Apple Financial Holdings, Inc.
Technology Change Management Policy

November 22, 2021

Contents

POLICY NAME: TECHNOLOGY CHANGE MANAGEMENT POLICY

REVIEW AND TRACKING CHART

Effective Date*:	November 22, 2021
Version Number:	2.5
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 30, 2020
Next Board Review Date*:	September 2022
Designated Management Committee:	Technology Operations Planning Committee (TOPC)
Last Management Review Date*:	November 19, 2021
Next Management Review Date*:	September, 2022
Policy Owner:	Anthony Scarola, FVP IT GRC and Change Management Officer

I. POLICY PURPOSE STATEMENT AND SCOPE

The Technology Change Management Policy (the "Policy") applies to the development, implementation, management, and monitoring of Technology Change 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.

- **Change Authority:** The person or group responsible for authorizing a change. The correct Change Authority must be assigned to each type of change to ensure that changes are both efficient and effective. Appropriate Segregation of Duties must exist between a Change Requestor and the Change Authority. Within AFH, the Change Authority includes the Change Advisory Board (CAB) or Emergency Change Advisory Board (ECAB); see *Section IX – Roles and Responsibilities*.

- **Change Owner / Assignee / Implementer**: The individual deemed as an owner of the Change Request throughout the request lifecycle. He/she may also take the role of the Change Requestor and support the process for creating and submitting a Change Request. Appropriate Segregation of Duties must exist between a Change Requestor and the Change Authority. The Change Owner ensures that the necessary tests have been performed [if necessary] so that the change request is followed up by appropriate urgency. The Change Owner would also document the process across the request life cycle.

- **Change Manager / Process Owner**: The Change Manager controls the lifecycle of all Changes. His/her primary objective is to facilitate a dialog with the appropriate stakeholders to help ensure a minimal overlap of the scheduling of Changes and work to ensure minimum disruption to IT services. He/she is also responsible for the appropriate documentation of changes. This individual is also responsible for identifying enhancements to, documenting and communicating the procedures for Technology Change Management. For important changes, the Change Manager will refer the authorization of changes to the CAB; see *Section IX – Roles and Responsibilities*.

- **Change Model**: A repeatable approach to the management of a particular type of change.

- **Change Requester**: The individual who submits the change request, accountable for ensuring that the change meets all Bank policy requirements [as appropriate] and is reviewed by the appropriate manager(s), if applicable. Appropriate Segregation of Duties must exist between a Change Requestor and the Change Authority.

- **Change Schedule**: A calendar that shows planned and historical changes. Used to help plan changes, assist in communication, avoid conflicts and assign resources. It is also used after changes have been deployed to provide information needed for incident management, problem management and improvement planning.

- **Configuration Item (CI)**: Any component that needs to be managed in order to deliver an IT service.

- **Configuration Management Database (CMDB)**: A database used to store configuration records throughout their lifecycle. The CMDB also maintains the relationships between configuration records.

- **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.

- **ITIL:** Previously known as the Information Technology Infrastructure Library. A framework of guidelines and best practices originally developed by the British government's Central Computer and Telecommunications Agency (CCTA) for delivering IT services. It provides a systematic approach to IT service management to assist in the management of risk, strengthen customer relations, establish cost-effective practices and build a stable IT environment that allows for growth, scale and change.

- **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.

- **Request for Change ("RFC")**: The RFC is a documented request for any AFH Technology Change. The RFC includes a description of a proposed change used to initiate change management. The request must be approved by the appropriate Change Authority. Each requested change is categorized as either a "Standard Change", a "Normal Change", or an "Emergency Change." These terms are further defined below in Section III.3.b.1), *Change Categories*.

- **Segregation of Duties**: Addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. It includes dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions[1].

- **Technology Change ("Change")**: The addition, modification or removal of any authorized, planned or supported service or service component that could have an effect on IT services. Such changes may arise reactively in response to problems or externally imposed requirements, e.g. legislative changes, or proactively from seeking improved efficiency and effectiveness or to enable or reflect business initiatives, or from programs, projects or service improvement initiatives. Changes must be applicable to the Bank, add value and meet a business need. Note, access changes related to the logical user access control [to include privileged users] process are excluded from the scope of this Policy. Refer to the *Identity Access Control and Authentication Policy* and procedures for further details.

