Apple Financial Holdings, Inc.
Service Desk and Problem Resolution Policy

December 15, 2021

Contents

POLICY NAME: SERVICE DESK AND PROBLEM RESOLUTION POLICY

REVIEW AND TRACKING CHART

Effective Date*:	December 15, 2021
Version Number:	1.3
Policy Level:	Policy Level 3
Corresponding Board Review Frequency:	Triennial (Every 36 Months)
Board or Designated Board Committee:	Board Operations & Technology Committee (O&T)
Last Board Review Date*:	December 15, 2021
Next Board Review Date*:	December 2024
Designated Management Committee:	Technology Operations 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 Service Desk and Problem Resolution Policy (the "Policy") applies to the development, implementation, management, monitoring of service delivery management at Apple Financial Holdings, Inc. ("AFH"), inclusive of Apple Bank for Savings and its subsidiaries (collectively, "ABS," "Apple," or the "Bank"), to the extent applicable to such entity, in accordance with applicable state and federal statutes, rules and regulations.

All ABS employees and third party resources engaged by the Bank must comply with the terms of 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.
- **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.
- **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 3:** A Regular Board Review Cycle level for a Policy, designated by Risk Management in consultation with Legal. Level 3 Policies require Triennial 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.

- **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 development, implementation, management, and monitoring of service delivery management.

2. Objectives

The objective of this Policy is to establish a standardized and consistent approach to providing technical support to all lines of business. The Bank operates an internal service desk tasked with providing technical support to the organization's business divisions, users/customers, and other relevant stakeholders. Regardless of what type of help is being provided, the goal of the service desk is to deliver high-quality service to customers in a timely manner.

3. Key Components of Policy

The Service Desk function provides technical support for Bank applications and systems. The Service Desk responds to inquiries via phone, email, instant messaging (IM) and tickets. The Service Desk consists of dedicated staff trained in problem resolution, equipped with a centralized service management application, and supported with knowledge-based systems that serve as a reference resource to common problems.

The Service Desk is expected to record and track incoming problems and requests. Documentation in the incident management system should include but is not limited to such data as user name and telephone number, problem description, affected system (platform, application, or other), prioritization code, current status toward resolution, the party responsible for resolution, root cause (when identified), target resolution time/date, user status updates, as well as any other pertinent information. The Service Desk must identify and authenticate requestors before providing support or sharing sensitive information.

The incident management system helps prioritize incidents, track problems through resolution, analyze tickets to identify trends or potential systemic issues, and analyze Service Desk overall performance and management. The incident management system supports internet and intranet access so users can monitor ticket resolution.

The Service Desk evaluates and prioritizes issues to ensure the most critical problems receive prompt attention. A few key factors the Service Desk considers when establishing priority include the number of users or customers affected, revenue losses, expenses incurred, reputation of the bank and/or the number of SLAs affected, impacted or breached.

Incident Management

IT service management is broken up into incidents and problems. An incident is defined as any of the following: unplanned interruption in service or loss of quality, a reduction in the quality of a service, or an event that has not yet impacted the service to the customer or user. Incident management is the process of managing the lifecycle of incidents. The purpose of incident management, according to ITIL 4, is “to minimize the negative impact of incidents by restoring normal service operation as quickly as possible.”

A problem is defined as a cause of one or more actual or potential incidents. According to ITIL 4, the purpose of problem management is to “reduce the likelihood and impact of incidents by identifying actual and potential causes of incidents, and managing workarounds and known errors.”

Problem management is the process of managing the lifecycle of all problems that happen or could happen in an IT service.

Problem resolution involves other groups such as: IT Network Infrastructure, IT Server Infrastructure, Information Security, and vendors (where applicable). This document defines the roles and responsibilities of each of these groups and describes the incident management model in detail including severity levels, priority codes and service level response objectives.

Service Desk

The Service Desk manages incidents and requests and is the single point of contact between the end-user and IT. The top priorities of the Service Desk are to ensure a consistent response to problem resolution, service requests, status reporting and notification of changes related to the technology environment. Incidents are events that result in interruption of one or more services. Service Requests do not specifically result in the same degradation or failure. Instead, they are needs or wishes such as enhancements or changes.

Service Desk consists of multiple support levels designed to provide support based on the level of expertise required and criticality of the issue.

- **Level 1** – Basic level support - Requests and incidents are logged into the incident management system. Elementary problems are resolved. Examples: basic “how-to” questions, password resets, account creation, etc.
- **Level 2** – This in-depth technical support. Example: hardware diagnostics.
- **Level 3** – Expert application, system or hardware support. May require the assistance

of Network or Server Infrastructure.

- **Level 4** – Not generally provided by the Service Desk, may be directed to a vendor or external support organization specific to the system or application.

Service Desk Responsibilities

- The Service Desk is expected to provide problem resolution according to the complexity and experience dealing with the specific issue.
- Tickets are well documented to capture information to either escalate or build the knowledge base.
- Service Desk technicians are adequately trained in the technologies and applications implemented within the enterprise.
- Review reports and analyze incidents in an effort to identify trends or potential "problems."

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 Triennial (36 Month) Board Review and Approval Cycle (Policy Level 3)

The Policy Owner is responsible for initiating a Regular Board Review Cycle on a Triennial (every 36 months) basis prior to the Next Board Review Date. The Policy Owner will track the Next Board Review Date for the Policy and begin the review process early enough to provide ample time for all necessary approvals to occur in a timely manner.

Once an 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 3)

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 3)

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 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 Triennial 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 EMSC shall consider matters that cannot be decided by the Designated Management Committee.

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.

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.

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

- N/A

XIII. REVISION HISTORY

Version	Date	Description of Change	Author	Approver
1.0	08/2018	New Policy	P. Nucum	Board Operations & Technology
1.1	07/2019	Update to reflect enhanced CISO role.	K. Shurgan	TOPC
1.2	08/2020	Update to reflect policy changes.	M. Siegel	TOPC
1.3	12/15/2021	Update to reflect revised policy template.	M. Siegel	TOPC and O&T