Apple Bank for Savings

Identity Access Management & Authentication (“IAM&A”) Policy

February 24, 2021

Contents

REVIEW AND TRACKING CHART

Effective Date*:	February 24, 2021
Version Number:	2.0
Policy Level:	Policy Level 2
Corresponding Board Review Frequency:	Biennial (Every 24 Months)
Board or Designated Board Committee:	Board Risk Committee (“BRC”)
Last Board Review Date*:	February 24, 2021
Next Board Review Date*:	February 2023
Designated Management Committee:	Information Security Sub-Committee (“ISSC”) / Management Risk Committee (“MRC”)
Last Management Review Date*:	February 11, 2021
Next Management Review Date*:	February 2022
Policy Owner:	Chief Information Security Officer (“CISO”)

I. POLICY PURPOSE STATEMENT AND SCOPE

The Identity Access Management & Authentication ("IAM&A") Policy (the "Policy") applies to the implementation, management, monitoring and oversight of access controls and identity and access management functions including, but not limited to: user provisioning and de-provisioning, privileged user monitoring, user recertification, management of user accounts, *etc*., at 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 ABS employees and third party resources engaged by the Bank must comply with the terms of this Policy to the degree applicable to them.

For the purpose of this Policy, ATM IAM/password activities are managed by a Third Party Service Provider ("TPSP") and are excluded from this Policy.

II. DEFINITIONS

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

- **Applications:** Applications (*i.e.,* software), managed by both vendors (*i.e.,* hosted solutions) and by Technology (*i.e.,* on-premises systems).

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

- **Authentication Management:** A term which refers to the management of the Bank's authentication systems. Authentication systems are systems that verify a user's identity (typically in the form of a username & password, *i.e.*, credentials) in order to grant that user the appropriate level of authorization to use or access resources on the Bank's internal network, to make changes or to perform day-to-day, business-as-usual ("BAU") activities.

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

- **Cloud Offerings:** Any solution which leverages private or public cloud technology as identified by the vendor; for example, software-as-a-service ("SaaS"), infrastructure-as-a-service ("IaaS") and platform-as-a-service ("PaaS"), *etc*.

- **Computing Devices:** Computing Devices consists of physical and virtual desktop and server operating systems ("OS").

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

- **Data Custodian:** Data Custodians are accountable for data assets from a technical perspective; Data Custodians are accountable for the technical controls of data including security, scalability, configuration management, availability, accuracy, consistency, audit trail, backup and restore, technical standards, policies and business rule implementation (definition subject to updates in the *Data Governance Policy*).

- **Identity Access Management ("IAM"):** A framework around defining and managing the roles and access privileges of individual users and the circumstances in which users are granted (or denied) those privileges. The goal is to grant access to the right enterprise assets to the right users in the right context, from a user's system onboarding to permission authorizations to the off-boarding of that user as needed, in a timely fashion.

- **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.

- **IT Assets:** Please reference the *AFH IT Asset Management Policy*.

- **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.*

- **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 and serves in an advisory capacity.

- **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.

- **Multi-Factor Authentication ("MFA"):** Authentication through verification of at least two of the following types of authentication factors:

    - Knowledge factors, such as a password; or
    - Possession factors, such as a token or text message on a mobile phone; or
    - Inherence factors, such as a biometric characteristic.

- **Policy Level 2:** A Regular Board Review Cycle level for a Policy, designated by Risk Management in consultation with Legal. Level 2 Policies require Biennial approval by the Board or a Designated Board Committee.

- **Policy Owner:** The person responsible for managing and tracking a Policy. This includes initiating the review of the relevant 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 PPA (as defined in this Section) for upload to AppleNet. Additionally, the Policy Owner is responsible for presenting revisions and Policy exception requests for consideration.

- **Policies and Procedures Administrator ("PPA"):** The PPA is a member of Risk Management. The PPA monitors the occurrence and timeliness of scheduled Policy reviews, obtains the updated versions of Policies, and ensures that 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 the PPGP (as defined in this section) to Bank Personnel.

- **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.

- **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.

- **Privileged Accounts:** A privileged account is an account that by virtue of function and/or security access, has been granted special privileges within an information system or network resource that are significantly greater than those available to the majority of users.

  These accounts have special administrative or elevated privileges that may include the ability to do any or all of the following on a global basis within the system or network resource:

  - Administer users (*e.g.*, add, remove, disable accounts, and/or modify permissions); and
  - Make or affect configuration or other changes (*e.g.*, database administration, firewall configuration).