- **Technology Change Management**: Aims to control the lifecycle of Technology Changes through the use of standardized methods and procedures for efficient and prompt handling of all changes in order to minimize the number and impact of unanticipated issues. In addition, it does this by maximizing the number of successful changes by ensuring that risks have been properly assessed

[1] NIST SP 800-53 Controls: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/control?version=5.1&number=AC-5

[by people who are able to understand the risks and the expected benefits], by authorizing changes to proceed by the Change Authority, and by managing the Change Schedule.

III. KEY POLICY COMPONENTS

1. Executive Summary

This document outlines ABS's Technology Change Management Policy which defines and documents the principles and guidelines implemented by the organization so that modifications to technological Bank assets and Configuration Items (CIs), in accordance with the *AFH IT Asset Management Policy* and the *AFH IT Operating Model*, are captured, transparent, and reviewed. The policy establishes governance, oversight and categories of changes. Additionally, the policy is designed to work in conjunction with and be supported by the *AFH Technology Change Management Procedures* as well as other applicable policies and procedures.

2. Objectives

The objective of this Policy is to establish a standardized and consistent approach to managing and enabling value-added change, in an effort to reduce risks related to unauthorized changes potentially leading to performance, regulatory and/or financial impacts. The Policy provides information and requirements to relevant stakeholders regarding the principles and guidelines AFH employs so that best practices are in place and in compliance with regulatory, legal and other obligations, including—but not limited to—Payment Card Industry (PCI) obligations. By following this Policy, Changes should be streamlined with the aim of avoiding unnecessary bureaucracy by using the full Technology Change Management process only for significant changes.

Effectiveness and efficiency of Technology Change Management should be continuously improved, by creating Change Models and pre-approval methods for reoccurring changes; breaking bigger changes down into smaller, more manageable pieces that carry less risk; and by using automation for checks, testing and deployment.

3. Key Components of Policy

a) Change Request Sources

Changes usually originate from sources including Bank employees; the Technology Service Desk; from regulatory/Audit/self-identified or other issues; directly from 3rd party service providers (i.e., vendors, software manufacturers); the Enterprise Project Management Office (EPMO); the Board; or via technology steering or other Board committees (e.g., New Products and Initiatives Committee [NPIC], Technology Operations Planning Committee [TOPC]); and other areas.

Regardless of the source, all Changes, with the exception of those initiated by 3rd party service providers (vendors), are required to flow through the Technology Change Management Process. Vendors should have their own change management process. When such 3rd party Changes are planned to impact the Bank's self-managed assets, such Changes are required to adhere to the *Technology Change Management Policy*. Refer to *the IT Operating Model Standards* for further details.

b) Change Management Process

The AFH Technology Change Management process follows the general specifications of ITIL, the IT service management industry framework. The five main activities involved in the process are: **record**, **plan**, **approve**, **execute** and **review**.

Record

All Changes, regardless of the type, must be recorded (documented) in the Apple Bank change management platform so that the appropriate stakeholders can understand the reason for and priority of a change. Recording facilitates assessment, review, evaluation, prioritization, scheduling and communication of changes. *See also section X, Record Retention*.

Plan

The goal of the Plan phase is to ensure a successful change while causing minimal disruption to existing services and components. Activities in this phase include aligning tasks and preparing resources and components. This is the point when back-out plans will be developed; i.e., what happens when things go wrong. During this phase, stakeholder engagement and communication is essential, so that the change can address maximum need. If external third parties are involved, contracts should outline the requirements for communications plans and procedures—as applicable—to include change authorization/approvals, implementation coordination and scheduling. Also refer to the *IT Operating Model Standards* for details on management roles and responsibilities. Standard changes might not require much planning, but stakeholder communication and resource planning will still be required. Despite the urgency, emergency changes will require planning, but this can be high-level, requesting less detail compared to normal changes.

1. Change Types

All Changes must be assigned a change type. AFH identifies three types: **standard**, **normal** and **emergency**.

