]. At this point, the vendor will either end or limit support for the asset. Extended support [including bug-fixes and security updates] may be available after this point, typically for a fee.

- **End of Support ("EoS"):** The point in time when the support vendor indicates that it will no longer provide extended support [including bug-fixes and/or security updates] for an asset, even for a fee.

- **End of Useful Life ("EoUL"):** The point in time in which an asset has fulfilled the purpose for which it was required, according to AFH. This point-in-time may or may not match the EoL cycle indicated by the vendor or manufacturer. Reasons for invoking EoUL may include but are not limited to newer technology, degraded performance, incompatibility or security concerns.

- **Golden Image:** An image which is reviewed by InfoSec that has the functionality, security and settings applicable to the Bank's Technology environment.

- **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.

- **Service Management:** A set of specialized organizational capabilities for providing value to customers in the form of services.

- **Technology Management:** The management of Information Technology to include network and infrastructure, applications, systems and services. Includes process-driven approaches towards management, focusing on customer need, and activities to design, plan, deliver, operate and control services offered to customers. Managed by the Chief Technology Officer ("CTO"), reporting to the Chief Executive Officer ("CEO"), and several reporting divisions to include Business Continuity and Disaster Recovery ("BC"/"DR"), Change Management, Data Warehouse, Digital Operations and Items Processing, Governance Risk and Compliance ("GRC"), Infrastructure and Support, and Systems and Standards. In addition, the Chief Information Security Officer ("CISO"), reporting to the Chief Risk Officer ("CRO"), provides IT and Information Security risk management governance and oversight from a 2nd line of defense position.

- **Vulnerability:** In computer security, a vulnerability is a weakness which can be exploited by a threat actor, such as an attacker, to perform unauthorized actions within a computer system. To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerabilities are also known as the attack surface. Vulnerability Management is the cyclical practice that varies in theory but contain common processes which include: discover all assets, prioritize assets, asses or perform a complete vulnerability scan, report on results, remediate vulnerabilities, verify remediation and repeat.

- **Voice over Internet Protocol ("VoIP"):** Is a technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line.

III. KEY POLICY COMPONENTS

1. Executive Summary

This document outlines AFH's Policy with respect to the identification, management, monitoring, and remediation of vulnerabilities. AFH Information Security and Information Technology departments will maintain detailed process and procedures documents, separate from this policy, to support the policy and drive consistent application of the requirements.

2. Objectives

The objective of this Policy is to establish a standardized and consistent approach to the identification, assessment, management, monitoring, and remediation of vulnerabilities.

3. Key Components of Policy

The policy requires the identification of vulnerabilities discovered (*via* scanning) on Computing Devices, IT Infrastructure, IT Network Infrastructure and Applications using an official, Bank authorized vulnerability scanning tool.

Vulnerability scans ("scans") can only be performed using the official Bank authorized vulnerability scanning tool. Any other vulnerability scanning tools cannot be used unless there is a documented approval by the Chief Technology Officer ("CTO") and Chief Information Security Officer ("CISO").

A. Vulnerability Identification

The scanning activity performed by the vulnerability scanning tool must cover all Computing Devices, IT Infrastructure, IT Network Infrastructure and Applications without any exclusions.

No information technology asset shall be configured to block the scanning activity performed by the official Bank authorized vulnerability scanning tool. In addition, IT and InfoSec cannot suppress any identified vulnerabilities unless there is a documented exception with business justification in accordance with all policies, procedures, standards and manuals and in compliance with Exception to Policy Procedure.

IT must conduct vulnerability assessments ("scans") on all Computing Devices, IT Infrastructure, and Applications prior to being placed in the Production environment. IT Network Infrastructure must utilize an approved *golden image* prior to being placed in the Production environment.

InfoSec must conduct vulnerability assessments ("scans") on all Computing Devices, IT Infrastructure, IT Network Infrastructure and Applications at a minimum, monthly basis or more frequently as deemed applicable.

