



Data Retention and Disposal Policy

Version 1.0 · Adopted October 13, 2026 · Owner: Luis Orlando Rodriguez Cabrera, Founder and Information Security Officer

Version	1.0
Adopted	October 13, 2026
Owner	Luis Orlando Rodriguez Cabrera, Founder and Information Security Officer
Parent policy	Information Security Policy v1.0 (section 9)
Related	Privacy Policy (xtra-dev.com/privacy), Access Control Policy v1.0
Security contact	security@xtra-dev.com (monitored group address)
Review cycle	At least annually, after any security incident, and whenever a new data category or system is introduced

1. Purpose and scope

This policy sets how long Wyxloop Corp ("Wyxloop") keeps each category of data handled by the Xtra-dev platform (xtra-dev.com), including the consumer financial data its internal finance module MyXCapital receives from data aggregators (Plaid, SimpleFIN), and how that data is disposed of when the retention period ends or when its deletion is requested. It applies to production databases, backups, logs, files in object storage, third-party services acting on Wyxloop's behalf, and the devices used to administer them. Wyxloop keeps no paper records.

2. Principles

- **Keep only what is needed:** data is retained for the shortest period required by its purpose, the law, or an active user relationship.
- **One schedule, enforced by software:** retention periods are implemented in automated jobs and platform settings, not left to memory.
- **Disposal is complete:** deletion removes the live record, and backups that still contain it expire on their fixed rotation.
- **Requests are honored:** data subjects and aggregators can request deletion; requests are completed within 30 days.
- **Legal holds win:** data under a legal hold or a tax or accounting obligation is kept for as long as that obligation lasts, then disposed of.

3. Retention schedule

Data category	Where it lives	Retained for	Disposal
Consumer financial data from aggregators (accounts, balances, transactions)	Production database (MyXCapital)	While the bank connection is active and the account owner keeps the account in the tool	Disconnecting removes the connection at the aggregator (Plaid <code>/item/remove</code> ; SimpleFIN access revoked) and stops synchronization; the owner deletes accounts and transactions at any time (hard delete); deletion requests completed within 30 days
Aggregator credentials (Plaid access tokens, SimpleFIN access URLs)	Production database, encrypted (AES-256-GCM)	While the connection is active	Cleared on disconnect, removal or revocation; never written to logs or exports
Daily net-worth snapshots (aggregated totals, no transaction detail)	Production database	While MyXCapital is in use	Deleted with the module data on request
Workspace and administrator accounts (profile, password hash, MFA settings, sessions)	Production database	While the account is active; 90 days after deactivation	Hard delete after 90 days unless the law requires longer
Security and audit event log (logins, MFA, administrative actions, sync events)	Production database	180 days (state-bearing records, e.g. billing and backup events, are kept with the record they belong to)	Automated nightly retention job
Security alerts (acknowledged or resolved)	Production database	90 days	Automated nightly retention job
Contact-form submissions and lead data	Production database	Up to 24 months after the last interaction	Deleted by the retention job or on request
Customer mailbox mirror (deleted messages)	Production database	30 days after deletion in the mailbox	Automated nightly retention job

Data category	Where it lives	Retained for	Disposal
Product-catalogue scraping events	Production database	30 days	Automated nightly retention job
Billing, invoices, receipts and tax records	Production database, Stripe	As required by tax law (typically 5 to 7 years)	Disposed of when the statutory period ends
Application and access logs (no financial data, no secrets)	Hosting platform	Rotated by the platform; at most 12 months	Automatic rotation
Database backups (full, encrypted)	Hosting platform (3 most recent on the host) and private object storage (up to 45 copies, at most 30 days)	30 days	Automatic rotation; a record deleted from the database leaves every backup within 30 days
Backup job records produced by the platform's own backup worker	Production database	90 days	Automated retention job
Ephemeral files (uploads in transit, import previews)	Application memory and temporary storage	Duration of the request	Discarded when the request completes

4. Deletion and consumer requests

- The account owner can disconnect a bank, delete an account, delete individual transactions or undo an entire import from MyXCapital; these are immediate hard deletes in the production database.
- Requests from a data subject, a financial institution or an aggregator (for example a Plaid data-deletion request) are sent to security@xtra-dev.com, verified, executed and confirmed in writing within 30 days.
- When a connection is removed, the aggregator is informed (Plaid `/item/remove`), so the aggregator stops retrieving data on Wyxloop's behalf.
- Deleted data persists in encrypted backups only until they rotate (30 days at most) and is never restored except to recover from a failure, in which case the deletion is re-applied.

5. Disposal methods

Medium	Method
Database records	SQL hard delete (no soft-delete for financial data); transactions and backups rotate within 30 days
Encrypted secrets	The encrypted value is overwritten or cleared; the encryption key is rotated on suspicion of exposure, which renders older ciphertext unreadable
Object storage (backups, media)	Object deletion through the provider's API; buckets are private and server-side encrypted
Virtual servers and volumes	Volumes are destroyed through the hosting provider when a server is decommissioned; data is never moved to new hardware without encryption
Administrator workstations	Full-disk encryption at all times; on retirement, the disk is cryptographically erased (key destroyed) or securely wiped before reuse or disposal
Third-party services (Stripe, Microsoft 365, Plaid, SimpleFIN)	Data is deleted from the Wyxloop side and the provider's own deletion mechanism is used where available; provider retention is governed by their published terms

6. Roles and enforcement

- The Information Security Officer owns this schedule, runs the quarterly review of retention jobs and backup rotation, and handles deletion requests.
- Retention periods are enforced by a nightly automated job for logs, alerts, leads and mirrors, by hosting-platform settings for backups and logs, and by user-driven actions for financial data. Job runs and failures are logged and alerted.
- A legal hold is recorded in writing by the ISO with its scope and reason; affected data is excluded from disposal until the hold is lifted.

7. Review

This policy, the schedule above and the configured retention settings are reviewed at least annually and after any incident, and the review is noted in the operations log. Questions and requests: security@xtra-dev.com.

Related documents

- [Information Security Policy \(v1.0\)](#)
- [Access Control Policy \(v1.0\)](#)
- [Privacy Policy](#)