Apple Bank for Savings

Data Classification Policy

February 24, 2021

Table of Contents

I. POLICY PURPOSE STATEMENT AND SCOPE 4

II. DEFINITIONS 4

III. KEY POLICY COMPONENTS 6
1. Executive Summary 6
2. Objectives 6
3. Key Components of Policy 6
a. Confidential 7
b. Restricted 7
c. Internal 7
d. Public 7
4. Escalation Procedures 8

IV. REQUIRED PERIODIC REVIEW AND APPROVAL CYCLE 8

V. OFF-CYCLE REVIEW AND APPROVAL PROCESS 9

VI. DESIGNATED COMMITTEES AND POLICY LEVEL REVIEW 9

VII. EXCEPTIONS TO THE POLICY 9

VIII. RETIREMENT OF POLICIES 9

IX. ROLES AND RESPONSIBILITIES 9

X. RECORD RETENTION 10

XI. QUESTIONS AND CONTACT INFORMATION 10

XII. LIST OF REFERENCE DOCUMENTS 10

XIII. REVISION HISTORY 11

XIV. APPENDIX 1 12

REVIEW AND TRACKING CHART

Effective Date*:	February 24, 2021
Version Number:	1.1
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*:	February 11, 2021
Next Management Review Date*:	February 2022
Policy Owner:	Chief Information Security Officer ("CISO")

I. POLICY PURPOSE STATEMENT AND SCOPE

The Data Classification Policy (the "Policy") applies to the implementation, management, monitoring, and compliance with classifying data assets 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 (*i.e.,* software), managed by both vendors (*i.e.,* hosted solutions) and by Technology (*i.e.,* on-premises solutions).
- **Biennial or Biennially:** Every twenty-four (24) months.
- **Cloud Offerings:** Any solution which leverages private or public cloud technology as identified by the vendor; for example, software-as-a-service ("SaaS"), infrastructure-as-a-service ("IaaS") and platform-as-a-service ("PaaS"), *etc*.
- **Computing Devices:** 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. The Control Form is available on AppleNet.
- **Corporate Systems:** For the purpose of this Policy, Corporate Systems are a subset of IT Assets which require Bank and Non-Bank Employees (*e.g.*, consultants) to be connected to the Bank's network in order to access Bank Applications, Computing Devices, Cloud Offerings, IT Infrastructure and IT Network Infrastructure.
- **Data Steward (First Line):** Data Stewards are appointed by functional area senior leadership and act as the hands-on resource within the business to create/manage critical data elements, report data quality issues, and to conduct other data governance responsibilities around control and use of data (definition subject to updates in the *Data Governance Policy*).
- **Data User:** The Data User directly accesses Bank data and/or uses business intelligence views (definition subject to updates in the Data Governance Policy).
- **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 Asset:** A definable piece of information stored in any manner which is recognized as 'valuable' to the organization.
- **IT Assets:** Please reference the *AFH IT Asset Management Policy*.

- **IT Infrastructure:** IT Infrastructure includes components such as Hypervisor OS, Storage Arrays, *etc.*

- **IT Network Infrastructure:** IT Network Infrastructure consists of network-related IT Infrastructure which includes components 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.

- **Multi-Factor Authentication ("MFA"):** Authentication through verification of at least two of the following types of authentication factors:

    - Knowledge factors, such as a password; or
    - Possession factors, such as a token or text message on a mobile phone; or
    - Inherence factors, such as a biometric characteristic.

- **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.

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

III. KEY POLICY COMPONENTS

1. Executive Summary

Information assets are vital assets to the company just like physical property. In order to determine the value of such assets and how they should be handled, data elements must be categorized and classified according to their importance to company operations and the need for confidentiality.

Once the data classification levels are determined, the company can identify and take all commercially reasonable steps necessary to confirm that its data assets are protected appropriately. The protection of all company data assets, such as computer facilities, equipment, systems, applications and software, information about accounts, loans, business relationships, customers, clients, counterparties, service providers and vendors, as well as documentation and all other data and information necessary for the conduct of company business (collectively, "Information Assets"), is a basic responsibility of management.

This document outlines AFH's Policy with respect to the implementation, management, monitoring, and compliance with Data Classification.

2. Objectives

This policy applies to all Information Assets (see *definition*, Section I, above), including but not limited to data related to employees, whether handled by employees, contractors, vendors, suppliers, third party service providers, or their staff or agents, irrespective of the medium on which the information resides and regardless of format (*i.e.*, electronic, paper or other physical form).

This policy sets forth the minimum acceptable requirements for the use and protection of all Information Assets and does not preclude application of more stringent requirements when justified by unique business needs, assessed risks and/or legal and regulatory obligations.

3. Key Components of Policy

All AFH personnel have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored or used by AFH, irrespective of the medium on which the data resides and regardless of format (such as in electronic, paper or other physical forms).

Information assets owned, used, created or maintained by the Bank, must be classified into one of four categories:

a) Confidential

b) Restricted

c) Internal

d) Public

a. Confidential

Confidential Information is the highest level of data classification. Unauthorized disclosure, compromise, or destruction of this information could provide a significant advantage to a competitor, or result in severe damage and penalties to the Bank, its clients, customers, business relations, counterparties or employees. It is intended solely for use within the Bank. Access is limited to those with an explicit, predetermined and stringent "*business need-to-know*", and is further limited to the lowest level of access necessary to fulfill the business requirements.

b. Restricted

Restricted Information is the second highest data classification, and is information that is designated by the Data Steward (or otherwise) as Restricted. Unauthorized disclosure, compromise, or destruction of this information could - directly or indirectly - result in significant adverse impact on the Bank, its clients, customers, business relations, counterparties, vendors, third-party service providers or employees. Adverse impacts may include financial loss, damage to reputation, loss of business, jeopardy to the security of organizational assets, and potential legal action. Restricted information is intended primarily for use within the organization and access is limited to those with "*business need-to-know*" and non-Bank personnel covered by a non-disclosure agreement.

