**Apple Bank for Savings**

**Encryption Policy**

**February 24, 2021**

Page 1

Contents

[REVIEW AND TRACKING CHART 3](#_Toc20210)

[I. POLICY PURPOSE STATEMENT AND SCOPE 4](#_Toc20211)

[II. DEFINITIONS 4](#_Toc20212)

[III. KEY POLICY COMPONENTS 7](#_Toc20213)

[1. Executive Summary 7](#_Toc20214)

[2. Objectives 7](#_Toc20215)

[3. Key Components of Policy 7](#_Toc20216)

[a. Encryption Key Length 7](#_Toc20217)

[b. Encryption In-Transit 8](#_Toc20218)

[c. Encryption At-Rest 8](#_Toc20219)

[d. Key Management 9](#_Toc20220)

[4. Escalation Procedures 9](#_Toc20221)

[IV. REQUIRED PERIODIC REVIEW AND APPROVAL CYCLE 10](#_Toc20222)

[V. OFF-CYCLE REVIEW AND APPROVAL PROCESS 11](#_Toc20223)

[VI. DESIGNATED COMMITTEES AND POLICY LEVEL REVIEW 11](#_Toc20224)

[VII. EXCEPTIONS TO THE POLICY 11](#_Toc20225)

[VIII. RETIREMENT OF POLICIES 11](#_Toc20226)

[IX. ROLES AND RESPONSIBILITIES 11](#_Toc20227)

[X. RECORD RETENTION 13](#_Toc20228)

[XI. QUESTIONS AND CONTACT INFORMATION 13](#_Toc20229)

[XII. LIST OF REFERENCE DOCUMENTS 13](#_Toc20230)

[XIII. REVISION HISTORY 13](#_Toc20231)

[XIV. APPENDIX 1 14](#_Toc20232)

Page

***POLICY NAME: Encryption Policy***



# REVIEW AND TRACKING CHART

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

Page 3

# I. POLICY PURPOSE STATEMENT AND SCOPE

The Encryption Policy (the “Policy”) applies to the implementation, management and monitoring of encryption (including encryption key management) at Apple Bank for Savings and its subsidiaries (collectively, “ABS,” “Apple,” or the “Bank”) in accordance with applicable state and federal statutes, rules and regulations.

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

# II. DEFINITIONS

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

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

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

* **Auditable Information Technology (“IT”) Assets:** For the purpose of this Policy, a subset of IT Assets which includes, but is not limited to Applications, Computing Devices, IT Infrastructure, IT Network Infrastructure and any Cloud Offerings.

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

* **Bring Your Own Key (“BYOK”) Technology:**  A cloud computing security model that allows cloud service customers (the Bank) to use their own encryption software and manage their own encryption keys.

In this model, the business applications which are hosted in the cloud are configured so that all its data will first be processed by the Bank's Key Management Service, which then writes the ciphertext (encrypted) version of the data to the cloud service provider's data store. The ciphertext (encrypted) data is then retrieved from the cloud provider's data store and is readily decrypted by the Bank’s Key Management Service upon retrieval. In addition, the Bank can simply delete its keys to perform crypto-shredding, rendering any ciphertext (encrypted) data unreadable.

* **Certificate Authority (“CA”):** An entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. One particularly common use for certificate authorities is to sign certificates used in HTTPS, SSL, TLS, *etc.*

* **Cloud Offerings:** Any solution which leverages private or public cloud technology as identified by the vendor; examples of cloud offerings include software-as-a-service (“SaaS”), infrastructure-asa-service (“IaaS”) and platform-as-a-service (“PaaS”).

* **Computing Devices:** Consists of physical and virtual desktop and server operating systems (“OS”).

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

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

* **Encryption:** The conversion of data from a readable format into an encoded format that can only be read or processed after it has been decrypted.When properly implemented, encryption provides an enhanced level of assurance that the data, while encrypted, cannot be viewed or otherwise discovered by unauthorized parties in the event of theft, loss or interception.

* **Immaterial Change:** A change that does not alter the substance of the Policy in any way, but rather is a change only to grammar, formatting, template, typos, and the like.

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

* **IT Infrastructure:** Consists of Hypervisor OS, Storage Arrays, *etc.*

* **IT Network Infrastructure:** Consists of an OS of network-related IT Infrastructure such as routers, switches, firewalls, virtual infrastructure, VoIP technology, *etc.*

* **Legal Contact:** The attorney from the Legal Department assigned to the group responsible for this Policy. The attorney does initial and ongoing reviews of the Policy and serves in an advisory capacity.

* **Material Change:** A change that alters the substance of the Policy in any way or how it is applied, such as a change to a definition, phrase, vendor name, threshold, or anything beyond an Immaterial Change as defined above.

* **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.

* **Public Cloud:** Infrastructure is shared by multiple businesses and owned and operated by a cloud service provider. The cloud computing services are delivered to the Bank *via* the Internet.

* **Private Cloud:** Infrastructure is hosted either on-premises or at a cloud service provider offering greater levels of control and security. The cloud computing services are dedicated exclusively to the cloud user (the Bank).

* **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.