Standard

- Routine, no- to low-risk, pre-authorized, well understood and fully documented, and can be implemented without needing additional authorization.
- Often initiated as a service request, but may also be an operational change.
- Require a risk assessment and authorization by CAB only during creation, or modification due to business change or occurrence of an incident.
- Ideal candidates for automation to help speed up the process and increase efficiency.
- Examples:
  - Software applications on the "pre-approved" list (e.g., standard-build applications such as Microsoft Office); may require appropriate level of manager approval for software requiring acquisition/licenses (e.g., Visio); reference the *Technical Reference Model (TRM) Standards* for details
  - Installation of patches or security configuration enhancements with the

    exception of those requiring immediate implementation with impact to the production environment, as these are deemed “emergency changes”
  - Installation of “pre-approved” non-infrastructure hardware components (workstations, laptops, printers and related accessories)
  - Installation of infrastructure “hot swappable” hardware components (hard drives, memory, fans, etc.), not known to interrupt service

<u>Normal</u>

- A change that needs to be scheduled, assessed and authorized by the CAB following a standard process.
- Initiation is triggered by the creation of a manual or automated change request.
- Further categorized as *High*, *Medium* or *Low* significance, depending on the level of risk involved. Risk assessment considers the following factors:
  - Change complexity
  - Level of difficulty to back out the change
  - Business criticality
  - System resiliency
  - Change failure impact
  - Impact of not implementing the change
  - Branch impact
  - Back office impact
  - Information classification (sensitivity) impact
  - Regulatory compliance / Audit issue relationship
- Examples:
  - Installation of software not on the “pre-approved” list; reference the *Technology Reference Model (TRM) Standards for details*
  - Installation of infrastructure components (routers, switches, servers, circuits, etc.)
  - Connectivity (physical or logical) to 3rd party service providers over WAN, Internet, VPN, etc.
  - Project-related changes not included in the “Standard Changes” category
  - Firewall/IPS [or other security tool/control] changes
  - Implementation of any Policy/Standard/Procedure changes (i.e., control changes) as a result of documented changes after approval of the revised document by management committee/CTO as required
  - Anything else not included in the “Standard” or “Emergency Changes” categories; anything not previously addressed via Change Management, risk-assessed or on “approved” lists; or, any other change in which the Change Requestor wishes to be moved through the CAB

<u>Emergency</u>

- A change that must be implemented as soon as possible, e.g. to resolve an outage/incident or implement a security patch with potential impact to the production environment.
- The process for assessment and authorization is expedited to ensure quick implementation.
- Assessed and authorized by the ECAB; *see Section IX – Roles and*

Responsibilities.

- Requires CTO [or an appointed delegate] approval at a minimum.
- Examples:
  - Changes necessary to bring services into alignment with business or client-facing availability requirements (e.g., a downed infrastructure component [server, switch, router, etc.], or element thereof [excluding “hot swap” parts]) requiring immediate replacement to meet SLA or allowable downtime
  - Installation of patches or configuration modifications addressing “very high severity” or known exploitable security vulnerabilities in accordance with the Information Security Program Policy / Vulnerability Management Policy

Approve

Formal authorization/approval is required for all technology changes being made by the Bank and managed by IT. This provides clearance for scheduling and procurement. Conversely, failure to approve changes might result in challenges around accountability or resource allocation, particularly if the change goes poorly. Unapproved changes could result in unfavorable/unforeseen impact to the Bank. Where changes could significantly impact business operations, the highest level of approval is required. Changes impacting information/system security require CISO approval. Technology Changes should be approved by the CAB. Approval details must be recorded (i.e., documented) for both accountability and compliance requirements. Some changes may come to the CAB pre-approved by a higher-level authority such as the NPIC, TOPC or management-defined committees. A standard change does not require further CAB authorization beyond the initial model preauthorization, except when deviations occur. An emergency change will still require authorization, but this would be done by a separate authority, the ECAB, in order to expedite the approval process. If approved Changes cannot be completed within the scheduled implementation window, Changes must go back to CAB as a new request for approval. The CAB Charter will define the CAB membership and necessary approval levels.

