



Information Security Policy

Version 1.1 · Adopted October 13, 2026 · Owner: Luis Orlando Rodriguez Cabrera, Founder and Information Security Officer

Version	1.1
Adopted	October 13, 2026
Revised	October 16, 2026
Owner	Luis Orlando Rodriguez Cabrera, Founder and Information Security Officer
Security contact	security@xtra-dev.com (monitored group address)
Review cycle	At least annually, and after any security incident or material change to the platform

1. Purpose and scope

This policy defines how Wyxloop Corp ("Wyxloop") identifies, mitigates and monitors information security risks for the Xtra-dev platform (xtra-dev.com) and its internal finance module, MyXCapital, which receives consumer financial data from data aggregators (Plaid, SimpleFIN). It applies to every person, system and vendor that stores, processes or transmits that data.

Wyxloop is a small company. The founder performs the engineering, operations and security roles described below; no other staff or contractors have access to production systems or consumer financial data.

2. Roles and responsibilities

- **Information Security Officer (ISO):** the founder. Owns this policy, approves access, reviews logs and alerts, runs incident response, and signs off on releases that touch financial data.
- **Security contact:** security@xtra-dev.com, delivered to the ISO's mailbox and monitored every business day. Vendors, partners and users may report concerns there.

3. Data classification and handling

Class	Examples	Handling
Secret	Aggregator access tokens, API secrets, encryption keys, passwords	Never stored in source code or logs. Kept in the deployment platform's secret store (environment variables) or encrypted in the database with AES-256-GCM using a key held outside the database.
Restricted	Bank and card transactions, balances, account masks, institution names received from Plaid or SimpleFIN	Stored only in the production database; shown only to the authenticated account owner; never sold, shared or used for any purpose other than the owner's own financial management.
Internal	Application logs, security event logs, configuration	Access limited to the ISO. Financial data is not written to logs.
Public	Website content, product listings	No restrictions.

Full account numbers are optional in MyXCapital; when entered they are encrypted with AES-256-GCM and only the last four digits are ever displayed.

4. Access control

- All administrative access requires a password plus time-based one-time-password (TOTP) multi-factor authentication, and new devices must be confirmed before a session is trusted. Sessions expire and can be locked.
- MyXCapital is a separate, multi-user module reachable only by people an administrator invited or granted access to. Each person has one private workspace; the server derives it from the signed-in session on every request and never from client input, so no user, administrator included, can read or change another person's financial data through the application. Every MyXCapital session requires MFA, and administrators can list who has access and remove it.
- Least privilege applies to every integration: Plaid is requested only for the Transactions product; SimpleFIN access URLs are read-only; third-party API keys are scoped to the minimum required.
- Server access is over SSH as a non-root user; root login is disabled; the firewall exposes only SSH (rate-limited), HTTP and HTTPS. The administration panel of the hosting platform is not reachable from the public Internet.
- Access is reviewed whenever an integration or account changes, and credentials that may have been exposed are rotated immediately.

5. Encryption

- In transit: all public traffic uses HTTPS with TLS 1.2 or higher, HTTP Strict Transport Security (one year, including subdomains) and automatic upgrade of insecure requests. Calls to Plaid, SimpleFIN, Stripe and Microsoft Graph use HTTPS only.

- At rest: aggregator access tokens, access URLs and account numbers are encrypted with AES-256-GCM before they reach the database. Database backups are stored in private object storage. User passwords are hashed with bcrypt.

6. Secure development and change management

- Code lives in a private Git repository. Changes are made on a feature branch, pass the automated test suite (unit tests with fake data stores, over 300 tests) and static analysis (ESLint) before deployment, and are reviewed for security (authentication, input validation, injection, secret handling) before release.
- The application enforces a strict Content Security Policy, CSRF tokens on state-changing requests, rate limiting, schema-based input validation and parameterized database access through an ORM.
- Webhooks from Plaid are verified with Plaid's signed JWT (ES256) before processing. Secrets are never committed; the deployment platform injects them at runtime.
- Deployments are immutable container builds; database migrations run automatically and are versioned.

