Apple Financial Holdings, Inc.

System Development Life Cycle Policy

November 22, 2021

Contents

POLICY NAME: SYSTEM DEVELOPMENT LIFE CYCLE POLICY

REVIEW AND TRACKING CHART

Effective Date:	November 22, 2021
Version Number:	2.1
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:	November 18, 2020
Next Board Review Date:	November 2022
Designated Management Committee:	Technology Operations and Planning Committee (TOPC)
Last Management Review Date:	November 19, 2021
Next Management Review Date:	November 2022
Policy Owner:	Debi Gupta, CTO Technology Department

I. POLICY PURPOSE STATEMENT AND SCOPE

The System Development Life Cycle (SDLC) Policy (the "Policy") applies to the development, implementation, management, monitoring, and compliance with System(s) Development at Apple Financial Holdings, Inc. ("AFH"), inclusive of Apple Bank for Savings and its subsidiaries (collectively, "ABS," "Apple," or the "Bank"), to the extent applicable to such entity, in accordance with applicable state and federal statutes, rules and regulations.

All Bank employees and third party resources engaged by the Bank that perform System(s) Development under the auspices of the Bank must comply with the terms of this Policy to the degree applicable to them. Other third-party resources (vendors/manufacturers) must have appropriate and secure SDLC processes in place, in-line with this Policy and considering a risk-based approach, to be reviewed through the vendor management onboarding and review process.

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.
- **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.
- **Information Technology (IT) System(s):** A set of technologies (i.e., Hardware, Software, network, etc.), working together as parts of a mechanism or an interconnecting network.
- **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.

- **Software:** Also "application". Anything from a single program [or suite of programs] to larger constructs such as an operating system, an operating environment or a database, on which various smaller application programs, processes or workflows can run. The term includes but is not limited to software code; desktop/mobile/web applications; commercial off-the-shelf applications; 3rd party business applications/services; embedded software [controlling machines and devices]; reports; and application, network and operating system scripts. Bank acquired or developed Software is considered an IT Asset as defined by the IT Asset Management Policy.

- **Software Development:** Also "application development". The translation of a business need into a computer software product. As of this Policy version, the Bank performs application-level development within three categories: 1) report writing; 2) screen and logic coding; and 3) data interfacing/conversion and related scripting.

- **System(s) Development:** A process for the development and deployment of information systems which may include hardware only, software only, or a combination of both. Note that Systems Development may include Software Development when required.

- **System Development Life Cycle ("SDLC"):** A framework outlining the requirements for the development, acquisition and implementation of strategically important IT Systems (i.e., those systems critical to the Bank's operation). The SDLC does not apply to or include business-as-usual (BAU) or maintenance activities to existing non-critical Systems, which would only follow the *Technology Change Management Policy* and related procedures.

- **Triennial or Triennially:** Every thirty-six (36) months.

III. KEY POLICY COMPONENTS

1. Executive Summary

This document outlines ABS's Policy with respect to the implementation, management, monitoring, compliance with the principles and standards for the development and implementation of systems.

2. Objectives

The objective of the SDLC Policy is to document and inform relevant stakeholders and users about the Bank's system(s) development principles in adherence with applicable laws and regulations (GLBA, FFIEC, NYDFS); industry standard practices (e.g., NIST); and with the Payment Card Industry Security Standards Council (PCI SSC) requirements.

3. Key Components of Policy

A. SDLC Phases

Structured SDLC techniques enhance the control over related projects by dividing complex tasks into manageable phases, allowing time to review each for successful completion before allocating resources to subsequent phases. Some SDLC projects will be facilitated and managed by the Enterprise Project Management Office (EPMO) and must follow the EPMO project management process in addition to adhering to the SDLC phases. See the *Enterprise Project Management Office Policy* for details. The four SDLC phases are: ***plan, create, test*** and ***deployment***. Prior to planning an SDLC project, a feasibility study (an assessment of the practicality and pre-determined justification of the system) must be performed by the business / product owner and the outcome results in system development as a viable option as approved by the CTO. At a minimum, the two criteria to judge feasibility are cost and value to be obtained.

1. Plan

After a system development project is identified, a viable strategy for deployment must be developed. This includes exploring how new functionality may improve the Bank's presence in our market, impact operations and impact Bank employees after the proposed deployment of new systems. The depth and formality of the plan should be commensurate with the characteristics and risks of the project. At a minimum, all SDLC project plans must clearly define the requirements for the business and for each additional phase (creation, testing and deployment), depending on the scope of the project.

2. Create

After the SDLC project plan is developed and approved, system creation can begin. This includes development of the functional user requirements, technical requirements, the human resources and technology components (hardware and software) and the estimated costs to complete the project. Technology employees will work closely with business stakeholders, Risk Management [to include Information Security], third-party and other applicable stakeholders to envision both the detailed requirements and architecture of the SDLC project. Obtain approval for and procure system development (i.e., programming, coding, report-writing), packaged application software and/or system hardware as needed. See the *Vendor Management Policy* for details. Next, the necessary segregated

environments must be established (i.e., development, test and production) in accordance with the plan; and the system is created in preparation for deployment testing.

If software development will be required as part of the system, and if that software will be used in conjunction with critical and/or sensitive Bank information, at a minimum, a software development plan must be documented to address the areas of preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; general design; detailed design; development; quality assurance and acceptance testing; implementation; post-implementation maintenance and review. Appropriate controls must be designed into the software to validate correct processing with respect to their handling of input data, internal processing, inter-process messaging, and message integrity and output data, to prevent errors, loss, unauthorized modification or misuse of sensitive information. This methodology ensures that the software will be adequately documented and tested due to the potential high level of risk. Development must be performed in accordance with IT secure coding requirements inclusive of regulatory requirements, Bank policy and industry best-practices. Information Security Department should be consulted for these coding and testing standards and guidelines.