# III. KEY POLICY COMPONENTS

## 1. Executive Summary

The Encryption Policy (the “Policy”) applies to the implementation, management, monitoring and compliance with the use of encryption, as a control, to reduce the likelihood of data loss, theft or unauthorized access at Apple Bank for Savings and its subsidiaries (collectively, “ABS,” “Apple,” or the “Bank”) in accordance with applicable state and federal statutes, rules and regulations. The Policy will define and document encryption principals and requirements for data both in-transit and at-rest based upon the classification of the data.

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.

## 2. Objectives

The goal of the Encryption Policy is to define and document encryption principles and requirements for data both in-transit and at-rest based upon the classification of the data. The objective is to inform the Bank’s Data Custodians, Data Stewards and other relevant stakeholders of the Bank’s encryption requirements.

## 3. Key Components of Policy

The policy requires the identification and encryption of all data both in-transit and at-rest based upon the classification of the data (see *Data Classification Policy*).

The Bank must employ encryption strength sufficient to protect information from disclosure. Encryption methods must be reviewed periodically (at a minimum, one per calendar year) to ensure that the types and methods of encryption are still secure as technology and threats evolve.

Where applicable, encryption products for confidentiality of data at-rest and data in-transit must incorporate Federal Information Processing Standard (“FIPS”) approved algorithms for data encryption.

## a. Encryption Key Length

In order to provide the highest level of security, while balancing throughput and response times, encryption key lengths and algorithms should be aligned with current industry standards.

The encryption key length and algorithms must be equal or greater to what is required by the Bank’s *Encryption Standard*.

## b. Encryption In-Transit

Based upon data classification, data requiring encryption in-transit must be enforced by leveraging up-to-date, valid and non-expired certificates. For data which needs to be encrypted in-transit, between internal Bank systems, the Bank is required to utilize the Bank’s own certificate signing authority (a certificate signed by a root Certificate Authority [“CA”]). The Bank prohibits the use of third-party/vendor, self-signed certificates within the Bank’s Production environment.

The encryption key length and algorithms must be equal or greater to what is required by the Bank’s *Encryption Standard*.

Internal emails (*i.e.*, where both the origination and destination is an internal Bank employee with an @applebank.com email address) are encrypted by default.

Requirements relating to employee encryption of external emails containing Confidential or Restricted data (i.e., where the email originates from an an internal Bank employee with an @applebank.com email address but is delivered to an external party without an @applebank.com email address) are addressed in the User Agreement.

## c. Encryption At-Rest

Data encrypted at-rest must be of the type and have a strength equal or greater to what is required by the *Data Classification Policy*.

Pre-Boot Authentication (“PBA”) / Power-On Authentication (“POA”) is required for all Computing Devices (excluding Computing Devices that are hosted on an encrypted vSAN or do not contain a Trusted Platform Module [TPM] chip). Full disk-level encryption must be enabled on all Computing Devices, IT Infrastructure components and Automated Teller Machines (“ATMs”).

Photocopiers, fax machines, multi-function printers (“MFPs”) and similar devices may contain a hard drive, flash memory or other storage medium that stores digital images of documents which are copied, transmitted or printed by these devices. Encryption is required for photocopiers, fax machines, MFPs and their associated data storage mediums.

## d. Key Management

The Bank must have an active and up-to-date inventory of all encryption keys and the technologies and/or IT Assets related to those keys in order to ensure all encryption keys are rotated, at minimum, once per year. In order to achieve this, a Cryptographic Key Management Framework (“CKMF”). CKMF includes policies, procedures, standards and devices that are used to protect, manage, and distribute key information.

Encryption keys in the inventory must be rotated within a one (1) year period regardless of the classification of the data. Any encryption key which cannot be rotated (*e.g.*, a technical reason) requires an individual from Technology / IT to submit an Exception to Policy Request as per the *Exception to Policy Procedure*.

For Public Cloud Providers that will host, store, or process data classified as Confidential, the vendor must have the ability to support Bring Your Own Key (“BYOK”) technology. Any Business Owner that proceeds with a vendor which cannot provide this service/technology must submit an Exception to Policy Request as per the *Exception to Policy Procedure*.

Keys used for encrypting AFH information must be classified as Confidential as the keys will be used to encrypt/decrypt data which may similarly be classified as Confidential. Key Owners need to ensure keys will be generated, stored and managed in a secure and approved manner. Keys must be changed periodically based on industry standards and best practices. Keys must have at least two members of Senior Management assigned to a single key. All access, management, use and/or other key management-related activities must be logged.

Secure Socket Layer (“SSL”) certificates must be renewed at least once every two years (biennially).

For the purpose of this Policy, Pre-Shared Keys used for Virtual Private Network (“VPNs”) are not considered security/encryption certificates.

If it becomes known to the Bank that an encryption key has been compromised, the encryption key must be changed as per the *Encryption Procedure*.

## 4. Escalation Procedures

The Policy Owner will monitor this Policy. Any non-compliance with this Policy will be escalated to the Designated Management Committee for resolution. If the Designated Management Committee cannot resolve the issue, it will be escalated to the Executive Management Steering Committee (“EMSC”) for further consideration. If the issue cannot be resolved by the EMSC the issue will be escalated to the Board or Designated Board Committee for further consideration.

