Apple Financial Holdings, Inc.

Encryption Procedures

June 1, 2021

Contents

PROCEDURES NAME: Encryption Procedure

REVIEW AND TRACKING CHART

Effective Date*:	*June 1, 2021*
Version Number:	2.5
Review Frequency:	Annual (Every 12 Months)
Last Business Area Leader/Department Head Review Date*:	*June 2021*
Next Business Area Leader/Department Head Review Date*:	*June 2022*
Business Area Leader/Department Head:	Debi Gupta, CTO
Overarching Policy or Policies:	AFH Encryption Policy
Procedures Owner:	Michael Lamparello, Stephen Apruzzese

I. PROCEDURES PURPOSE STATEMENT AND SCOPE

The Encryption Procedure (the "Procedures") apply to the implementation, management, monitoring, compliance with remote access management of technology infrastructure at Apple Financial Holdings, Inc. ("AFH"), inclusive of Apple Bank for Savings and its subsidiaries (collectively, "ABS," "Apple," or the "Bank") in accordance with applicable state and federal statutes, rules and regulations and Bank policy.

All AFH employees and third party resources engaged by the Bank must comply with the terms of these Procedures to the degree applicable to them.

II. DEFINITIONS

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

- **Business Area Leader or Department Head:** The management level person who is responsible for (1) the business unit that has developed a set of Procedures and (2) the Annual review and approval of Procedures.

- **Control Form:** The form to be submitted to the PPA (defined in this Section) in connection with revised Procedures. The Control Form is available on AppleNet.

- **Legal Contact:** The attorney from the Legal Department assigned to the group responsible for these Procedures. To the extent needed, the Procedures Owner may consult with the Legal Contact in drafting and updating the Procedures.

- **Policies and Procedures Administrator ("PPA"):** The PPA is a member of Risk Management. The PPA monitors the occurrence and timeliness of scheduled Procedure reviews, obtains updated versions of Procedures, and ensures that they are uploaded to AppleNet within seven days of the approval dates of the documents. The PPA will also provide guidance on the PPGP (defined in this Section) to Bank Personnel.

- **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.

- **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.

- **Procedures Owner:** The person responsible for managing and tracking a set of Procedures. This includes initiating the required Annual review of the relevant Procedures and recommending updates to the Procedures, to the extent needed. Procedures Owners are responsible for providing the approved documents to the PPA (defined in this Section) for upload to AppleNet. The Procedures Owner will monitor these Procedures. Any non-compliance with the

Procedures will be escalated to the Business Area Leader or Department Head for resolution.

III. KEY PROCEDURES COMPONENTS

1. Executive Summary

This document outlines AFH's Procedures with respect to the implementation, management and compliance with encryption in accordance with the *AFH Encryption Policy.*

2. Objectives

The objective of these Procedures is to establish a standardized and consistent approach to implementation, management and compliance of encryption inclusive of network and systems.

3. Key Components of Procedures

A. Network Infrastructure (Route-Switch Environment)

Cryptographic Key Management Procedure

Overview

This section outlines Key Management for the Database and Server Storage encryption systems that are used in the environment including key generation, access, changes, audit and logging.

Key Generation

- Encryption keys are generated during initial encryption of the data.

- Keys are automatically generated directly by the Encryption Software or a Key Management Service.

Key Management:

- See appendixes for details on key management.

B. Server Infrastructure

- The Server Infrastructure Group manages encryption Keys and Key Management Systems.

- Access to Keys and Key Management Systems are managed by Active Directory Group Membership to the Server Infrastructure Group. Additional members to this group require a helpdesk ticket and approval by management for tracking.

- Encryption Keys are cycled (rotated) during system upgrades/migrations. Forms of encryption such as databases require approval from upper management due to downtime required for key cycling.

• Maintenance windows are scheduled with the Business Units to perform new key generation and re-encryption of data.

Server Storage Encryption

• Virtual machine encryption keys are managed in VMWare vCenter utilizing CloudLink KMSCloudLink KMS.

• vSAN Storage is encrypted for all Virtual Machines in the Scarsdale Production VxRail Cluster and is applied via the vSAN Default Storage Policy.

• A CloudLink KMSCloudLink KMS cluster is in place to manage keys for vSan encryption. Access to CloudLink KMS is limited to the Server Infrastructure team.

• Virtual machines that are hosted outside of the cluster (non-production machines in single VMWare hosts) have the VM Encryption Policy applied to all Virtual Hard Disk files.

SQL Server Encryption

• SQL Databases with Non-Public Information, in both Production and Test environments, are encrypted utilizing Netlib Encryptionizer for SQL.

• Keys are managed via the Encryptionizer for SQL Server Application installed on each SQL server.

Netlib Encryptionizer:

The Netlib Encryptionizer software licensed per machine and is tied to the hardware i.e. CPU, RAM and MAC. Changes to the SQL server's hardware will invalidate the license and lock all encrypted data. To install an instance of Encryptionizer on another Server will require Netlib to invalidate the current license and enroll a new Server. This can only be completed by named contacts in the Netlib Support website. Refer to SQL Database Encryption with Netlib Encryptionizer section in B. Appendix.

