Apple Financial Holdings, Inc.
Identity Access Management and Authentication Procedure

July 26, 2021

Contents

PROCEDURES NAME: Identity Access Management and Authentication Procedure

REVIEW AND TRACKING CHART

Effective Date*:	July 26, 2021
Version Number:	1.0
Review Frequency:	Annual (Every 12 Months)
Last Business Area Leader/Department Head Review Date*:	July, 2021
Next Business Area Leader/Department Head Review Date*:	July, 2022
Business Area Leader/Department Head:	Debi Gupta, CTO
Overarching Policy or Policies:	Identity Access Management and Authentication Policy; Information Security Policy; Remote Access Policy
Procedures Owner:	Judy Nagle, Jose Mendez, Maria Siegel, Franklin Cabral, Stephen Apruzzese

I. PROCEDURES PURPOSE STATEMENT AND SCOPE

The Identity Access Management and Authentication Procedure (the “Procedure”) applies to the development, implementation, management, monitoring and deactivation of Bank/contractor user accounts (identity) and access management (i.e., the user account lifecycle), remote access and authenticaation (i.e., passwords, MFA) at Apple Financial Holdings (“AFH”), inclusive of Apple Bank for Savings (“Apple” or the “Bank”) in accordance with Bank policy. References to AFH herein are equally applicable to the Bank, unless otherwise noted.

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

II. DEFINITIONS

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

- **Authentication** - A security method used to verify the identity of a user and authorize access to a system or network.

- **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.

- **Critical Applications/Systems List:** The Critical Applications/Systems List is developed and maintained by the Bank’s Information Security department. The list includes critical applications/system names, description, Data Owners (authorized approvers) and Data Custodians (authorized administrators). During the user access review procedure, the list is reviewed for appropriate access by the authorized approver. As a first step to performing the procedures outlined below, the most current application/system list must be obtained from the Bank’s Information Security Department. Refer to the appendix for details.

- **Data Custodian:** The person responsible for the day-to-day activities related to access management for a particular application or database. The Data Custodian will also typically have a backup. The Data Custodian and backup are the authorized administrators for an application. The Data Custodian and backup if applicable will be identified within the Critical Applications/Systems List.

- **Data Owner:** The business-line person responsible for the application or database as applicable and data contained within it. Typically the Data Owner will also typically have a backup. The Data Owner or backup are the only individuals authorized to approve access. The Data Owner and backup if applicable will be identified within the Critical Applications/Systems List.

- **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.

- **Password** A sequence of characters that is used to authenticate a user to a file, computer, network, or other devices. Also known as a passphrase or passcode.

- **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.

- **Remote Access -** Used by way of a Virtual Private Network ("VPN") to provide secure network access to Bank users and where applicable consultants/vendors.

- **Virtual Private Network (VPN) -** A secure network implemented over an insecure medium, created by using encrypted tunnels for communication between endpoints.

III. KEY PROCEDURES COMPONENTS

1. Executive Summary

This document outlines AFH's Procedures with respect to the implementation, management, monitoring, and compliance with the Bank's identity and user access requirements, remote access and authentication/password requirements.

2. Objectives

This document outlines AFH's Procedures with respect to the management, monitoring and compliance with the *AFH Identity Access Management and Authentication Policy*, the *Information Security Policy* and the *Remote Access Policy*.

3. Key Components of Procedures

A. Setting Up New Accounts[1]

Upon confirmation that a new hire has accepted a position, HR sends an email to the “newhire” distribution list with the employee’s name, title, department, manager, and start date. The hiring manager completes the onboarding form and sends it to the Service Desk and User Entitlement teams.

There is a 10-day turnaround time from the day the onboarding form is submitted to the Service Desk and User Entitlement Group. Teller positions are only a 5-day turnaround. Every effort will be made to accommodate exceptions when possible; however, users should not expect final set up to be complete until either 5 or 10 days.

Employee access privileges will be based on their role and responsibilities at Apple Bank. The user access form will contain the access privileges (including role-based access if applicable) and employee information necessary to setup the account. See the appendix section for links to the appropriate form.

