Apple Financial Holdings, Inc.
Infrastructure Audit and Monitoring Procedure

April 23, 2021

Contents

PROCEDURES NAME: Infrastructure Audit and Monitoring 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:	Security Audit and Monitoring Policy (Information Security)
Procedures Owner:	Michael Lamparello; Stephen Apruzzese

I. PROCEDURES PURPOSE STATEMENT AND SCOPE

The Infrastructure Audit and Monitoring Procedure (the "Procedures") apply to the implementation, management, monitoring, compliance with audit and monitoring 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 forresolution.

III. KEY PROCEDURES COMPONENTS

1. Executive Summary

This document outlines AFH's Procedures with respect to the implementation, management and compliance with AFH Security Audit and Monitoring Policy.

2. Objectives

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

3. Key Components of Procedures

A. Network Infrastructure

1. **The Network Management Systems (NMS), a SolarWinds module**, is used to monitor the status of all network devices. The Technology teams receive notifications/alerts from NMS which are used to identify anomalies. These alerts are received immediately and are acted upon by the Technology teams. NMS is used to report on the status of network devices, servers, and normal services; additional monitoring tools are also used to report on anomalies, the Technology teams works directly with the application or system owner to investigate and determine if the behavior is suspicious or expected. If monitored behavior is determined to be malicious the system(s) and/or application will be fixed immediately or isolated; remediating any potential threat(s) will be the first priority of root-cause analysis followed by proactive steps to ensure long-term safety of applications and systems. NMS reports are reviewed on a scheduled periodic basis as documented in System Monitoring procedures. Configuration Management System, another SolarWinds module, helps in the configuration of network devices, using templates including sending events to the SIEM and Network Time Protocol pointing to a master clock in the network.

2. **Firewall Policy Rules Review**: This is the procedure to be followed by the Network Infrastructure group (team responsible to maintain AFH firewalls) and Information Security (Team responsible to oversight operation security compliance) group to review the firewall rules on a quarterly basis. However, more frequent review can be performed during the year if necessary or required.

    a. The Quarterly Policy Rule review will be performed jointly by the Network Infrastructure group and Information Security within 2 weeks of the close of the quarter.
    b. A meeting invite should be sent out which will include Network Infrastructure team, and Information Security team as participants.
    c. Recommended firewall rules can be downloaded at any time prior to the meeting between the two departments for review.
    d. During the meeting each rule will be reviewed for the following but not limited

to:

i. Rule hit counts
ii. Source IP/Network/URL
iii. Destination IP/Network/URL
iv. Source Ports
v. Destination Ports
vi. Groups that uses the rule
vii. Domain Category

e. If any modification is needed, it will be recorded, and a follow up meeting will be held if necessary, otherwise email communication is sufficient.

Modification Guideline:
If a rule is deemed unnecessary by the team, it will first be disabled and monitored for any activities for at least two weeks prior to deletion.

3. **Security Information and Event Management (SIEM)** is setup to for the monitoring of infrastructure associated with “Critical Systems.” These logs and alerts are monitored on a scheduled periodic basis. The SIEM is managed by the Information Security team. The list of Critical Systems is to be obtained from the Information Security team.

   The SIEM is used to automate the log aggregation, analysis, monitoring, and reporting associated with data specific to network intrusion and anomalous events that are found in voluminous system logs. The Technology team is responsible for using the SIEM console and reports to identify network security incidents and to investigate them. Typical security incidents that are reported in the SIEM include, but are not limited to:

   - Advanced Persistent Threats
   - Bots
   - Denial of Service Attacks
   - Distributed Denial of Service Attacks
   - DNS Queries
   - Geo-protection
   - High Connection Rate Anomalies
   - Malware
   - Port Scans
   - Viruses

   The SIEM is monitored 24/7 by a Bank MSSP vendor Deepwach. DeepWatch opens security incident tickets if the specific use case has triggered an alert the Information Security investigated the ticket and works with Server Infrastructure or Network Team to determine the root cause of the alert. All alerts, regardless of the priority, are investigated based on the established SLA’s within the Service Level Agreement SOC/SIEM Process System Monitoring

   Network Devices and Servers are monitored 24 x 7 by NCR, and ServiceNow tickets are created automatically in the Apple Bank ServiceNow instance to alert the Network and Server Infrastructure group to any outages or failures in those devices.

B. Security Monitoring - Server

SecurityMonitoring is performed by Splunk via a Deepwatch forwarding server. In order to forward all logs from servers and applications, traffic must be directed to these servers, which is then sent to the Splunk hosted application.

The process to have logs forwarded to the SIEM has been automated through Kace to all devices. After a device has been added to Kace, a managed installation will automatically install this application silently. If for some reason the software is not installed (verify in Kace that UniversalForwarder is installed), you can follow the associated user manual for instructions on performing a manual installation.

Logging level for Server is set to a default level for system logging. NTP settings are controlled by Server Infrastructures DNS servers for a centrally controlled and synchronized time setting.

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

- Security Audit and Monitoring Policy

XI. REVISION HISTORY

Version	Date	Description of Change	Author	Approver
2.0	April 26, 2021	Updated to align with Security Audit and Monitoring Policy	M. Lamparello; S. Apruzzese	Debi Gupta, CTO
1.1	January 8, 2019	Add firewall rules review procedure	M. Mirza	K. Shurgan
1.0	November 28, 2018	Align with new policy.	K. Shurgan	Board Operations & Technology Committee