Apple Financial Holdings, Inc.
IT Asset Management Policy

September 17, 2021

Contents

POLICY NAME: IT ASSET MANAGEMENT POLICY

REVIEW AND TRACKING CHART

Effective Date*:	September 17, 2021
Version Number:	1.5
Policy Level:	Policy Level 2
Corresponding Board Review Frequency:	Biennial (Every 24 Months)
Board or Designated Board Committee:	Board Operations & Technology Committee (O&T)
Last Board Review Date*:	September 2020
Next Board Review Date*:	September 2022
Designated Management Committee:	Technology Operations Planning Committee (TOPC)
Last Management Review Date*:	September 17, 2021
Next Management Review Date*:	September, 2022
Policy Owner:	Debi Gupta, CTO Technology Department

I. POLICY PURPOSE STATEMENT AND SCOPE

The AFH IT Asset Management Policy (the "Policy") applies to the implementation, management, monitoring and compliance with IT Asset Management ("ITAM"), to the extent applicable, 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.

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

II. DEFINITIONS

- **Annual or Annually:** Every twelve (12) months.
- **Biennial or Biennially:** Every twenty-four (24) months.
- **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.
- **End of Life (EoL):** The point in time when the support vendor indicates that an asset has reached the end of its useful life. At this point, the vendor will either end (see End of Support [EoS]) or limit support for the asset. Extended support [including bug-fixes and security updates] may be available after this point, for a fee.
- **End of Support (EoS):** The point in time when the support vendor indicates that it will no longer provide standard or extended support [including bug-fixes and/or security updates] for an asset, even for a fee.
- **End of Useful Life (EoUL):** The point in time in which an asset has fulfilled the purpose for which it was required, according to AFH. This point-in-time may or may not match the EoL cycle indicated by the vendor or manufacturer. Reasons for invoking EoUL may include but are not limited to newer technology, degraded performance, incompatibility or security concerns.
- **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 Asset:** Anything (tangible or intangible) that has value to the organization, including, but not limited to, a computing device, IT system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., servers, workstations, routers, switches, firewalls, keyboards), as well as people and intellectual property (including software). Such IT Assets are managed and maintained by Apple Bank and exclude those managed and maintained by 3rd party service providers (e.g., Application Service Provider assets), with the exception of the business application service catalog management task itself. Refer to the IT Operating Model for details on support types and management responsibilities and the AFH Vendor Risk Management Policy for vendor risk management requirements.

Note: IT Assets are the lowest level at which technology is planned, acquired, implemented, and operated. All IT hardware and software shall be associated with the comprising system/investment and tracked and monitored throughout their lifecycles in accordance with AFH ITAM processes.

- **IT Service Management (ITSM):** The implementation and management of quality IT services that meet the needs of the business. IT service providers perform ITSM through an appropriate mix of people, processes, and information technology. See also "Service Management."

- **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.

- **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.

- **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 Management:** A set of specialized organizational capabilities for providing value to customers in the form of services.

- **Technology Management**: The management of Information Technology to include network and infrastructure, applications, systems, people and services. Includes process-driven approaches towards management, focusing on customer need, and activities to design, plan, deliver, operate and control services offered to customers. Managed by the Chief Technology Officer (CTO), reporting to the CEO, and several reporting divisions to include Business Continuity and Disaster Recovery (BC/DR), Change Management, Data Warehouse, Digital Operations and Items Processing, Governance Risk and Compliance (GRC), Infrastructure and Support, and Systems and Standards. In addition, the Chief Information Security Officer (CISO), reporting to the Chief Risk Officer, provides IT and Information Security risk management governance and oversight from a 2nd line of defense position.

III. KEY POLICY COMPONENTS

1. Executive Summary

This document establishes the AFH policy for managing information technology (IT) assets throughout their entire lifecycle. It establishes the business rules and guidelines for consistency and compliance in executing the AFH Information Technology Asset Management process and procedures. AFH Technology Department maintains detailed process and procedures documents separate from policy documents to support continuous refinement of processes and procedures in an effort to mature the Bank's IT management continuously.