The Service Desk, User Entitlement Group or other applicable Data Custodians will seek approval from the Data Owner, where required, referencing the Critical Applications/Systems List maintained by InfoSec.

The Active Directory password will be randomly generated using the following website - *https://passwordsgenerator.net/* - The password length is set to 14 characters and the complexity requirements must comply with Apple Bank policy. The randomly generated password will be copied and pasted into the new user’s Active Directory account.

The password will not be recorded or shared. Once the Service Desk Analyst has completed the setup of the PC, the new employee’s password will be reset in order to test the configuration, settings, drive mappings, etc., and cache the password for the new hire.

The Service Desk Analyst will force the user to change the password at next logon. On the new employee’s first day a Service Desk Analyst will work with the new employee to walk the user through the VPN process. The new employee will enter the temporary password and will be immediately prompted to change it. The Analyst will review the password complexity guidelines with the new employee so a password length of 14 characters is created in addition to the other password complexity requirements in accordance with Apple Bank policy.

The Service Desk Analyst will also provide the new user with the Okta Self-Service Password Reset Instructions.

Reference the appendix for details regarding the various account types.

Apple Bank reserves the right to withdraw such privileges pursuant to contract stipulations as well as actions spelled out by our Electronic Communications policy or Acceptable Use policies

[1] This process is as it is performed today; however, will be revised as the process changes in the near future.

and other policies that govern employee and contractor relations.

B. Recertification

The access rights of each user in each key application must be recertified periodically (at least annually / as defined in Identity Access Management and Authentication Policy). This must be performed by the authorized approvers (which may be the Data Custodian and the Data Owner within IT or the Business Owner). Refer to the Bank's most recent Critical Applications/Systems List, developed and managed by the Information Security Department, for details related to authorized approvers. See the appendix for details.

The following process applies to those applications where IT is the Data Custodian. Information Security will be responsible for recertification of the remaining applications except where the application owner assumes the responsibility.

The Data Custodian of each application will produce a system-generated report of all user accounts, and their levels of access.

The Data Custodian will either perform the authorized access review or seek input as needed on authorized access from the users' direct supervisor in order to complete the review and recertification.

If required, the Data Custodian will request the employee roster, termination report, department transfers (and promotions/position changes) from Human Resources. This will help reconcile and verify the users in the application.

The Data Custodian will perform an access review of each user in the application and make appropriate adjustments in access.

The Data Custodian will review and sign user account recertification reports to verify the results of the recertification and that appropriate corrective actions were taken. If weaknesses in the user account controls for the system are discovered, appropriate remediation will be pursued.

The result will be forwarded to Information Security for final review and make further adjustments, if called for.

Information Security will retain all users account recertification documentation in accordance with Bank's Record Retention Policy (currently, 7 years).

C. Active Directory Recertification

The goal of the Active Directory Recertification Process is to identify all accounts currently within Active Directory and their current status (e.g., active, disabled, expired, etc.)

The recertification process aims to find the delta of account, which are active; however, should have been marked for disablement and/or deletion.

Active Directory is reviewed and accounts are cross-referenced (validated) with the Bank's Human Resources employee roster/list.

Re-certification review will focus on the following:

- Users cross-reference to the most current HR Roster List. Any user not matched, will be reconciled with Human Resources.
- All Consultants are checked to make sure they are still active.
- All privileged user accounts are reviewed and verified. (Enterprise, Scheme, Domain Access Levels)
- Service Accounts are identified and reviewed.
- Disabled Accounts only exist for the purpose of a litigation hold.
- Last Login Activity is reviewed for disabled accounts retained for litigation hold purposes.
- Identify all Never Expired Password Accounts and provide business justification.

Refer to the AFH Identity Access Management and Authentication Policy for details.

D. Privileged Account Access Reviews

On a frequency outlined within the AFH Identity Access Management and Authentication Policy, [currently quarterly], the Data Custodians, with the oversight of Information Security, performs a privileged user access review for the critical/sensitive applications identified by Information Security. Other than the frequency of review, the procedures are the same as for non-privileged account access reviews.

