

Data Retention and Disposal Policy

Lifecycle Governance, Deletion Schedules, and Cryptographic Shredding Standards for Koney (koney.money)

DOCUMENT ID KML-DAT-POL-2026	EFFECTIVE DATE September 22, 2026	REVIEW CYCLE Annual / Continuous	SECURITY LEVEL Public • Compliance
ENTITY NAME Kingmohan45 Labs (MSME Reg.)	TARGET APPLICATION Koney (koney.money)	SCOPE Plaid Financial Data & User Store	ISSUING AUTHORITY Office of Information Security

1.0 Purpose and Strategic Objectives

1.1 Kingmohan45 Labs ("the Organization") is dedicated to protecting consumer data through disciplined lifecycle management. This Data Retention and Disposal Policy ("Policy") defines operational requirements, mandatory retention schedules, automated disposal mechanisms, and cryptographic shredding criteria applicable to all information collected, processed, and stored by Koney (koney.money).

1.2 The primary objective of this Policy is to enforce strict data minimization: retaining consumer financial data only as long as necessary to provide personal finance management (PFM) services, honoring statutory compliance requirements, and ensuring guaranteed, permanent disposal upon account unlinking, profile closure, or user deletion requests.

2.0 Scope of Applicability

2.1 This Policy governs all primary data stores, secondary backups, serverless worker caches, log streams, object stores, and database replicas across the Organization's production environment (including AWS infrastructure, Cloudflare edge networks, and local application persistent volumes).

2.2 The controls specified herein directly apply to all data retrieved from financial integration partners (including Plaid Inc.), consumer credentials, transaction records, account balances, and security audit logs.

3.0 Data Classification and Retention Schedules

Data collected by Koney is classified based on sensitivity and retained strictly according to the defined lifecycle schedules:

Classification	Data Types	Active Retention	Post-Termination / Deletion Action
Financial Tokens (Restricted)	Plaid Access Tokens, Item IDs, Institution Identifiers	Duration of active bank connection	Immediate revocation with Plaid API + cryptographic shredding within 24 hours.
Transaction & Balance Records (Confidential)	Bank account balances, transaction details, categories, merchant names	Duration of active user account	Cascade purged from primary database immediately; automated backup purge within 30 days.
User Profile & Identity (Confidential)	Email address, display name, user preferences, password hashes	Duration of active user account	Hard-deleted upon user request or account cancellation; completed within 30 days.
Security & Audit Logs (Internal)	Authentication timestamps, IP logs, API access history, admin access records	90 calendar days rolling	Automated lifecycle expiration and secure overwriting; never tied to financial records post-purge.

4.0 Consumer Data Rights and Automated Deletion Workflows

4.1 Affirmative Right to Deletion: In compliance with global privacy standards, consumers maintain the right to delete individual financial institutions or their entire Koney account at any time directly through the application settings or by contacting privacy@koney.money.

4.2 Single Bank Unlinking Protocol:

- When a user unlinks an institution, an automated API call (`/item/remove`) is immediately dispatched to Plaid to revoke upstream token authorization.
- All associated encrypted access tokens, transaction history records, and balance entries stored within Koney's database are deleted via synchronous transactional cascades.

4.3 Full Account Termination Protocol:

- Upon user account deletion, all active institution tokens are revoked with Plaid.
- All user entity records, budget configurations, linked accounts, and transactions are hard-deleted from production databases immediately.
- Disaster recovery backups and WAL archives age out and are permanently overwritten on an automated 30-day lifecycle schedule.

5.0 Data Sanitization and Cryptographic Disposal Standards

5.1 Cryptographic Shredding: All sensitive financial records and Plaid authentication secrets stored at rest are encrypted using AES-256 with unique key hierarchies. Upon disposal, the encryption key material governing the user's specific records is destroyed, rendering any residual block storage cryptographically unrecoverable.

5.2 Cloud Infrastructure Disposal: In accordance with NIST SP 800-88 Revision 1 (Guidelines for Media Sanitization) and cloud provider standards (AWS), decommissioned storage volumes (EBS), database snapshots, and persistent caches undergo secure logical overwriting prior to reallocation.

5.3 Zero Data Monetization or Broker Retention: Koney strictly forbids retaining, aggregating, anonymizing for sale, or brokering consumer transaction records to third parties or advertising networks. Once disposed of, zero derivative data remains.

6.0 Compliance Enforcement and Periodic Review

6.1 Annual Policy Review: This Policy is formally reviewed at least annually by the Information Security Officer to ensure alignment with changing privacy regulations and third-party partner requirements.

6.2 Disposal Verification Audits: Periodic automated tests and synthetic deletion scripts are executed against staging and production replicas to verify that cascade deletion triggers operate reliably without orphan records.

7.0 Executive Attestation and Ratification

This Data Retention and Disposal Policy has been officially reviewed, approved, and enacted by the executive leadership of Kingmohan45 Labs. All terms herein are binding and in full operational effect.

APPROVED ON BEHALF OF KINGMOHAN45 LABS:

Mohan Kumar Ragamsetty

Founder & Information Security Officer
Kingmohan45 Labs

GOVERNANCE & AUTHORITY:

Entity: Kingmohan45 Labs (MSME Reg.)

Platform: Koney (koney.money)

Date: September 22, 2026

Status: Active • Operational Compliance