2. Objectives

AFH acknowledges the need to manage its IT Assets throughout the five lifecycle stages (**planning, acquisition, deployment, management** and **retirement/disposal**) in a centralized IT Asset repository that accounts for the presence and purchase of all hardware and software. (See Appendix A: IT Asset Lifecycle Management Overview for details.) Therefore, AFH is establishing this Policy and the ITAM program to implement a systematic process that joins contractual, financial, inventory and IT governance functions to support 1) management of IT Assets throughout their lifecycles and 2) strategic decision-making for the AFH IT environment.

The main objective of this Policy is to ensure formal, centralized ITAM capabilities, including software license management (SLM), a proactive approach to software asset management including business application service management via Application Portfolio Management (APM), Software Asset Management (SAM), and Hardware Asset Management (HAM). These centralized ITAM capabilities will enable AFH to (a) control IT costs, (b) facilitate negotiations with IT vendors, (c) manage the risk of licensing agreement violations, and (d) work towards a decrease in vulnerabilities that may lead to a cyberattack on the AFH infrastructure. Implementing the ITAM program will also achieve compliance with AFH Information Security Program Policy; relevant regulatory mandates, policies, and guidance, including, but not limited to, GLBA, FFIEC, FDIC, NYDFS, FRB and CFPB; industry standards such as NIST and ITIL; as well as the Payment Card Industry Security Standards Council (PCI SSC).

3. Key Components of Policy

a) General Controls

AFH Technology Management must act in a fiscally responsible manner, to include implementing an ITAM program to support the optimization of IT costs to perform mission and business functions in the most efficient manner that adds the most value.

Technology Management develops ITAM processes and procedures for program implementation, built around the five lifecycle stages: **planning and budgeting**; **acquisition**; **deployment**; **management**; and **retirement or disposal**. Processes must include clearly-defined roles and responsibilities, proper governance and controls, and integration points with other processes. Processes should trigger changes to contract terms and conditions to accommodate for changing technology, vendor, and internal requirement.

Technology Management must develop, maintain, and communicate to end users this policy and ITAM processes and procedures, and their integration with other policies and processes that support the management of IT Assets and services.

Technology Management must acquire and implement an asset management tool to support core lifecycle processes, and, to the extent practicable, integrate the solution with recognized ancillary data sources used to maintain the asset data (e.g., IT help desk).

b) Planning and Budgeting

Technology Management should analyze usage and other data to make cost-effective decisions and inform IT resource planning, budgeting, and future acquisitions.

The IT Asset inventories and usage should be assessed and controls established to ensure maximum use of IT equipment, installed software, and services (i.e., ensure that AFH needs, and is using, all IT Assets that the Bank is paying for). This is key to performing demand management.

As a guideline, Technology Management should—in an ongoing manner—right-size the number of IT Assets, operational requirements [including continuity of operations] and initiatives designed to create efficiency through the effective implementation of technology. Right-sizing denotes a process by which some level of review and capacity planning is performed to ensure the right amount of technology (i.e., no more, no less) is acquired and deployed to employees to ensure an adequate balance of operational efficiency. In addition, Technology Management and all Technology department employees should promote further efficiencies in IT by leveraging appropriate IT solutions that consolidate activities such as desktop services, email and collaboration tools.

Technology Management must analyze the risk of EoL and EoS, in accordance with the *AFH Information Security Program Policy*, and—in collaboration with Information Security and the business lines—must implement plans to manage that risk appropriately.

c) Acquisition

All AFH employees must perform all hardware and software acquisitions in accordance with the *AFH Vendor Risk Management* and *AFH Enterprise Project Management Office* policies.