E. Active Directory Change Management

- All onboarding, transfer and off-boarding forms are archived by the Service Desk; the forms are attached to the corresponding ServiceNow ticket.
- All changes noted under the Active Directory Re-Certification is documented in ServiceNow and held for evidence.
- Documentation for ancillary system changes made by the User Entitlement Department are stored as part of the daily activity on Fortis and in the future, DocuWare.

F. Disabling/Removing User Accounts

Step 1: Initiation of Termination

- The manager completes the employee separation form and sends to HR (hrterms@applebank.com).
- HR sends an email to the "terminated" distribution list with the employee's name, title, and termination date.
- Initiated via email from HR, a Service Desk Queue Coordinator will create a ServiceNow ticket for each terminated employee, then send an email confirmation/reply to HR that a ticket has been created for those terminated employees including the ticket number(s).
- The Service Desk Specialist assigned to the "termination ticket" sets the account to expire on the termination date specified in the HR notification. On the employee's termination date (or last official work day) the Service Desk will disable the employee's account at the end of the business day if not otherwise specified in the termination notification. All security groups and distribution lists are removed.

- The Service Desk will also coordinate access to the employee's email account and home drive with employee's manager for 30 days. A notification will be sent out to employee's manager via email.

    - Use case:
        - If the replacement is hired within the 30 day period and manager would like the replacement to have access to the former employee's email and home drive – manager must submit a request to the Service Desk for access.
        - If the mailbox is required after 30 days, the terminated employee's email address will become an alias of whomever the manager designates and will continue to be an active mailbox. A request must be sent to the Service Desk to export the historical email content so it can be imported to the designated person's Gmail as its own folder. Home drive will remain accessible until otherwise noted from the manager.

    - Use case:
        - **Immediate Terminations and High Risk Employees**
          Advance notice of the termination prior to the termination meeting gives the IT department sufficient time to disable access while the meeting is taking place. From an IT perspective, the following tasks must be completed in order to revoke access.
          If the user has a phone and it needs to be wiped, the account needs to be active and the password CANNOT be changed for the wipe to work.

            - Disable ID(s) in Active Directory
            - Disable OKTA account
            - Delegate access of the mailbox and Personal Drive (F:\) to the terminated employee's manager. Sync with OKTA.
            - Disconnect the user's VPN session.

    - Use case:
        - When a sensitive employee requests time off of two weeks or more (consecutively) in ADP, a ticket will be automatically created in ServiceNow for the Service Desk to disable user remote access only, not Gmail. Notification email will be sent to employee.

Step 2: Termination/Exit Interview (immediate steps for high-risk employees as identified by their managers)

- HR determines the need, timing, and terms of separation, then notifies IT [via email], who then performs the following tasks:
    - Remotely turn computer off and delete the computer account in Active Directory. Note: Accounts will only be disabled for litigation hold purposes.
    - Immediately disable the employee's access to all systems beginning with Active Directory.
    - Remove all organizational data from employee-owned devices using one of the following options:

    - HR observes the user deleting email accounts from their phone.
    - IT remotely wipes device(s).
- Department Manager or HR ensures the terminated employee returns any company-owned equipment such as laptops, tablets, USB drives, etc.
- Department Manager, when applicable, should compile a list of locations where the employee-stored data is

Step 3: Phone

- Telecomm department will ensure the employee's telephone is not forwarded to any external numbers, such as a cell phone.
- Telecomm department will change voicemail password.
- Department Manager will change the outgoing voicemail message in accordance with the organization's communication guidelines.
- Department Manager will assign another team member to monitor the voicemail until the phone number is deleted or reassigned.

Step 4: Email Access

- Email account is disabled in G-Suite and the mailbox data is archived unless otherwise requested. The Service Desk will also coordinate access to the employee's email account and home drive with employee's manager for 30 days. A notification will be sent out to employee's manager via email.
- Access to MFA (e.g., OKTA) is revoked.
- Terminated employee is removed from email distribution lists.