- **Privileged Access Management ("PAM"):** The cybersecurity strategies and technologies in order to exert control over privileged / elevated access and permission for users, accounts, processes and systems across an IT environment. PAM helps to organize and condense the Bank's attack surface and prevent and potentially mitigate the material damage arising from external attacks as well as from insider malfeasance or negligence.

- **Regular Board Review Cycle:** The required periodic Board or Designated Board Committee approval process for a Policy, the frequency of which is determined by the designation of a Policy as a Level 1, Level 2, or Level 3 Policy.

- **Service Account:** An account that is used by an application or service to interact with the operating system or an account used by applications to access databases, run batch jobs or scripts or provide access to other applications, *etc*.

- **User Account:** A user account is a standard user account which does not have special administrative or elevated privileges. These accounts may be owned by both Bank and non-Bank employees (*e.g.*, consultants).

III. KEY POLICY COMPONENTS

1. Executive Summary

This document outlines the Bank's Policy with respect to the implementation, management, monitoring, and compliance in regards to identity and access management related functions and password controls. The Bank's IAM&A Policy will define and document the Bank's access controls and identity and access management functions and password controls to protect, and reduce risk to, business operations by establishing requirements for creating, maintaining, and controlling access to Applications, IT Infrastructure, IT Network Infrastructure and Computing Devices.

2. Objectives

The goal of the Bank's IAM&A Policy is to define and document IAM principles and requirements for creating, maintaining, and controlling access to Applications, IT Infrastructure, IT Network Infrastructure and Computing Devices. The objective is to inform the Bank's employees and other relevant stakeholders of the Bank's IAM and user and privileged users account management and password requirements.

3. Key Components of Policy

The policy requires access control requirements, granting & removing user access, privileged account management ("PAM") / administrative access, review of access rights, requirements for access requests and relevant approvals in addition to user and other accounts' password requirements.

The Bank must ensure that access to Applications, IT Infrastructure, IT Network Infrastructure and Computing Devices are limited solely to authorized users whose business needs, job functions, and responsibilities require such access, or to users on a need-to-know basis.

Any Service Account must have a designated Data Custodian assigned to the account.

a. Access Control Policy

Access to the Bank's Applications, IT Infrastructure, IT Network Infrastructure and Computing Devices will be limited solely to users whose business needs, job functions, and responsibilities require such access, or to users on a need-to-know basis.

It is prohibited for an individual to request and approve their own access. All requests must be approved by the employee's immediate Manager.

Access reviews for all users including privileged users to the Applications, IT Infrastructure, IT Network Infrastructure and Computing Devices will be conducted periodically and, at a minimum, annually.

Using a risk-based approach, Applications, Computing Devices, IT Infrastructure and IT Network Infrastructure components generally will be centrally managed by Information Technology ("IT"). The aforementioned items which are not managed by IT may be managed by the Business but must follow the guidelines and principals set forth within this Policy.

b. Granting & Removing User Access

The Bank has a process for establishing, activating, modifying, reviewing, disabling and removing accounts (*e.g.*, Privileged Accounts and User Accounts) that is documented, implemented and maintained in the Bank's *User Access Procedures*, which must be followed by IT.

Access granted to non-Bank employees will follow the same onboarding/off-boarding process as Bank employees.

c. Account Management

Active Directory ("AD") / Network Accounts

Inactive accounts must be disabled after thirty (30) days of inactivity. After sixty (60) days, the inactive account must be deleted.

Privileged Users are not permitted to use their Privileged Accounts to conduct non-privileged activities.

Non-Integrated Application Accounts

For the purpose of this Policy, ancillary systems in which user management is performed by a department other than IT, that Business Unit must designate a Data Custodian for IAM related activities such as entitlement reviews. If the ancillary system cannot be integrated with the Bank's enterprise IAM solution, the Data Custodian should configure (or request configuration by a TPSP) the Application to meet the requirements (*e.g.*, non-integrated application password complexity, inactive account disablement) set forth in this Policy.

Voluntary Terminations

The user network account must be disabled before close-of-business on the last day of employment. For non-integrated systems, such application user accounts should be disabled within seventy-two (72) hours.

Involuntary Terminations

The user network account must be disabled immediately, on the day of termination. For non-integrated systems, such application user accounts should be disabled within four (4) hours.

d. Authentication

As a best practice, the Bank will require strong passwords and stringent password management for all accounts.