The results and reports of scanning activity by the official Bank authorized vulnerability scanning tool are classified as Confidential and must be handled in accordance with the requirements within the Data Classification Policy.

InfoSec may engage an independent, third party provider to conduct an annual vulnerability management program assessment to validate the effectiveness of the vulnerability management program.

All vulnerabilities discovered on Bank IT Assets must remediated in accordance with the remediation priorities defined within the Service Level Agreement ("SLA").

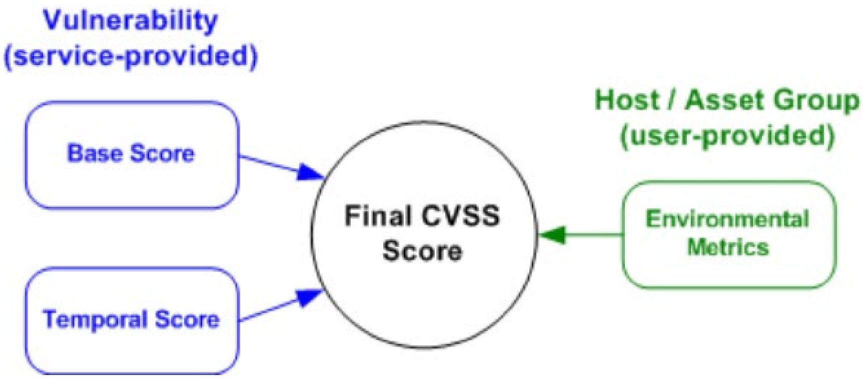
B. Service Level Agreement ("SLA")

InfoSec will evaluate all identified vulnerabilities and the Severity Rating assigned to the vulnerability by the vulnerability scanning tool which will be based upon the Common Vulnerability Scoring System ("CVSS"). The severity rating considers both the criticality and exploitability of the vulnerability.

InfoSec may adjust, as deemed applicable, the Severity Rating assigned to a vulnerability based on compensating controls or other mitigating factors.

The Severity Rating of vulnerabilities depends upon its CCVS score. The score will be aligned into a four-tiered model using the same language as defined in the Risk Management Framework Policy.

The final score is based upon vulnerability criticality and is calculated using three factors: base score (provided by an authoritative source), temporal score (also provided by an authoritative source, indicating urgency) and environmental metrics (defined by InfoSec, this assigns attributes to assets where different factors can adjust from the score, *e.g.*, logical location, classification of the data stored on a particular asset, compensating controls and other mitigating factors).



InfoSec will not recalculate the CVSS score of a vulnerability; however, the Severity Rating (aligned to the Risk Management Framework Policy) may be reassigned based on risk to the Bank. The vulnerability is subject to the SLA of its newly assigned Severity Rating.

The SLA dictates the remediation priorities, *i.e.*, the timeframe in which the vulnerabilities must be addressed and remediated upon discovery according to its rating. There are separate SLAs for the four asset groups: Computing Devices, IT Infrastructure, IT Network Infrastructure and Applications.

The SLAs are displayed in the table below:

Severity Rating/SLAs	**SLA – *Computing Devices**	**SLA – IT Infrastructure**	**SLA – IT Network Infrastructure**	**SLA – **Applications**	**CVSS Score**
Very High	Seven (7)	Seven (7)	Seven (7)	Seven (7)	10 - 9
High	Thirty (30)	Thirty (30)	Thirty (30)	Thirty (30)	8.9 – 7.0
Medium	Ninety (90)	One Hundred Eighty (180)	One Hundred Eighty (180)	Ninety (90)	6.9 – 4.0
Low	Three Hundred Sixty-Five (365)	Three Hundred Sixty-Five (365)	Three Hundred Sixty-Five (365)	Three Hundred Sixty-Five (365)	3.9 – 0.1

The numerical values displayed in the two SLA columns in this table are in calendar days.
*ATM patches are deployed by a third party service provider and are not subject to aforementioned SLAs.
**Applications that are managed by third party service providers are not subject to the aforementioned SLAs.
Any devices which do not fall into the aforementioned categories will use the most restrictive SLA timeline.