AFH employees should only acquire IT Assets on the AFH Technical Reference Model (TRM), the standardized list of technologies and versions approved for use in the AFH production environment, instead of purchasing duplicative technologies, provided an approved technology meets the business need. Employees must follow the process for alternatives and exceptions for the approval of any nonstandard assets.

d) Deployment

The Technology department must establish a comprehensive IT Asset inventory by identifying and collecting information using automated [where feasible] discovery and inventory tools. Inventory processes may be manual only where automation is not practicable.

Any tool used for Software Asset Management (SAM) must specifically collect information about software license agreements and track and maintain identified software licenses to assist the agency in implementing decisions throughout the SLM lifecycle.

In addition to the above, asset catalog processes must also capture the vendor's EoL and EoS dates for purposes of replacement/disposal planning and risk management.

e) Management

Technology Management should maintain comprehensive IT Asset data by tracking all assets from purchase to retirement and disposal, including data collected at integration points with ITSM (e.g., capacity management, configuration management, incident management, and service-level management).

Business Application Services Custodians (i.e., employees in or outside of IT who are responsible for the general management of business application services) are responsible for reporting all acquired software to IT for further management purposes in an effort to ensure all software [and applicable licenses] is tracked and maintained.

Technology Management should ensure that the hardware and software asset management lifecycle processes have integration points with the ITSM processes, primarily with configuration and change management, because the processes impact each other (i.e., a change to a platform may affect licensing).

Technology employees must ensure that assets are receiving patches in a timely manner and are configured securely (i.e., hardened) in accordance with the *AFH Information Security Program Policy* and *AFH Vulnerability Management Policy.* Additionally, employees must maintain version control in compliance with underlying contracts where applicable.In the event Technology Management determines assets must continue to be implemented (i.e., used in the production environment) past their EoL or EoS dates, Technology Management, [in collaboration with the Information Security department], will identify and implement the appropriate mitigating controls. Technology Management also must adhere to the *Exception Policy* to confirm that risks are communicated and understood by relevant stakeholders (i.e., the Board of Directors, Board committees, Executive Management, etc.)

Software License Management (SLM) should be centralized within the Technology department. Technology Management should provide awareness and education relevant to SLM to improve understanding of legal and compliance requirements, including what is expected of users with regard to the protection of intellectual property rights.

The Technology Department should monitor the performance of the program and IT Assets by developing compliance reports (reporting, at a minimum, the compliance position of managed software through proper SLM) and by developing key performance indicators (KPIs) to quantify the performance of the ITAM program. Some asset and configuration management KPIs to consider [as a guideline] may include:

- Percent of software licenses deployed relative to the total software licenses purchased
- Percent of licenses purchased but not accounted for in the asset repository
- Percent of IT Assets nearing and currently in EoL and/or EoS state
- Percent of software assets under maintenance contract
  Note: This KPI monitors the number of deployed software assets that are within their warranty or covered by a valid maintenance contract relative to the total number deployed.

Technology Management should actively manage AFH's relationships with vendors to develop, manage, and control vendor contracts, relationships, and performance for the efficient delivery of contracted products and services; minimize potential business disruption; and derive the most value from vendors. Refer to the *AFH Vendor Risk Management Policy* for details.

f) Retirement / Disposal

If AFH elects to retire/dispose of assets, the *Apple Bank Disposal of Documents Procedure,* the *Record Retention and Disposal* Policy, and the *IT Asset Management Procedure* must be followed.

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.

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(A) 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. Any exception to this Policy must be made in accordance with the

requirements set forth in Apple Bank's Exception Policy.

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.

Internal Audit: 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.

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.

Chief Information Security Officer (CISO) or Delegate Thereof:

- Is responsible (R[1]) for developing and continually enhance the *AFH Information Security Program Policy*.
- Provide guidance and direction to Technology Management (i.e., is consulted [C[1]]) on the development of information security controls and analytics (i.e., KRIs, KPIs) to ensure related risks are appropriately managed.
- Is responsible (R[1]) for performing various risk assessments for IT Assets and reports the results to the Designated Management Committee(s) and/or Designated Board Committee(s), or the Board, as appropriate.
- Is informed (I[1]) as to the results of the ITAM process through reports and/or direct access to the related ITAM tools.