User Active Directory ("AD") / Network Password Complexity Requirements

A strong password as defined by the Bank is fourteen (14) characters with **three of four** of the following attributes:

- Uppercase letters,
- Lowercase letters,
- Base ten (10) digits (*i.e.*, 0 through 9)
- Special characters (*i.e.*, !, $, #, %).

User Active Directory ("AD") / Network Password Management

Upon suspicion that a password is believed to be compromised, it must be changed immediately.

Usernames and passwords (*i.e.*, credentials) should not be written down, but should be committed to memory (*i.e.*, it is something you know).

If an employee elects to use a password management solution, it must be the Bank's password management solution.

All default / starter passwords are never to be used for business-as-usual ("BAU") purposes; once access is gained through use of a default / starter password, it must be immediately changed.

Users will be locked-out after three (3) repeated, failed access attempts. Users will remain locked out until they request a password reset through the Bank's self-service portal or contact the Bank's Service Desk.

Passwords must be changed, at a minimum, every one hundred eighty (180) days. A reminder will be provided to employees prior to password expiration.

Passwords should be unique to each system (*i.e.*, the same password should not be used across multiple different systems, sites, web portals, devices).

Passwords which are changed must be different from the previous twelve (12) passwords.

Passwords are classified as Confidential as per the *Data Classification Policy* and must not be shared with anyone. Passwords are never to be stored in plain/clear text and must be encrypted with the appropriate strength designated by the *Data Classification Policy*. The Bank and its employees (including IT) will never ask you for your password.

Non-Integrated Application Password Complexity Requirements

A strong password should consist of twelve (12) characters with the following attributes: uppercase letters, lowercase letters, numbers and special characters. In addition, passwords should not consist of dictionary words and/or names (*e.g.*, portion of the user's account name or full name), have sequential patterns or include non-public personally identifiable ("NPPI") information.

Users should not utilize the "Save Password" feature in any application and/or web portal.

Non-Integrated Application Password Management

Upon suspicion that a password is believed to be compromised, it must be changed immediately.

Usernames and passwords (*i.e.*, credentials) must not be written down. Passwords must be committed to memory (*i.e.*, it is something you know). Default passwords are never to be used and must be changed immediately upon discovery.

Passwords must be changed, at a minimum, every one hundred eighty (180) days.

Passwords should be unique to each system (*i.e.*, the same password should not be used across multiple different systems, sites, web portals, devices).

Passwords which are changed should be different from the previous twelve (12) passwords.

Passwords are classified as Confidential as per the *Data Classification Policy* and must not be shared with anyone. Passwords are never to be stored in plain/clear text and must be encrypted with the appropriate strength designated by the *Data Classification Policy*. The Bank and its employees (including IT) will never ask you for your password.

Users should not utilize the "Save Password" feature in any application and/or web portal.

For Non-Integrated Applications where MFA is utilized, for the second factor (*e.g.*, push notifications, One-Time Password ["OTP"], key fob) the aforementioned Password Management requirements may not be applicable.

e. Privileged Account Management ("PAM") / Administrative Access

The allocation and use of Privileged Access to the Bank's assets and services must be restricted and controlled. Special attention shall be given to the allocation of privileged access rights, which allow users to override system controls.

Users which will be using the PAM solution and will have access to Privileged Accounts must have Multi-Factor Authentication ("MFA") enabled.

All privileged account requests must be approved by InfoSec including accounts which process financial transactions and/or accounts which, if compromised, may have an immediate, adverse material impact to the Bank.

Privileged user accounts will be separate from non-privileged user accounts and privileged user accounts will only be used when Privileged Access is required to complete a specific task or function. Passwords for Privileged Accounts will be rotated within twenty-four (24) hours after the specific task or function which was requested has been completed.

All of a user's Privileged Access to the Bank's Applications, IT Infrastructure, IT Network Infrastructure and Computing Devices must be revoked or revised immediately (within 24 hours) from the time that Information Technology is notified that user's change in employment status, job function, or responsibilities no longer justifies that user's need for such access.

Service Accounts should not be used by more than one service, application or system. Passwords for Service Accounts should be rotated on a monthly basis (*i.e.*, every thirty [30] days or sooner).

Users with Privileged Access will not extend a user group's permissions if such permissions would provide inappropriate access to any user within that group.

Privileged User Password Complexity Requirements

A strong password as defined by the Bank is twenty-five (25) characters with all four of the following attributes:

- Uppercase letters,
- Lowercase letters,
- Base ten (10) digits (*i.e.*, 0 through 9),
- Special characters (*i.e.*, !, $, #, %).