C. Vulnerability Remediation

All security patches must be installed to the production environment after non-production testing, by Information Technology personnel, based on the *AFH Technology Change Management Policy* and in accordance with the SLA defined in the section above.

Upon the remediation of discovered vulnerabilities (*e.g.*, installation of a patch, hotfix) a remediation scan must be conducted by *AFH Technology* to ensure the remediation has been applied effectively resulting in the elimination of the vulnerability (*i.e.*, validation scanning).

InfoSec will provide oversight of remediation and patches for ATMs; however, this activity has been outsourced to a third party provider.

D. Vulnerability Management Oversight and Reporting

In collaboration with the Technology Department, InfoSec will develop and maintain Key Risk Indicators ("KRIs") (*i.e.*, risk metrics) to identify and report on acceptable/unacceptable levels of vulnerability risk. InfoSec will provide oversight and will report on Very High, High and Medium vulnerabilities which have not been remediated (within the timeframe established by the aforementioned SLAs) to the appropriate management committee.

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 (Policy Level 2)

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 (Policy Level 2)

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:

Chief Information Security Officer (“CISO”): will provide oversight and will report both high and critical vulnerabilities that are not remediated with the below Service Level Agreement (“SLA”) to the appropriate management committee(s).

Chief Technology Officer (“CTO”): The CTO and designated representatives are responsible for creating and reviewing new and updated Technology policies and in charge of day-to-day oversight of execution.

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.

Information Security ("InfoSec"): InfoSec is Responsible ("R")[1] for the prioritization of vulnerabilities. In addition, InfoSec will Consult ("C")[1] and Inform ("I")[1] Information Technology regarding the selection of the vulnerability scanning tool, the scheduling of scan times and *ad-hoc* scanning, adjustment of severity ratings of vulnerabilities protected by compensating controls and mitigating factors. In addition, InfoSec will escalate Very High, High and Medium vulnerabilities not remediated within the established SLA to the appropriate management committee(s).

Information Technology ("IT"): IT is Responsible ("R")[1] and Accountable ("A")[1] to appropriately configure authentication parameters for credentialed scans. In addition, IT will remediate discovered vulnerabilities within the SLA by deploying patches and other solutions in compliance with the IT Change Management Policy. If a vulnerability cannot be remediated, IT must follow the process outlined in the Exception Policy.

Senior Management: Members of 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.

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.

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

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. LIST OF REFERENCE DOCUMENTS

1. Exception to Policy Procedure;
2. IT Change Management Policy;
3. IT/InfoSec Responsible, Accountable, Consult & Inform ("RACI") Matrix;
4. IT Asset Management Policy; and,
5. Exception Policy

XII. REVISION HISTORY

Version	Date	Description of Change	Author	Approver
1.2	10/15/19	Current "Vulnerability & Patch Management" Policy as published on AppleNet	K. Shurgan	Aditya Kishore Former CTO
2.0	9/29/20	Major revisions with input from IT, and Legal & Privacy	Joseph Martano AVP, Cyber Risk Analyst	Max Tumarinson SVP, CISO

XIII. APPENDIX 1

Control Reference(s)

Assets	Computing Devices, IT Infrastructure, IT Network Infrastructure & Applications
Examples (not a complete list)	▪ Assets (*e.g.*, servers, endpoints, virtual) ▪ Bank solution: Vulnerability Management Scanning Tool
Controls	▪ Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported; ▪ Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: o Enumerating platforms, software flaws, and improper configurations; o Formatting checklists and test procedures; and o Measuring vulnerability impact; ▪ Analyzes vulnerability scan reports and results from security control assessments; ▪ Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and ▪ Shares information obtained from the vulnerability scanning process and security control assessments with [*Assignment: organization-defined personnel or roles*] to help eliminate similar vulnerabilities in other information systems (*i.e.*, systemic weaknesses or deficiencies).
Control Source	NIST SP 800-53 Rev. 4 RA-5