Execute

The Execute phase includes just that: the implementation of the change. Execute and implement the change per the agreed schedule and steps recorded by all stakeholders. Communication is critical. Customers and employees need to know what to expect from the change, both in the short-term and over time. For changes with high business impact, communication must include stakeholders from Business Continuity/Disaster Recovery department to ensure resiliency plans are adequately updated. Execution can be done in a staging environment for testing and validation, whenever feasible, or it can be released during a sprint, depending on the pre-approved execution methodology. Back-out plan testing should be performed for high-risk changes to the extent feasible prior to moving such changes to production. Pre-planned end-user testing is vital to ensure functional and non-functional requirements, though the level of testing might vary depending on the type of change. Post-implementation testing should be performed by the stakeholders, as dictated by the risk level of the change, and should be documented in the Change Management Process (though exceptions can be made for Emergency Changes). Changes to application servers and network devices require an appropriate level of internal and/or external scans (i.e., security configuration, vulnerability and/or penetration testing, as appropriate), considering a risk-based approach, to be performed after the change, as soon as practicable. For example, security scans must be performed on any Internet-facing infrastructure components. Some Changes might require expedited execution, and once approved by the CAB, this must be reflected in the Change Schedule. Emergency change execution is always expedited. If a change goes wrong, the back-out plan must be activated. If a change fails and results in an outage, and incident should be entered into the system for tracking purposes. (Reference the *Technology Issue, Exception, & Incident Management* Procedures.)

Review

After a change is executed, a post-evaluation review should be conducted, as appropriate, to determine whether the change was successful. Particularly when a change fails, the post-evaluation offers sources for continual improvement. The review should confirm that the change met the original objectives that were recorded and approved; ensure stakeholders and end-users are satisfied with the outcome; verify no major or unexpected side effects resulted; and, consider root causes and corrective and preventative actions, in cases when a change failed. Where the CAB is involved, a post-implementation review should take place during a follow-up meeting as a part of the closure. A project status or closeout meeting can also be used to provide a platform for review of changes, but must include the relevant CAB stakeholders. Communication and documentation of the change review is vital for stakeholder engagement. Failure to perform this activity could lead to loss of improvement opportunities as well as lack of closure or feedback from key stakeholders on the change. The final closure of the change ticket should be performed by someone other than the Change Implementer, preferably a manager or their delegate.

c) Reporting

All emergency changes must be provided to the TOPC on a monthly basis. The report should be provided as an insert to the TOPC handout.

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 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.

Change Advisory Board (CAB): A group of people that advises the Change Manager in the assessment, prioritization and scheduling of Changes. This board is usually made up of representatives from all areas within the IT organization, Information Security, the business, and third parties such as suppliers. The CAB is responsible for authorizing Normal changes, and pre-approves Standard changes. Reference the CAB Charter for membership details.

Change Manager / Process Owner: *See Section II – Definitions.*

Change Requester: *See Section II – Definitions.*

Chief Information Security Officer (CISO) and Information Security Department: The CISO and the Information Security Department are accountable (A[2]) for providing 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 Program Policy*.

Chief Technology Officer (CTO): The CTO and designated representatives are responsible (R[1]) for creating and reviewing new and updated Technology policies and in charge of day-to-day oversight of execution.

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 [Annual, Biennial, Triennial] basis according to the Policy Level (*refer to the Review and Tracking Chart*).

[2] Standard RACI: Responsible (R), Accountable (A), Consulted (C), and Informed (I).

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.

Emergency Change Advisory Board (ECAB): A sub-set of the Change Advisory Board who makes decisions about high impact Emergency Changes. Membership of the ECAB may be decided at the time a meeting is called, and depends on the nature of the Emergency Change. Reference the CAB Charter for ECAB membership details.

Executive Management Steering Committee (EMSC): To the extent necessary, the EMSC 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.

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

- *Information Security Program Policy*
- *IT Asset Management Policy*
- *IT Operating Model Standards*
- *Record Retention Policy*
- *Technical Reference Model (TRM) Standards*
- *Technology Change Management Procedures*
- *Technology Issue, Exception & Incident Management Procedures*
- *Vulnerability Management Policy*

XIII. REVISION HISTORY

Version	Date	Description of Change	Author	Approver
1.0	08/2018	New Policy	J. Nagle & Y. Zimmermann	Board Operations & Technology
1.1	07/2019	Policy update to reflect enhanced CISO role.	K. Shurgan	Board Operations & Technology
2.0	09/2020	Enhanced policy to be more in-line with ITIL v3/4 change management/enablement standards.	A. Scarola	Board Operations & Technology
2.5	10/XX/2021	Enhanced alignment of policy with current IT capabilities; clarified vendor-related change management requirements; updated referenced policies and procedures.	A. Scarola	Technology Operations Planning Committee