Encryption Key Management:

SQL Encryption Keys are generated when a database is initially encrypted. Generating new keys require the databases to be decrypted then re-encrypted while offline. This requires a large maintenance window on critical Production systems. Once the encryption key is generated after initial encryption, it is not cycled.

Veeam Backup Appliance:

Encryption keys are generated within our Veeam application. This is applied to any backups that are performed and exported through the application. Key Management is controlled within the application, where a retention period of one month is held. Keys are rotated automatically through the Veeam management console based on this retention period. Retrieval and storage of keys are kept secure from within the console.

Distributing keys to intended users:

- Encryption data-at-rest keys handled by the server team are not intended for end users

Storing and obtaining access to keys by authorized users:

• SQL Encryption: SQL administrators within the Server Infrastructure team store the keys in a password protected limited permission file.

• VMWare VSAN Encryption: VMWare administrators, identified via AD group, have access to the KMS settings in vCenter.

Changing and updating keys:

• All data-at-rest keys are generated during encryption and are updated when new media is added i.e. database or disk

Addressing compromised keys:

• All data-at-rest keys possibly compromised are cycled.

Archiving, revoking and specifying how keys should be withdrawn or deactivated:

• Data-at-rest keys are active until they are cycled. Inactive keys are not archived.

Recovering keys that are lost or corrupt:

• SQL Encryption: Key files are recovered from file system backups

• VMWare VSAN Encryption: Keys are managed by a clustered KMS. The KMS has four nodes spread across four host servers in two datacenters for high availability.

Logging of key management:

• SQL Encryption: SQL Database activity is logged using Netwrix Auditor.

• VMWare VSAN Encryption: vCenter access uses AD account monitored by Netwrix.

Defining activation and deactivation dates:

• SQL Encryption: Keys are activated when databases are created. Key deactivation only occurs when databases are restored from backup or are deleted.

• VMWare VSAN Encryption: vCenter access uses AD account monitored by Netwrix

C. Systems (Server, Desktop)

Encryption of Servers and Desktop/Laptops are performed with BitLocker Key Encryption. Scripting through Kace is performed by the Service Desk on user devices (Workstations and Laptops). Servers are encrypted when identified to contain PII data by the Information Security team.

4. Escalation Procedures

The Procedures Owner will monitor these Procedures. Any non-compliance with the Procedures will be escalated to the Business Area Leader or Department Head for resolution.

IV. REQUIRED ANNUAL (12 MONTH) REVIEW

Procedures are required to be reviewed and approved at least Annually by the Business Area Leader or Department Head. The Procedures Owner is responsible for initiating an Annual review of the Procedures. The Procedures Owner will track the review date for the Procedures and begin the review process early enough to provide ample time for the appropriate review to occur in a timely manner.

Once updated Procedures have been approved by the Business Area Leader or Department Head, the updated Procedures shall go into effect and the Procedures Owner shall be responsible for delivering the approved Procedures together with a Control Form 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 Procedures are stored and made available to the employees of the Bank.

The Next Business Area Leader/Department Head Review Date shall be adjusted accordingly.

V. OFF-CYCLE REVIEW AND APPROVAL PROCESS

If the Procedures require changes to be made outside the Required Annual (12 Month) Review outlined in the previous section, the same steps as outlined in the previous section shall apply.

VI. EXCEPTIONS TO THE PROCEDURES

Requests for exceptions to these Procedures must be specific and may only be granted on specific items, rather than to entire sections. AFH staff must communicate their exception requests in writing to the Procedures Owner, who will then present the request to the Business Area Leader or Department Head for consideration.

VII. ROLES AND RESPONSIBILITIES

The key roles and responsibilities for these Procedures are summarized below:

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

Business Area Leader or Department Head: *See Section II – Definitions*.

Internal Audit: The Internal Audit team is responsible for the periodic audit of these Procedures. 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*.

PPA: *See Section II – Definitions*.

Procedures Owner: *See Section II – Definitions*.

Senior Management: Members of management and business units are responsible for developing and implementing these Procedures which align with the requirements of the overarching Policy or Policies to which these Procedures relate, and ensuring compliance and understanding of these Procedures.

VIII. RECORD RETENTION

Any records created as a result of these Procedures should be held pursuant to the Bank's Record Retention Policy. Should records created as a result of these Procedures require a different retention period (either a shorter or longer time period), the Procedures Owner must describe the rationale for a different retention period and share the rationale with the Business Area Leader or Department Head, who shall in turn document the deviation and supporting rationale in such a way that it can be presented to relevant parties upon request.

IX. QUESTIONS AND CONTACT INFORMATION

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

X. LIST OF REFERENCE DOCUMENTS

- *AFH Encryption Policy*

XI. REVISION HISTORY

Version	Date	A	Author	Approver
2.6	June 1, 2021	Updated to include Veam encryption key management.	S. Apruzzese	Debi Gupta, CTO
2.5	April 23, 2021	Updated to align with the new *AFH Encryption Policy* (InfoSec).	M. Lamparello; S. Apruzzese	Debi Gupta, CTO
2.0	March, 2020	Updated to align with updated *AFH Encryption Policy.*	J. Mendez and team	Debi Gupta, CTO

1.0	November, 2018	Align with new procedure.	K. Shurgan	Board Operations & Technology Committee