Data Retention and Disposal Policy

Owner and Contact

- Policy Owner: Brad (Founder), brad@axite.ai
- Security Contact (monitored): security@axite.ai

Purpose and Scope

Defines how AskMyMoney retains and disposes of data, including Plaid-derived financial data, PII, logs, and backups. Applies to all environments (dev, staging, prod), workforce members, contractors, and vendors that process our data.

Data Classification

- Restricted: Plaid access tokens, financial account data, transaction data, user identifiers (email, name), secrets/keys.
- Confidential: Internal operational data, support tickets, analytics without direct identifiers.
- Internal: Non-public business data.
- Public: Content explicitly published for public use.

Retention Rules

- Plaid access tokens: Stored encrypted (AES-256-GCM) and retained only while the user maintains a linked item. Deleted immediately on user-initiated deletion or item revocation.
- Plaid account/transaction data: Retained while the user account is active and necessary to deliver product features; purge within 30 days of account deletion or upon verified erasure request.
- Audit logs (auth, admin actions, data access): Retain 12 months unless legal/contractual needs require longer; ensure log integrity and restricted access.
- Webhooks and operational logs: Retain 90 days unless rolled into audit logs; redact secrets and PII where possible.
- Backups: Encrypted at rest; retain 30 days rolling by default. Apply the same deletion requests to backups by ensuring restore-and-purge or backup expiry within the window.
- Vendor data: Follow vendor contracts; enforce minimum necessary data sharing and request deletion on termination.

User Rights and Consent

- Capture explicit user consent for data collection, processing, and storage; record timestamp and policy/version.
- Honor data subject requests (access, deletion, correction) within applicable legal timelines. Verify identity prior to action.

Disposal Procedures

- Application-layer deletion: Remove Plaid access tokens, mark items deleted, and purge related Restricted data from primary stores; record deletion in `plaid_item_deletions` for audit.
- Backups: Allow encrypted backups to expire based on retention; if early purge is required, restore-then-delete the relevant records or destroy backup sets where supported.
- Media sanitization: Rely on cloud provider sanitization for managed storage; for any local media, use NIST-compliant wipe or physical destruction.

Controls and Enforcement

- Separation of environments; no production Restricted data in dev/test.
- Access to retention/deletion functions restricted to authorized roles; changes are logged.
- Review retention rules annually and when new data types or regulations apply.
- Monitor for end-of-life storage or services and migrate before support ends.

Review and Exceptions

- Policy reviewed at least annually by the security owner.
- Exceptions must document scope, compensating controls, and an expiration date.