3. Test

After creation, the new system must be tested in accordance with the documented test plan and the stakeholders' requirements to include functionality, interoperability (i.e., with vendor-supplied technology) and security. Testing must be performed in a non-production, test environment. Development and quality assurance/test staff must not be permitted access to production systems unless absolutely required by their respective job duties/descriptions and only after approval by the CTO.

Where software development is required, software test engineers must perform appropriate testing to confirm each component of the code works in accordance with business and other stakeholder's requirements.

The Bank must strive to not test with live, sensitive (confidential and/or restricted) data, due to the threat to its confidentiality and/or integrity. If the system allows it, testing of systems must be accomplished with anonymized (e.g., encrypted, masked, etc.) data that mimics the characteristics of real data, or on copies of real data with any sensitive (confidential and/or restricted) data appropriately sanitized, obfuscated or otherwise protected. As a general principle, the risk of test data disclosure should be less than that of the production environment. Information Security and related Data Protection Policies should be consulted for guidance, as needed.

Data output from applications should be validated to confirm that the processing of stored information is correct and appropriate to the circumstances.

Application testing must occur and any defects found within the system during testing must be addressed, risk-assessed and prioritized for resolution before software is moved into production.

Governance documentation regarding the use of the system (i.e., procedures and/or user manuals) must be developed. Revisions and final approval may occur shortly after

deployment but before the project is complete.

New product/service/technology systems involving personal information processing activities may require a Data Protection Impact Assessment (DPIA); consult the Privacy Office to obtain a determination. Its purpose is to ensure appropriate controls are implemented. See the *Apple Bank Privacy Policy* and the *Data Protection Impact Assessment (DPIA) Process* document for details.

Business line management approval is required before moving on to the Deployment phase.

4. Deployment

After final system testing is complete and stakeholders and customers accept the solution, the system is transitioned to production, with CTO approval, with the intention of meeting the requirements gathered from the above phases. Refer to the *Technology Change Management Policy* for detailed requirements.

After the system is moved into production, User Acceptance Testing (UAT) should be completed as well as user training. A Post Implementation Evaluation Report should also be completed to ensure the system is functioning properly per stakeholder requirements. If required per evaluation results, any modifications, configuration changes and/or bug fixes should also be performed. After the system has been in production with ample time for use, a user satisfaction survey should also be completed to gauge usefulness and productivity of the system. Refer to the *System Development Life Cycle Procedure* document for further guidance and details.

Documentation regarding the use of the system (i.e., procedures and/or manuals) must also be finalized and approved before the SDLC project is complete. The system must be appropriately recorded (i.e., inventoried) for future maintenance, security, support and End of Life (EoL) / End of Support (EoS) planning and other requirements. See the *IT Asset Management Policy* and related procedures for details.

After all required deployment steps are complete and final user acceptance testing and stakeholder/business line management sign-offs are received, the SDLC project is complete.

B. System Support and Disposal

After deployment, the system must be administered, supported and maintained to include production and EoL/EoS planning in accordance with the *IT Asset Management Policy*, *Information Security Program Policy*, *Vulnerability Management Policy*, *Service Desk and Problem Resolution Policy*, *Record Retention and Disposal Policy,* and *Vendor Management Policy*.

C. Documentation

All SDLC project documentation must be updated and maintained during all phases of the project. Documentation must be archived in accordance with retention requirements, for at least the life of the system. See section X, *Record Retention*, for detailed requirements.

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(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. 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 (R[1]) 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 (R[1]) for initially approving this Policy and reviewing the Policy on a [Annual, Biennial, Triennial] basis according to the Policy Level (*refer to the Review and Tracking Chart*).]

Designated Management Committee: The Designated Management Committee is responsible (R[1]) 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

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

Board Committee, or Board, as appropriate.

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

Senior Management: Members of management and business units are responsible (R^2) 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.

Internal Audit: The Internal Audit team is responsible (R^2) 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.

CISO and Information Security: The CISO and the Information Security Department is accountable (A^2) to provide effective oversight and governance to ensure that all Information Security policies, processes and procedures are being adhered to for the purposes of system acquisition, development, and maintenance. This includes, but is not limited to, roles and responsibilities, operations, monitoring and/or other key components as set forth in the Information Security policy.

CTO: The CTO and his designated representatives are responsible (R^2) to ensure that the Bank's SDLC Policy and processes are adhered to for all related system development projects.

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.

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

XII. LIST OF REFERENCE DOCUMENTS

- Apple Bank Privacy Policy
- Enterprise Project Management Standard Operating Policy
- Information Security Program Policy
- IT Asset Management Policy
- Record Retention and Disposal Policy
- Service Desk and Problem Resolution Policy
- Technology Change Management Policy
- Vendor Risk Management Policy
- Vulnerability and Patch Management Policy

XIII. REVISION HISTORY

Version	Date	Description of Change	Author	Approver
1.0	8/21/18	New policy.	J.Nagle & Y. Zimmermann	Board Operations & Technology
1.1	07/2019	Updated to reflect enhanced CISO role.	K. Shurgan	Board Operations & Technology
2.0	November 2020	Updated to reflect new policy template. Renamed from *Software* to *System*. Aligned with ITIL framework guidelines.	A. Scarola	Board Operations & Technology
2.1	November, 2021	Updated to reflect new policy template. Enhanced definitions, approval requirements, roles and responsibilities.	A. Scarola	TOPC