Chief Technology Officer (CTO) or Delegate Thereof is accountable (A[1]) to:

- Establish an ITAM program and ensure executive sponsorship and governance.
- Define policy, process, and procedures for ITAM to include automated, repeatable processes to aggregate software license and maintenance requirements and associated funding, as appropriate, for commercial and commercial off-the-shelf (COTS) software acquisitions. The processes should include a means to review existing software that is currently in use against AFH's approved list of software and provisions for identified software not on the approved list (i.e., consider whether to add the product to the approved list or identify an approved alternative to replace it).
- Ensure appropriate management, through policy and procedure, of all AFH commercial and COTS software agreements and licenses.
- Ensure the recording of AFH inventory of IT Assets on a designated and approved frequency, including an inventory of all IT Assets, software licenses purchased, deployed, and in use, as well as expenditures on subscription services (including provisional SaaS).
- Ensure compliance with software license agreements, consolidation of redundant applications, and identification of other cost-saving opportunities.
- Review and approve all IT acquisition strategies and plans. For contract actions that contain IT that is outside of an approved acquisition strategy or acquisition plan, the CTO shall review and approve the action itself (e.g., procurement actions for alternatives or exceptions when existing approved solutions do not meet a business need).
- In consultation with leadership, evaluate the appropriateness of IT-related portions of statements of need (requests for proposal) or statements of work, especially in respect to the mission and business objectives supported by the IT strategic plan and in alignment with mission and program objectives.
- As member of the TOPC and NPI Committee, provide advice and approval recommendations [as appropriate] on technology acquisition strategies and plans.
- Ensure effective implementation of routine/continuous diagnostics (assessments) and mitigation for the Bank and integration with the ITAM program and tools.

IT Infrastructure Management is responsible (R[1]) to:

- Management Focus: Enterprise Architecture

[1] RACI: Responsible (R), accountable (A), consulted (C), and informed (I).

- Collaborate with business departments and IT Business Continuity leadership on the future state architecture to ensure business resiliency and continuity.
- Maintain the TRM, the list of technologies and the version(s) approved for the current production environment, the legacy technologies that should be retired/decommissioned, as well as determine future technologies that align with the target architecture and IT/IM strategic plan and roadmap.
- Own, implement and maintain the Alternative and Exception process for determining if a technology or version should be added to the TRM and allowed into the production environment.

- Management Focus: IT Assets (General)
  - Make key program decisions with the support of executive leadership.
  - Manage and coordinate all aspects of the ITAM program.
  - Ensure proper coordination and seamless process flows with related programs and services.
  - Ensure overall effectiveness and efficiency of the ITAM process and procedures.
  - Oversee ITAM communication and education to all stakeholders, including end users and ITAM staff.
  - Comply with relevant regulatory mandates, AFH policy and procedures.
- Management Focus: Software Assets
  - Reporting to the CTO, lead a Bank-wide effort, working in collaboration with Vendor Risk Management, as appropriate, to centralize license management, implement strategies to reduce duplication, and ensure the adoption of software best practices.
  - Manage, through policy and procedure, all Bank-wide commercial and COTS software agreements and licenses.
  - Employ a centralized SAM strategy that includes development of an approved list of software and an associated implementation plan. This plan should address, at a minimum, the lifecycle phases, funding aggregation, and other considerations, including the use of SaaS.
  - Catalog all business application services (e.g., BAM+, MISER) and endpoint out-of-the-box software (e.g., Microsoft Office, Adobe Acrobat) and related details on the CTO-set frequency. See the *IT Asset Management Procedures* and *Business Application Service Catalog Procedures* for details.
  - Lead an evaluation of software products in the AFH IT environment to validate that they are meeting business needs based on technical requirements.
  - Increase the use of Bank-wide software license agreements and implement strategies to reduce duplication of products meeting the validated needs.
  - Ensure, through effective market research, that terms and conditions in commercial license agreements are consistent with customary practices to the maximum extent practicable and are negotiated to meet the Bank's needs.
  - Ensure that the personnel involved in SAM (e.g., legal, acquisition, system administration, technical support, and users (as appropriate)) are trained in relevant software management topics, such as intellectual property and software contracts, license negotiations, license compliance laws, regulations, software audits, security planning, configuration management, provisional services (i.e., SaaS), and compliance.
  - Develop and implement an assessment and approval process to determine the cost and benefit of purchasing software maintenance programs. The process should include a means of assessing operational impacts and risks, including information security and privacy.