Senior management and the Board report, monitor and evaluate the Encryption Policy through the Technology and Operations Planning Committee (“TOPC”), Operations and Technology Committee (“OTC”), and Board meetings (or its designated Board Committee), when and as deemed appropriate. It is AFH’s policy to have appropriate escalation regarding Encryption. Please see escalation procedures in the *Encryption Procedures* for further information.

# IV. REQUIRED PERIODIC REVIEW AND APPROVAL CYCLE

1. **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.

1. **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. This includes, but is not limited to, staff entering the exception into the bank’s system of record (GRC) and a review by second-line-ofdefense to assess the potential risk and determine if it needs to be escalated to an appropriate governance committee for awareness or approval.

# VIII. RETIREMENT OF POLICIES

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

# IX. ROLES AND RESPONSIBILITIES

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

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

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

**Designated Management Committee:** The Designated Management Committee is responsible for reviewing and approving changes to the Policy as set forth herein on an annual basis (except in the year designated for Board approval) and submitting Material Changes to the Designated Board Committee, or Board, as appropriate.

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

**Information Security (“InfoSec”):** InfoSec is Responsible (“R”)[[1]](#footnote-1) for the oversight of encryption and key management activities. In addition, InfoSec will Consult (“C”)and Inform (“I”)Information Technology (“IT”) on encryption methodologies, strength and encryption key management activities, as appropriate.

**Encryption Key Owners (“Key Owners”):** Members of IT / Technology who are Responsible (“R”)and Accountable (“A”) for the creation and upkeep of an active and up-to-date inventory of all encryption keys and the technologies and/or IT Assets related to those keys in order to ensure all key management activities (*e.g.*, rotation, renewal) are completed, as required.

**Senior Management:** Members of management and business units are responsible for implementing this Policy, ensuring compliance and understanding of this Policy as well as developing procedures for his/her unit, to the extent needed, that align with the requirements of this Policy.

**Information Technology (“IT”):** IT is Responsible (“R”)and Accountable (“A”)to assign an individual within IT to be the Key Owner (coupled with the IT Asset associated with the aforementioned key) to perform all the various key management activities, to the extent needed, that align with the requirements of this Policy.

**Internal Audit (“IA”)**: The Internal Audit team is responsible for the periodic audit of this Policy. Internal Audit will review the processes and any related gaps will be identified as findings to be monitored and remediated.

**Legal Contact:** *See Section II – Definitions*.

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

**Policy Owner:** *See Section II – Definitions*.

**Risk Management**: Risk Management, in conjunction with Legal, determines the initial Designated Management Committee, Designated Board Committee (or Board, as appropriate), and Policy Level of the Policy and the Regular Board Review Cycle for this Policy, and re-evaluates the same at least annually.

# X. RECORD RETENTION

Any records created as a result of this Policy should be held for a period of 7 years pursuant to the Bank’s Record Retention Policy. Should records created as a result of this Policy require a different retention period (either a shorter or longer time period), the Policy Owner (in conjunction with the relevant business area leader) must describe the rationale for a different retention period and share the rationale with the Designated Management Committee.

# XI. QUESTIONS AND CONTACT INFORMATION

Questions regarding compliance with this Policy may be addressed to the Policy Owner listed in the tracking chart on the first page.

# XII. LIST OF REFERENCE DOCUMENTS

1. Data Governance Policy
2. AFH IT Asset Management Policy
3. Data Classification Policy
4. Encryption Standard
5. Exception to Policy Procedure
6. Encryption Procedure
7. IT/InfoSec RACI Matrix

# XIII. REVISION HISTORY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Description of Change** | **Author** | **Approver** |
| 1.0 | 10/23/2019 | Creation of Encryption Policy | Chief Technology Officer (“CTO”) | Board Risk Committee (“BRC”) |
| 2.0 | 2/24/2021 | Complete revision of Encryption Policy | Joseph Martano    AVP, Cyber Risk  Analyst | Management Risk  Committee (“MRC”);  Board Risk Committee  (“BRC”) |

# XIV. APPENDIX 1

Control Reference(s)

|  |  |
| --- | --- |
| Assets  Examples  (not a complete list)  Controls  Control Source | Computing Devices, IT Infrastructure, IT Network Infrastructure & Applications |
| * Assets (*e.g.*, servers, endpoints, virtual) * Data At-Rest and In-Transit * Encryption / Cryptographic Keys |
| * The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction*]. * The information system implements [*Assignment: organization-defined cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. |
| NIST SP 800-53 Rev. [SC-12,](https://nvd.nist.gov/800-53/Rev4/control/SC-12) [SC-13](https://nvd.nist.gov/800-53/Rev4/control/SC-13) |

1. All references herein to “Responsible”, “Accountable”, “Consult” and “Inform” tie back to the

   Information Technology (“IT”) / Information Security (“InfoSec”) RACI (Responsible, Accountable, Consult & Inform) Matrix [↑](#footnote-ref-1)