When technically feasible, all Applications, IT Infrastructure, IT Network Infrastructure and Computing Devices will contain a login banner which conveys the following:

- This computer and network are provided for use only by authorized members of Apple Bank;
- The use of this computer and network are subject to all applicable policies, procedures and standards of the Bank and any applicable laws and regulations;
- The use of this computer or network constitutes acknowledgement by the user that he/she is subject to all applicable laws, regulations and Policies, Procedures and Standards of Apple Bank.
- Any other use is prohibited.

f. Entitlement Reviews (Review of Access Rights)

Throughout the user account lifecycle, status changes such as promotions, transfers, demotions or terminations that alter a user's access rights or permissions must be reviewed and revised as necessary to ensure access remains limited only to those accounts that the user has a legitimate business purpose and authorization to access.

A formal account (including privileged accounts and shared drive permissions) review process will be developed and must be conducted at least annually and documentation of the review should be retained based upon the Bank's *Data Retention Policy*.

The following actions should be taken during the review:

- Remove or disable any accounts (including privileged accounts and shared drive permissions) belonging to individuals who have left the Bank, to the extent not addressed during normal business processes;
- Remove or disable any accounts or permissions (including privileged accounts and shared drives) for individuals who no longer require the account or permissions based on their current job function, to the extent not addressed during normal business processes; and
- Ensure that no unauthorized privileged accounts have been created.

4. Escalation Procedures

The Policy Owner will monitor this Policy. Any non-compliance with this 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 the Board or Designated Board Committee for further consideration.

Senior management and the Board report, monitor and evaluate this Policy through the Technology and Operations Planning Committee ("TOPC"), Operations and Technology Committee ("OTC"), and Board meetings (or its designated Board Committee), when and as deemed appropriate.

When Applications, Computing Devices, IT Infrastructure and IT Network Infrastructure are identified as being not in compliance with this Policy, the Business Owner or IT must submit a *Self-Identified Issue* within the GRC tool wherein it will be tracked and monitored for the entirety of its life cycle.

Identified discrepancies (*e.g.*, discovery of elevated privileges, violation of least privilege principals) should be remediated immediately. If the identified discrepancy is unable to be immediately remediated (*e.g.*, a technical reason), the Business Owner or IT must submit a *Self-Identified Issue* within the GRC tool wherein it will be tracked for the entirety of its life cycle.

As detailed above, whenever there is a change in a user's employment status (*e.g.*, termination, switching roles or moving between different departments) that user's access will be removed or revised immediately to ensure access is limited to only that needed for legitimate business purposes (*i.e.*, least privilege principal). In instances however where any employee is still required to retain their previous access for a limited timeframe (*e.g.*, to cross-train individuals), the Business Owner or IT must submit a *Self-Identified Issue* within the GRC tool wherein it will be tracked and monitored for the duration of the extended access.

To comply with this policy, for any Applications, Computing Devices, IT Infrastructure and IT Network Infrastructure which is unable to meet the requirements set forth within this policy (*e.g.*, technical limitation) the Business Owner or IT must submit a *Self-Identified Issue* within the GRC tool wherein it will be tracked for the entirety of its life cycle.

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 this Policy on a Biennial (every 24 months) basis prior to the Next Board Review Date. The Policy Owner will track the Next Board Review Date for this Policy and begin the review process early enough to provide ample time for all necessary approvals to occur in a timely manner.

Once the 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 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.

(B) Required Annual (12 Month) Management Review (Policy Level 2)

This Policy shall be reviewed annually by the Policy Owner, in consultation with the Legal Contact, and updated (if necessary).

If the changes are Immaterial Changes (i.e., no change to any substance of this Policy, but rather grammar, formatting, template, typos, etc.), or Material Changes that do not alter the scope and purpose of this Policy or do not lessen a requirement for transactions or actions governed under this 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).

If the changes are Material Changes that alter the scope and purpose of this Policy or lessen a requirement for transactions or actions governed under this Policy (e.g., lowering a loan review threshold from $5k to $3k), then this Policy shall be submitted to the Designated Management Committee for review and recommendation of the updated Policy to the Designated Board Committee for review and final approval. If the Designated Management Committee cannot agree on an issue or a change to the Code, it shall be submitted to the EMSC for consideration.

Once the updated Policy has received final approval by either the Designated Management Committee or 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 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.