Step 5: Network and Cloud Access

- The employee's VPN session is terminated, if applicable.
- The employee is removed from all access control security groups in Active Directory.
- The access of the employee to any corporate Dropbox account or similar platforms is revoked.
- The Service Desk will coordinate access to the employee's home drive with employee's manager for 30 days. A notification will be sent out to employee's manager via email.
- Department manager may identify a team member who will need access to the terminated employee's local and network files.

Step 6: IT User Entitlement Group

- Deletes or disables users from all applications which it manages.

Additional Steps for Off Boarding IT Staff

- Any administrative password the employee may have been exposed to must be changed while disabling the terminated employee's access.
- Any company equipment, manuals, keys, backups, etc., is retrieved.
- Records for external providers and services (e.g., website hosts, MSP, data center, etc.)

should be updated.

Monthly Account Validation (user & service):

- A termination report is provided by HR to the Service Desk on a monthly basis to certify all terminated employees have been disabled.
- An automated script is in place to perform account cleanup based on the following criteria.
  - 30/30/30 rule:
    - Inactive user account for >= 30 days => disable
    - Disabled account for >= 30 days => delete
    - Employee's laptop/workstation will be scanned first then wiped after 30 days
- Accounts deleted over six months will be permanently purged from all sources - (AD, OKTA, ServiceNow, etc.)
- Additional rule in ServiceNow – any assets that haven't been detected during the discovery scan for the last 30 days will be manually purged.

G. Contractor/Vendor User Account Procedures

HR sends an email to the "newhire" distribution list with the consultant's name, title is listed as "consultant," department, manager, and start date. The hiring manager completes the onboarding form and sends it to the Service Desk and User Entitlement teams.

The name of the contractor / vendor representative must be communicated to the Service Desk at least 5 business days before the access is needed. The Bank will maintain and monitor the current list of external contractors / vendors having access to the bank's network.

The termination of security access privileges for a contractor / vendor must be communicated to the Service Desk at least 1 business day before the contractor / vendor engagement will end.

H. Remote Access Procedures

1. Acceptable Conditions

   Remote access procedure applies to all users that are granted permission for remote connectivity. End user account creation is performed as follows:

   1) Onboarding form submitted to service desk
   2) User account is created in Active Directory
   3) User account is synched automatically with Okta services and the account is activated based on status in Active Directory
   4) Rights for VPN access are granted with Active Directory by group assignments based on the onboarding form

2. User Virtual Private Networks (VPN)

   - Refer to Section 3.A. above.

3. Servers

- Remote Desktop Protocol (RDP) access is managed through the Thycotic PAM portal. All RDP sessions are logged and monitored through this portal.

4. Desktops

   - Remote access to assist users by the Service Desk team are performed through DameWare which is accessed via the Thycotic PAM portal.

I. Password Procedures

1. Network Infrastructure

   Network device user authentication is integrated with Active Directory (“AD”) via RADIUS. AD regulates the password rotation period and complexity. If the network device loses connectivity to the RADIUS server, and therefore with AD, the device can be accessed physically via the console port connected to a laptop. This method is called Out of Band (“OOB”) access. Password complexity requirements and password rotation is implemented in all cases where technically feasible. OTB access must be stored in Thycotic and where feasible rotated.

2. Systems

   Users are required to change their password every six months in accordance with the password requirements outlined in the *ABS Identity Access Management & Authentication Policy* maintained by Information Security.

   Please note in order for the following process to be completed, it must be performed while connected to the Apple Bank network via VPN or from a PC directly connected to Apple Bank's local network (ex. Branch or Back office):

   - Press “Ctrl – Alt – Delete” simultaneously on your keyboard.
   - Select “Change a password”.
   - Enter your existing password followed by a new password based on the policy requirements**.** Click on the arrow pointing right to complete the password change.

A user can also change their password via the Okta Self Service Portal.

1. Open a browser and navigate to https://applebank.okta.com
2. Once there, select “Need help signing in?”
3. Select “Forgot password?”
4. Enter your full email address or user name and select the appropriate method to verify your identity.
5. After verification is complete, follow the on screen instructions to reset your password.