- Develop and execute the Bank's software management centralization plan in an effort to centralize license management, implement strategies to reduce duplication, and ensure the adoption of software management best practices.
- Ensure the risk related to EoL and EoS is appropriately managed.

- Management Focus: Hardware Assets
  - Implement and build controls for the hardware inventory to ultimately associate assets to lifecycle, status, locations, and documentation for hardware devices.
  - Catalog all hardware assets and related details on the CTO-set frequency. See the *IT Asset Management Procedures* for details.
  - Maintain visibility into hardware asset processes and build controls for hardware assets throughout the lifecycle to maximize value, provide data on hardware assets to support customer demand, maintenance and operations, and strategic decision-making.
  - Develop, implement, and promote policies, processes and procedures [as appropriate] for hardware asset acquisitions, installations, usage, and disposition.
  - Manage, through policy and procedure, hardware assets.
  - Ensure the risk related to EoL and EoS is appropriately managed.

Business Application Services Owners are responsible (R[2]) to:

- Ensure all business application services (software) is reported to IT for ITAM purposes.

X. RECORD RETENTION

Any records created as a result of this Policy should be held pursuant to the Bank's Record Retention and Disposal 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

The following documents are referenced within this Policy:

- *AFH Enterprise Project Management Office*
- *AFH Exceptions Policy*
- *AFH Information Security Program Policy*
- *AFH IT Operating Model*
- *AFH Record Retention Policy*
- *AFH Vendor Risk Management Policy*
- *AFH Vulnerability Management Policy*
- *Apple Bank Disposal of Documents Procedure*

[2] RACI: Responsible (R), accountable (A), consulted (C), and informed (I).

XIII. REVISION HISTORY

Version	Date	Description of Change	Author	Approver
1.0	September 2020	New policy.	A. Scarola	Board Operations & Technology; Technology Operations Planning Committee (TOPC)
1.5	September 2021	Updated policy to reflect enhancements in the definitions, changes related to external related policies, end-user responsibilities, and conformance to the policy template.	A. Scarola	Technology Operations Planning Committee (TOPC)

XIV. APPENDIX A: IT Asset Lifecycle Management Overview

IT Asset lifecycle management is a core process of ITAM that involves managing and optimizing the purchase, deployment, maintenance, use, and retirement or disposal of assets within an organization. Implementation of this process can benefit organizations by improving the ability to forecast needs. IT Asset lifecycle management strives for informed purchasing decisions, proactive resource replenishment, improvement of the quality of IT services, and knowledge of the total cost of ownership of an asset. Activities include the development and maintenance of policies, standards, processes, systems, and measurements that enable organizations to manage the IT Asset portfolio with respect to risk, cost, control, IT governance, compliance, and established business performance objectives. Figure 1 provides an overview of the ITAM lifecycle management process.

