Apple Financial Holdings, Inc.
Active Directory Privileged Account Change Review Procedures

October 31, 2021

Contents

REVIEW AND TRACKING CHART

Effective Date*:	October 31, 2021
Version Number:	2.0
Review Frequency:	Annual (Every 12 Months)
Last Business Area Leader/Department Head Review Date*:	October 30, 2021
Next Business Area Leader/Department Head Review Date*:	October 2022
Business Area Leader/Department Head:	Debi Gupta, CTO
Overarching Policy or Policies:	Information Security Program Policy
Procedures Owner:	Allen Lum, IT GRC-CM, Technology Department

I. PROCEDURES PURPOSE STATEMENT AND SCOPE

The Active Directory (AD) Privileged Account Change Review Procedures (the "Procedures") apply to the monitoring of AD changes by individuals with domain privileges at Apple Financial Holdings, Inc. ("AFH"), inclusive of Apple Bank for Savings and its subsidiaries (collectively, "ABS," "Apple," or the "Bank"), to the extent applicable to such entity, in accordance with applicable state and federal statutes, rules and regulations.

All ABS 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

Active Directory ("AD"): A Microsoft technology used to manage computers and other devices on a network. It is a primary feature of Microsoft Windows servers, an operating system that runs servers across the Bank's Information Technology Infrastructure.

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.

Domain Privileges: Privileges that allow a user to make changes to active directory. This may include modifying users, making changes to GPO and other changes to Active Directory (AD). In order to get these privileges a user must be member of a Domain Privileged group as specified in the AD documentation.

Domain Admin: An Individual who is responsible for managing the AD domain. A person would be included in a specific designated group with privileges which would enable then to make changes to AD.

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.

Technology Change: The addition, modification or removal of any authorized, planned or supported service or service component that could have an effect on IT services. Such changes may arise reactively in response to problems or externally imposed requirements, e.g. legislative changes, or proactively from seeking improved efficiency and effectiveness or to enable or reflect business initiatives, or from programs, projects or service improvement initiatives. Technology changes should be beneficial, delivering additional value to the organization. Refer to the *Technology Change Management Policy* for further details.

III. KEY PROCEDURES COMPONENTS

1. Executive Summary

This document outlines AFH Procedures with respect to the monitoring and validating existing Active Directory (AD) changes made by accounts within the Active Directory “Domain Admins” group, “Domain Join Admins” and/or that have administrative privileges.

2. Objectives

The objective of these Procedures is to establish a standardized and consistent approach to AD administrative events (changes) are reviewed on a weekly basis by an independent party (an individual) without administrative permission to AD. The IT GRC-CM group within IT performs the review of AD event logs and documents the events analyzed for further internal review.

3. Key Components of Procedures

Core Process

The reviewer will examine AD event logs for the administrative transactions (changes). This will include a sampling to verify helpdesk tickets (ServiceNow) or email threads containing authorization. The Netwrix Auditor application is used to extract AD event logs for analysis.

Step 1 – Determine which users have Domain Admin Access

Obtain a listing of the following two reports:

- Domain Admin – lists all Domain Admin members –(tech support)

- Domain Join Admins – lists Domain Admin members (service desk and tech support

The above reports show which users have Domain Admin Access. Currently only the above groups have privileged access to AD.

Via inquiry and observation determine if additional groups have been created which would grant Domain Admin access/privileged access.

Step 2 – Active Directory Report Generation

The following three reports will be generated from the applicable AD logging software:

- Active Directory Changes Report – shows all changes to AD
- Group Policy Changes Report – shows changes to Group Policies

Review the members of Domain Admin and Domain Join Admins for appropriateness.

Step 3 - Sample Testing – Active Directory Changes for Approval

a. Generate a listing of all Active Directory changes for the period under review
b. Filter the AD changes so that you only select those AD changes performed by members of the domain admin and the domain join admins.
c. Select a Sample of Active Directory changes for testing.
d. Select a Sample of GPOs for testing.

A judgmental sample technique is used for sample testing, to select changes for review. The industry-standard and accepted methodology is used by External Audit Firms and IA, and is based on a generally-accepted auditing and statistical practices.

Samples will be selected based on risk, type of change, and history of previous problems/issues. This sample set will be called “Selective Sample Testing”.

Ensure that samples are spread between AD changes and GPO Changes.

If the population for GPO changes is under 5 – select the entire population for testing.

Step 4 - Select the AD Changes and Request Service Now (SNOW) Tickets

- Generated a Service Now request for the GPO’s and AD changes selected for testing.
- The domain admin will come back with a SNOW Incident, Change or Task ticket number.
- Go to the SNOW UI and enter the ticket number. Service Now will return the actual change request, incident and/or Task with the supporting information on the change and other documents if applicable.

Step 5 – Service Now Tickets Review

Review the selected SNOW tickets containing the AD Changes selected for testing and determine if there are any issues. Look for the following:

1. Approvals
2. Documentation of the Changes (if applicable)
3. Supporting testing documentations (if applicable)

Schedule time with the IT Infrastructure team as needed to discuss any potential exceptions to the AD changes.

Step 6 – Analysis of All Changes

In this step we will summarize and review all AD Changes which have been made. Create a pivot table of all changes and summarize by the change detail.
Examine the number of changes by detail – i.e. – Password resets
Determine if there is a substantial number of a particular changes which may warrant further follow up investigation.

Step 7 – Review all Changes

In this step you will scan all the changes looking for any anomalies that may appear in the population.

Step 8 - Creation of Work Paper Lead Sheet

A lead sheet summarizing the results will be created.

The following will be included in the lead sheet:

- Control Tested
- Risk
- Specific Test Steps
- Supporting Documentations
- Results of test
- Conclusions
- Sign-off of test by Reviewer

Conclusions and supporting documentation such as emails and screenshots will be included as an embedded document or an additional attachments.

Step 7 - Exceptions / Issues Which Have Been Identified

All exceptions noted in the testing will need to be cleared by discussions with the subject matter experts and documented within the lead sheet.

If the exception can be rectified immediately and appears to be a one-off then we will need to make a notation in the work papers. This will show how the exception was resolved and any supporting documentation.

A self-identified issue (SII) may be generated as follows if there are any:

- Exception which cannot be remediated immediately
- No extenuating circumstances

- No compensating controls
- There is a lack or breakdown of the control process

Refer to the *Technology Issue Exception Incident Mgt Procedures* document for assistance in developing the SII.

Once identified, the issue must be verified and confirmed with the process owner. Once confirmed, the following SII form should be completed. See the Manual - Self-Identified Issues for an example of the self-identified issues. These issues will be entered into MetricStream GRC and tracked to remediation.

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 pursuant to the Bank's Record Retention and Disposal 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

- Information Security Program Policy
- Technology Change Management Policy
- Technology Issue Exception Incident Mgt Procedures

XI. REVISION HISTORY

Version	Date	Description of Change	Author	Approver
1.0	8/28/20	New procedure	Allen Lum, IT GRC-CM,	Debi Gupta, CTO

			Technology Department	
2.0	10/30/21	Updated procedures to include the use of service now. Remove detailed – how to items such as screenshots - to a user manual	Allen Lum, IT GRC-CM, Technology Department	Debi Gupta, CTO