3. Rotation of Passwords

   - Local Administrator passwords for all Servers and Workstations/Laptops are managed and rotated once a month and/or when a user performs a manual check out of that specific password.
   - Privileged Account passwords are managed and rotated once a week and/or when a user performs a manual check-out of that specific password.
   - Service Accounts managed by Thycotic are rotated once a month.

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 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 Policy
- Identity Access Management and Authentication Policy
- Remote Access Policy

XI. REVISION HISTORY

Version	Date	Description of Change	Author	Approver
1.0	July 2021	Updated to be in-line with changes to Information Security Policy, Identity and Access Management and Authentication Policy, and Remote Access Policy. In addition, merged three older documents to include User Access Procedures, Identity and Access Management Procedures, Remote Access Procedures and Password Procedures.	J. Nagle, M. Siegel, F. Cabral, S. Apruzzese	Debi Gupta, CTO

Appendix A

1. ACCOUNT TYPES

User Accounts

- **Administrative (''A" Account)**: A privileged account used to perform administrative function.
- **Application Admin Account**: A privileged account which is an Installation Account also used to administer an application.
- **Default Account**: Accounts that come with an operating system, such as Administrator in Windows.
- **Installation Admin Account**: A privileged account used to install a system.
- **Non-Privileged Account**: Any account that is not a Privileged Account, such as a general network account that is given to most employees.
- **Privileged Accounts**: Accounts with elevated privileges.
- **Read-Only Administrator ("R" Account)**: Allows read-only access to sensitive data.
- **Sensitive Transaction User ("STU" account)** is a "T" (temporary) account used for specific business-related transactions that require elevated privileges. STU accounts do not require a change request, but require managerial approval.
- **Temporary Account ("T" account)**: Used to make changes to the system environment. The use of this account requires a change request. These accounts are usuallyassociated with PAM systems.
- **Test Account**: Accounts used to test systems, usually assigned to IT Services for application testing (AT), Quality Assurance for business functionality testing (QT), Capacity Planning for performance testing, Head Office User Testing (HT), Power Business User Testing (BT) and Proof of Concept testers (POC).

System Accounts

- **Batch Account**: Used to execute a batch job.
- **Service Account**: Used by an application to authenticate the use of a service.
- **Transmission Account**: Used to execute a data transmission job.

2. CRITICAL APPLICATIONS/SYSTEMS LIST

See \\br202fs1\IS_IT_Shared\Application Data Owner\Application Data Owner Custodian List - 4.24.20.xlsx for the list as of 04/28/2020 or reach out to the Information Security Department for the most recent listing.

3. ONBOARDING FORMS

See http://applenet/forms/index.php?dir=Branchforms/FORMS/HUMAN%20RESOURCES/On-Boarding&

- New Employee/Transfer Onboarding Form
- New back office Employee Onboarding Form

4. APPLICATION-SPECIFIC USER ACCESS PROCEDURES

ADP

- Please refer to the ADP User Access Procedures
- Human Resources:
    - Susan Goro - EVP, Human Resources Director
    - Arlaina Sokolsky - FVP, Total Rewards Officer

BAM

- Please refer to the BAM User Access Procedures
- User Entitlement Group::
    - Judy Nagle MIS, FVP

FCM

- Please refer to the FCM Procedures
- User Entitlement Group:
    - Judy Nagle MIS, FVP

FEDLINE ADVANTAGE

- Please refer to the FedLine Advantage Subscriber Access & Security Manual
- Accounting:
    - Gina Stroescu – FVP, Assistant Controller
    - Ella Abramov – AVP, Assistant Controller

GMAIL

- Please refer to the G-Mail User Set-Up Procedures
- Service Desk:
    - Maria Siegel – VP, Service Delivery

MISER

- Please refer to the MISER User Access & Security Procedure
- User Entitlement Group::
    - Judy Nagle MIS, FVP

WIREPRO

- Please refer to the WirePro User Access Procedures
- User Entitlement Group::
    - Judy Nagle MIS, FVP