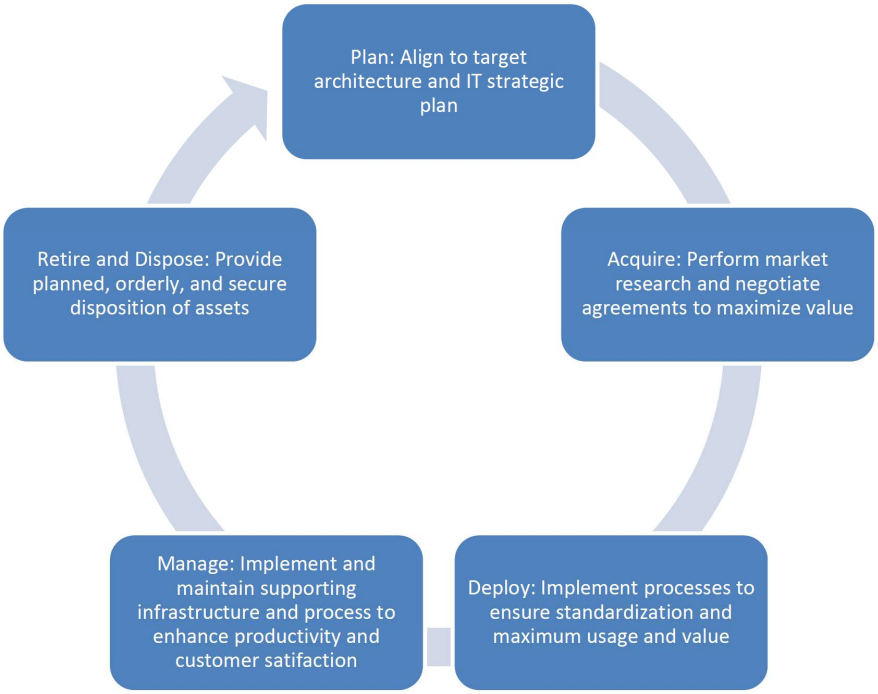

Figure 1. IT Asset Lifecycle Management Process

Plan

The planning phase involves the activities performed before procurement of the software, which include evaluating the technical and organizational requirements for the IT Asset. Asset requirements are defined based on an assessment of both service delivery needs and the capability of the existing asset base to meet these needs. Planning activities include, but are not limited to, defining the asset management strategy, planning for uncertainties, documenting business cases, and performing a cost-benefit analysis.

Acquire

For ITAM purposes, the acquisition phase is the process by which an organization plans and then manages the procurement process. This includes receiving a legitimate request and approval for goods and services (including standards, definitions, and supplier identification) and discounting targets and policies under negotiated discounts and contracts. Ultimately, the goal of the

procurement process is to enable the best price for the best product and service available to meet the organization's needs while providing full visibility to surplus.

Deploy

The deployment phase involves deploying new software and hardware requests through the defined approval method. If the asset request has been approved, the IT configuration manager will install software and hardware on the user's machine. He or she will ensure that the equipment is fully configured and ready for use. The asset repository must be correct before allocating any equipment. The asset entry should also include all software and hardware installed. Because the information about the asset will never be more accurate than it is at this stage, a best practice is for the IT Asset manager to determine the accuracy of the asset as it enters the configuration management database to enable a clean start.

Manage

The management phase involves the monitoring of an asset's maintenance needs and performance, management of refresh cycles, information management, asset valuation, and continuous assessment of the asset's use and functionality. Responsible parties should evaluate the existing asset's base condition, capability, and usage. Accurate recording, identification, valuation, and reporting procedures must be established so that informed decisions to maintain, modify, rehabilitate, find an alternative use for, or dispose of an asset, can be made.

Retire/Dispose

The retirement and disposal phase involves the planning and execution of the removal and disposal of assets, closing or cessation of contracts and licenses, and proper de-installation. The treatment of an asset that has either reached the end of its useful life, is considered surplus, or is underperforming. Retiring an asset can include disposal, replacement, renewal, or redeployment. Responsible parties should comply with relevant approval processes and, where possible, select a method, including retirement, replacement, renewal, or redeployment, that maximizes the financial benefits associated with the method.