Apple Financial Holdings, Inc.
Vulnerability Management Procedure

April 23, 2021

Contents

I. PROCEDURES PURPOSE STATEMENT AND SCOPE 4

II. DEFINITIONS 4

III. KEY PROCEDURES COMPONENTS 5
1. Executive Summary 5
2. Objectives 5
3. Key Components of Procedures 5
A. Network Infrastructure (Route-Switch Environment) 5
B. Systems (Server, Desktop) 5
4. Escalation Procedures 8

IV. REQUIRED ANNUAL (12 MONTH) REVIEW 8

V. OFF-CYCLE REVIEW AND APPROVAL PROCESS 8

VI. EXCEPTIONS TO THE PROCEDURES 8

VII. ROLES AND RESPONSIBILITIES 8

VIII. RECORD RETENTION 9

IX. QUESTIONS AND CONTACT INFORMATION 9

X. LIST OF REFERENCE DOCUMENTS 9

XI. REVISION HISTORY 10

PROCEDURES NAME: Vulnerability Management Procedure

REVIEW AND TRACKING CHART

Effective Date*:	*April 23, 2021*
Version Number:	2.0
Review Frequency:	Annual (Every 12 Months)
Last Business Area Leader/Department Head Review Date*:	*April 2021*
Next Business Area Leader/Department Head Review Date*:	*April 2022*
Business Area Leader/Department Head:	Debi Gupta, CTO
Overarching Policy or Policies:	Vulnerability Management Policy (Information Security)
Procedures Owner:	Jose Mendez; Stephen Apruzzese

I. PROCEDURES PURPOSE STATEMENT AND SCOPE

The Vulnerability Management Procedure (the “Procedures”) apply to the implementation, management, monitoring, compliance with vulnerability and patch management of technology infrastructure 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 and Bank policy.

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

II. DEFINITIONS

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

- **Business Area Leader or Department Head:** The management level person who is responsible for (1) the business unit that has developed a set of Procedures and (2) the Annual review and approval of Procedures.

- **Control Form:** The form to be submitted to the PPA (defined in this Section) in connection with revised Procedures. The Control Form is available on AppleNet.

- **Legal Contact:** The attorney from the Legal Department assigned to the group responsible for these Procedures. To the extent needed, the Procedures Owner may consult with the Legal Contact in drafting and updating the Procedures.

- **Policies and Procedures Administrator (“PPA”):** The PPA is a member of Risk Management. The PPA monitors the occurrence and timeliness of scheduled Procedure reviews, obtains updated versions of Procedures, and ensures that they are uploaded to AppleNet within seven days of the approval dates of the documents. The PPA will also provide guidance on the PPGP (defined in this Section) to Bank Personnel.

- **Policy, Standards, Procedures, and Manual Index:** An index, maintained by the PPA, which sets out the Policy, Standards, Procedures, or Manual name, Owner, regularly scheduled review dates, Regular Board Review Cycle (to the extent applicable), Designated Management Committee, and Designated Board Committee (to the extent applicable). The index is available on AppleNet.

- **Policy and Procedures Governance Policy (PPGP):** The PPGP establishes a standardized and consistent approach to the creation, review, approval and maintenance of Policies, Standards, Procedures, and Manuals across the Bank.

- **Procedures Owner:** The person responsible for managing and tracking a set of Procedures. This includes initiating the required Annual review of the relevant Procedures and recommending updates to the Procedures, to the extent needed. Procedures Owners are responsible for providing the approved documents to the PPA (defined in this Section) for upload to AppleNet. The Procedures Owner will monitor these Procedures. Any non-compliance with the

Procedures will be escalated to the Business Area Leader or Department Head for resolution.

III. KEY PROCEDURES COMPONENTS

1. Executive Summary

This document outlines AFH's Procedures with respect to the implementation, management and compliance with *AFH Vulnerability Management Policy*.

2. Objectives

The objective of these Procedures is to establish a standardized and consistent approach to implementation, management and compliance of infrastructure vulnerability and patch management inclusive of network and systems.