7. Vulnerability and patch management

- Operating system security updates are applied automatically (unattended upgrades) on the production host.
- Application dependencies are reviewed at least monthly and when a relevant advisory is published; container base images are refreshed on every deployment.
- Findings are prioritized by severity: critical and high issues are fixed before the next release, others within thirty days.

8. Logging, monitoring and alerting

- Security-relevant events (logins, MFA events, administrative actions, token changes, sync failures) are recorded in a security event log retained for 180 days.
- Application errors and failed background jobs raise alerts to an operations channel monitored by the ISO; sync connections that fail or need re-authentication are surfaced in the product and alerted.
- Logs never contain financial transaction data, access tokens or passwords.

9. Data retention and deletion

- Aggregator data is retained only while the corresponding bank connection is active. Disconnecting a bank removes the connection at the aggregator (Plaid /item/remove) and disables synchronization; the owner can delete accounts and their transactions at any time.
- Encrypted database backups are produced daily and rotated on a fixed schedule; deleted data leaves backups as they rotate.
- Any request from a data subject or aggregator to delete data is honored within thirty days.

10. Incident response

1. **Detect:** alerts, log review, vendor notices or reports to security@xtra-dev.com.
2. **Triage** within one business day: scope, affected data, severity.
3. **Contain:** revoke or rotate affected credentials (including removing aggregator Items and re-issuing keys), isolate affected systems, deploy fixes.
4. **Notify:** affected parties and aggregators (Plaid, SimpleFIN) without undue delay and no later than 72 hours after confirming an incident involving consumer financial data, including what happened, what data was affected and what was done.
5. **Review:** a written post-incident summary with root cause and preventive actions, and an update to this policy where needed.

11. Business continuity

- Daily automated database backups are stored off-site in private object storage; the restore procedure is documented in the operations runbook.
- Infrastructure configuration (containers, environment, migrations) is reproducible from the repository and the deployment platform, allowing the platform to be rebuilt on a new host.

12. Third parties

Wyxloop relies on the following providers, each used over encrypted connections with the minimum scopes required: Plaid and SimpleFIN (financial data aggregation), Stripe (payments; Wyxloop never stores card numbers), Microsoft 365 (email), Contabo (virtual server hosting), and S3-compatible object storage (backups). Vendor security posture and terms are reviewed before adoption and when they change.

13. Acceptable use and awareness

The ISO follows these rules and reviews them annually: unique credentials with MFA for every service, no sharing of credentials, no production data on unmanaged devices, prompt reporting of suspected incidents, and no use of consumer financial data beyond the purposes stated in section 3.

14. Operational security program and continuous improvement

The policy is operated through a recurring calendar owned by the ISO; results and exceptions are noted in the operations log.

Activity	Cadence
Review alerts, failed jobs and the security event log	Every business day
Dependency and advisory review; apply fixes by severity (section 7)	Monthly
Access review: admin accounts, MFA status, integration keys, aggregator connections	Quarterly
Backup restore test on a disposable database	Quarterly
Rotate long-lived secrets (API keys, encryption keys where supported)	Annually or on suspicion of exposure
Policy review and update; incident lessons folded back into controls	Annually and after each incident

New integrations that touch consumer financial data go through a short risk assessment (data involved, vendor security terms, least-privilege scopes, logging and deletion path) before they are enabled.

15. Policy maintenance

This policy is stored under version control alongside the platform's source code. Changes are recorded with their date and reason. Questions and reports: security@xtra-dev.com.

Revision history

Version	Date	Change
1.0	October 13, 2026	First adopted version
1.1	October 16, 2026	MyXCapital became a separate multi-user module: access by administrator invitation or grant, one private workspace per person, MFA mandatory for every MyXCapital user, administrators can list and remove access

Related documents

- [Access Control Policy \(v1.1\)](#)
- [Data Retention and Disposal Policy \(v1.0\)](#)
- [Privacy Policy](#)