V. OFF-CYCLE REVIEW AND APPROVAL PROCESS

Off-Cycle Policy Changes – Review and Approval Process (Policy Level 2)

If the Policy requires changes to be made outside the Regular 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 consultation 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 must communicate their exception requests in accordance with the process outlined in the bank's Exception Policy which covers all non-lending related exceptions. This includes, but is not limited to, staff entering the exception into the bank's system of record (GRC) and a review by second-line-of-defense to assess the potential risk and determine if it needs to be escalated to an appropriate governance committee for awareness or approval.

VIII. RETIREMENT OF POLICIES

In the event this Policy needs to be retired or merged with or into another Policy, the Policy Owner must notify the PPA and provide a rationale for the proposed retirement or merger. The Bank's General Counsel and Chief Risk Officer will review the rationale and determine whether the requested action is appropriate. Notice of retired Policies shall be provided to the Board or relevant Designated Board Committee on a semi-annual basis.

IX. ROLES AND RESPONSIBILITIES

The key roles and responsibilities for this Policy are summarized below:

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

Designated Board Committee: The Designated Board Committee provides general oversight over management's administration of the Policy. The Designated Board Committee is responsible for initially approving this Policy and reviewing the Policy on a Biennial basis according to the Policy Level (*refer to the Review and Tracking Chart*).]

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.

Executive Management Steering Committee ("EMSC"): To the extent necessary, the ESMC shall consider matters that cannot be decided by the Designated Management Committee.

Information Security ("InfoSec"): InfoSec is Responsible ("R")[1] and Accountable ("A") for the oversight of IAM activities and to conduct privileged user reviews, user recertifications and other entitlement reviews. InfoSec review and approval is required for privileged access requests. In addition, InfoSec will Consult ("C") and Inform ("I") Information Technology ("IT") on best practices for user account security, account management, Authentication Management requirements for user and Privileged Accounts to the extent needed, that align with the requirements of this 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.

Information Technology ("IT"): IT is Responsible ("R") to provision, deprovision and create, modify and delete accounts and to deploy configurations (*e.g.*, set account inactivity timer values, enforce password complexity requirements) to the extent needed, that align with the requirements of this Policy.

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.

Legal Contact: *See Section II – Definitions*.

Policies and Procedures Administrator ("PPA"): *See Section II – Definitions*.

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 the Regular Board Review Cycle for this Policy, and re-evaluates the same at least annually.

[1] All references herein to "Responsible", "Accountable", "Consult" and "Inform" tie back to the *Information Technology ("IT") / Information Security ("InfoSec") RACI (Responsible, Accountable, Consult & Inform) Matrix*

X. 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.

XI. 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.

XII. LIST OF REFERENCE DOCUMENTS

1. AFH IT Asset Management Policy
2. Data Classification Policy
3. Exception Policy
4. IT/InfoSec RACI Matrix
5. Identity and Access Management Procedure
6. User Access Procedures
7. Data Governance Policy

XIII. REVISION HISTORY

Version	Date	Description of Change	Author	Approver
1.1	10/15/2019	Creation of Identity & Access Management	Chief Technology Officer ("CTO")	Board Risk Committee ("BRC")
2.0	02/24/2021	Complete revision of Identity & Access Management ("IAM") Policy, including the merger of content from the prior Password Policy (which will subsequently be retired)	Joseph Martano AVP, Cyber Risk Analyst	Management Risk Committee ("MRC"); Board Risk Committee ("BRC")

XIV. APPENDIX 1

Control Reference(s)

Assets	Computing Devices, IT Infrastructure, IT Network Infrastructure & Applications
Examples (not a complete list)	▪ IT Assets (*e.g.*, servers, endpoints, virtual) ▪ Applications and Web Portals
Controls	▪ Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]: ○ An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and ▪ Procedures to facilitate the implementation of the access control policy and associated access controls; and ○ Reviews and updates the current: ▪ Access control policy [*Assignment: organization-defined frequency*]; and ▪ Access control procedures [*Assignment: organization-defined frequency*]. ▪ Separates [*Assignment: organization-defined duties of individuals*]; ▪ Documents separation of duties of individuals; and ▪ Defines information system access authorizations to support separation of duties. ▪ Enforces a limit of [*Assignment: organization-defined number*] consecutive invalid logon attempts by a user during a [*Assignment: organization-defined time period*]; and ▪ Automatically [*Selection: locks the account/node for an [Assignment: organization-defined time period*]; locks the account/node until released by an administrator; delays next logon prompt according to [*Assignment: organization-defined delay algorithm*] when the maximum number of unsuccessful attempts is exceeded.
Control Source	NIST SP 800-53 Rev. AC-1, AC-2, AC-3, AC-5, AC-6, AC-7