3. Key Components of Procedures

A. Network Infrastructure (Route-Switch Environment)

The Network Infrastructure Group is in charge of the Patch Management of Network devices, firewalls, including Voice servers. Below are the steps followed during the patching process:

1. A vulnerability report is generated by the Information Security Group after scanning the entire Bank network;
2. Information security requests that the Network Infrastructure Group assess if the vulnerabilities found after the scan are applicable to the devices based on their model and configured features;
3. The Network Infrastructure Group will prepare a list of affected devices for scheduled upgrade/patching;
4. The Network Infrastructure Group will contact the targeted device's manufacturers to determine the code versions to apply;
5. The engineers test the new code on a test/pilot device;
6. Upon testing success and further approval by the Change Advisory Board (CAB), the upgrades will be scheduled for after-hours installation; and the upgrade process is to be scripted in the SolarWinds Network Configuration Manager server and;
7. The SolarWinds executes the upgrade in multiple devices at the same time and send a job report at the end of the activity.

B. Systems (Server, Desktop)

The Server Infrastructure Group is in charge of the Patch Management of Servers, desktops and ESX hypervisor. Below are the steps followed during the patching process:

A. A vulnerability report is generated by the Information Security Group after scanning the entire server infrastructure;
B. Information security requests that the Server Infrastructure assess if the vulnerabilities found after the scan are applicable.
C. Server Infrastructure uses KACE which is a systems management and deployment

product which provides inventory and asset management, software distribution, and patch management.

KACE appliance is a centralized solution with easy-to-use deployment and support options, designed to quickly patch the infrastructure and related systems.

Weekly (Monday through Friday), a member of the Vulnerability and Patch Management group will perform KACE tasks to include reviewing reports to determine which servers and workstations require patching. In addition, research will be performed to re-certify inventory. Service Desk Tickets will also be monitored to ensure end-user patch-related concerns. Last, patches will be approved for deployment and installed.

Upon the deployment of a new server, a Server Build Checklist is followed, including deploying the Kace agent and ensuring that all available patches are deployed prior to being introduced to production thought the Kace appliance.

If a device's last inventory is out-of-date (more than 3 days) and that device is active, a member of the Vulnerability and Patch Management group will manually check-in the device.

See the *Systems Vulnerability and Patch Management User Manual* for details.

1. **Vulnerability Remediation Schedule**

   There are primarily two types of patches deployed onto the bank's network – Microsoft and 3rd party application patches.

   a. For every physical location, a server is selected to act as a local repository for patches and updates. File synchronization is enabled between the KACE appliance and such servers.

   b. Microsoft patches are deployed weekly and 3rd party application patches are deployed monthly.

   c. The patch distribution schedule is based on a weekly deployment of Microsoft and application patches:

Patch Type	Set of Systems	Sun	Mon	Tue	Wed	Thu	Fri	Sat
MS Critical (weekly)	POD				23:45			
	Branch Servers	23:00	23:00	23:00	23:00	23:00		
	Production 1				21:00			
	Production 2					21:00		
	Production 3						21:00	

Patch Type	Set of Systems	Sun	Mon	Tue	Wed	Thu	Fri	Sat
	Back Office					23:30		
	Test Branch	21:00						
	Test Branch POD	21:00						
	Test Back Office		21:00					
	Scarsdale DR						23:59	
	BR216WS030	22:00	22:00	22:00	22:00	22:00	22:00	22:00
	Branch 098	18:00	18:00	18:00	18:00	18:00	18:00	18:00
3rd Party (monthly)	Test Branch	21:00	21:00	21:00	21:00	21:00	21:00	21:00
	Production 1 (second Tue)		21:00					
	Production 2 (third Tue)		21:00					
	Production 3 (forth Tue)		21:00					

2. Vulnerability Classification

The vulnerabilities are:

a. Microsoft patches

b. Application, or 3rd party patches – Qualys reports are provided bi-weekly. Upon receipt of the reports, a member of the Vulnerability and Patch Management group is:

c. Reviewing the results

d. Providing a remediation via configuration changes or deploying security patches

e. Implementing other mitigating measures

f. Properly documenting any exceptions

See the *Vulnerability Management Policy* for higher-level detailed requirements for vulnerability classification and remediation timeframes.