c. Internal

Internal Information is primarily internal or proprietary information not meant for public knowledge or disclosure. Unauthorized disclosure, compromise, or destruction may result in some adverse impact to the organization, its customers, or employees. Due to its technical or business sensitivity, access is limited to employees and non-Bank personnel subject to a non-disclosure agreement.

d. Public

Public Information is information that can be disclosed to anyone or has been previously released into the public domain. Unauthorized disclosure, compromise, or destruction would neither violate an individual's expectation of privacy, expose the organization to financial loss or embarrassment, nor jeopardize the security of company assets. Although Public Information generally may be disclosed, disclosure of Public Information must not violate any pre-existing, signed non-disclosure agreements (*see* Confidential, above).

See *Appendix 1* for additional details and examples.

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.

To comply with this policy, for any Applications, Computing Devices, IT Infrastructure and IT Network Infrastructure which is unable to meet the requirements set forth within this policy (*e.g.*, due to a technical limitation), the Business Owner or IT must submit a *Self-Identified Issue* within the GRC tool wherein it will be tracked for the entirety of its life cycle.

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.

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.

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 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. IT Asset Management Policy
3. Exception Policy
4. Encryption Policy
5. Encryption Standards

XIII. REVISION HISTORY

Version	Date	Description of Change	Author	Approver
1.0	04/29/2020	Creation of Data Classification Policy	Joseph Martano AVP, Cyber Risk Analyst	Board Risk Committee (“BRC”)
1.1	02/24/2021	Minor changes were made to the Policy content and the Data Classification Policy was placed into the newest template	Joseph Martano AVP, Cyber Risk Analyst	Management Risk Committee (“MRC”); Board Risk Committee (“BRC”)

XIV. APPENDIX 1

Confidential Data

Sensitivity	**Very High**
Asset Value	High – Critical to Business
Examples (not complete list)	▪ Business-related information of the Bank where tampering with which, or unauthorized disclosure of, access to or use of which, would cause a material adverse impact to the business, operations or security (confidentiality, integrity and availability) of the Bank ▪ Confidential or proprietary bank information such as financial statements, performance and reporting data ▪ Confidential or proprietary information of any Bank counterparty, third-party service provider or other business relationship ▪ Board & Committee information ▪ Employee health information ▪ Audit reports ▪ Strategic plans ▪ Encryption keys ▪ Security logs ▪ Non-public information relating to mergers and acquisitions ▪ Non-public financial information of the Bank ▪ Attorney-client privileged materials, and information under non-disclosure orders from a regulatory or court authority ▪ Any information concerning an individual (customer, employee or otherwise) which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: – Social Security number; – Drivers' license number or non-driver identification card number; – Account number, credit or debit card number; – Any security code, access code or password that would permit access to an individual's financial account; – Biometric records. ▪ Information used to authenticate an individual's identity, such as passwords, PINS, and records and/or databases containing authenticating information ▪ Other non-sensitive, non-public individual (customer, employee or otherwise) Personal Information ▪ Protected health information

Controls	▪ Unauthorized transmission through any electronic messaging system (e-mail, instant messaging, text messaging) is prohibited. ▪ Authorized transmission must use encryption for data in transit and maintained at rest. ▪ Encryption must, at minimum, meet the standards specified in the Bank's Encryption Standards. ▪ Externally hosted applications that contain Confidential information must use MFA or have IP restrictions. ▪ Protections against data leaks are implemented. ▪ Privileged User Access as defined in the IAM&A Policy must use MFA to access Confidential Information. ▪ Destruction of data based on data retention policy.
Control Source	▪ NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28 ▪ NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12
	▪ NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4

Restricted Data

Sensitivity	**Moderate to High**
Asset Value	Medium to High
Examples (not complete list)	▪ System Configurations ▪ Personnel records ▪ Budget information ▪ Security Plans & Standards ▪ Network Diagrams and other technical information which can be used to identify Bank assets ▪ Marketing and sales plans or analyses ▪ Business email addresses ▪ Purchasing orders for IT hardware (supply chain risk) ▪ Joint-venture or partnership agreements ▪ Joint marketing Agreements ▪ Bank policies, procedures, processes ▪ Product/servicing pricing information ▪ Employee compensation data, and similar documents or information that are competitively sensitive ▪ Compliance findings ▪ Vendor and supplier lists and agreements ▪ Bank planning/strategy reports, or investment and business forecasts ▪ Regulatory filings

Controls	▪ Authorized transmission must use encryption for data in transit. ▪ Encryption must, at minimum, meet the standards specified in the Bank's Encryption Standards. ▪ Protections against data leaks are implemented.
Control Source	▪ NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28 ▪ NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12 ▪ NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4

Internal Data

Sensitivity	**Low to Moderate**
Asset Value	Low to Medium
Examples (not complete list)	▪ Telephone Directory ▪ Organization Charts ▪ Routine administrative & office information ▪ Employee status and work history ▪ Bank advertising
Control	▪ Protections against data leaks are implemented.
Control Source	▪ NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4

Public Data

Sensitivity	**Low**
Asset Value	Low
Examples (not complete list)	▪ Information which is lawfully made available to the general public from federal, state, or local government records; it does not include data that is available on the internet other than that captured in formal government records ▪ Marketing brochures ▪ Published annual reports ▪ Interviews with news media ▪ Business cards ▪ Public press releases ▪ Public portions of the organization's web sites ▪ Publicly posted job announcements
	▪ None
	▪ None