3. Reporting

To ensure oversight and general solution performance, reports are delivered to all members of the Vulnerability and Patch Management Group either daily or weekly. These reports are reviewed to ensure remediation of discovered vulnerabilities to ensure remediation was successful:

a. Qualys reports are reviewed bi-monthly, and;

b. KACE reports are reviewed based on the patch schedule.

4. Escalation Procedures

The Procedures Owner will monitor these Procedures. Any non-compliance with the Procedures will be escalated to the Business Area Leader or Department Head for resolution.

IV. REQUIRED ANNUAL (12 MONTH) REVIEW

Procedures are required to be reviewed and approved at least Annually by the Business Area Leader or Department Head. The Procedures Owner is responsible for initiating an Annual review of the Procedures. The Procedures Owner will track the review date for the Procedures and begin the review process early enough to provide ample time for the appropriate review to occur in a timely manner.

Once updated Procedures have been approved by the Business Area Leader or Department Head, the updated Procedures shall go into effect and the Procedures Owner shall be responsible for delivering the approved Procedures together with a Control Form 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 Procedures are stored and made available to the employees of the Bank.

The Next Business Area Leader/Department Head Review Date shall be adjusted accordingly.

V. OFF-CYCLE REVIEW AND APPROVAL PROCESS

If the Procedures require changes to be made outside the Required Annual (12 Month) Review outlined in the previous section, the same steps as outlined in the previous section shall apply.

VI. EXCEPTIONS TO THE PROCEDURES

Requests for exceptions to these Procedures must be specific and may only be granted on specific items, rather than to entire sections. AFH staff must communicate their exception requests in writing to the Procedures Owner, who will then present the request to the Business Area Leader or Department Head for consideration.

VII. ROLES AND RESPONSIBILITIES

The key roles and responsibilities for these Procedures are summarized below:

Bank Personnel: Bank Personnel are responsible for understanding and following relevant Procedures. Bank Personnel participate in the development or updates of Procedures that exist within their business unit. When creating or updating Procedures, Bank Personnel should follow the Policy and Procedure Governance Policy and utilize the associated Procedures template which is available on AppleNet.

Business Area Leader or Department Head: *See Section II – Definitions*.

Internal Audit: The Internal Audit team is responsible for the periodic audit of these Procedures. Internal Audit will review the processes and any related gaps will be identified as findings to be monitored and remediated.

Legal Contact: *See Section II – Definitions*.

PPA: *See Section II – Definitions*.

Procedures Owner: *See Section II – Definitions*.

Senior Management: Members of management and business units are responsible for developing and implementing these Procedures which align with the requirements of the overarching Policy or Policies to which these Procedures relate, and ensuring compliance and understanding of these Procedures.

VIII. RECORD RETENTION

Any records created as a result of these Procedures should be held for a period of 7 years pursuant to the Bank’s Record Retention Policy. Should records created as a result of these Procedures require a different retention period (either a shorter or longer time period), the Procedures Owner must describe the rationale for a different retention period and share the rationale with the Business Area Leader or Department Head, who shall in turn document the deviation and supporting rationale in such a way that it can be presented to relevant parties upon request.

IX. QUESTIONS AND CONTACT INFORMATION

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

X. LIST OF REFERENCE DOCUMENTS

- *AFH Vulnerability Management Policy*

XI. REVISION HISTORY

Version	Date	A	Author	Approver
2.0	April 23, 2021	Updated to align with new *AFH Vulnerability Management Policy*	J. Mendez; S. Apruzzese, M. Lamparello	Debi Gupta, CTO
1.0	November 28, 2018	Align with new procedure.	K. Shurgan	Board Operations & Technology Committee