



Access Control 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
Parent policy	Information Security Policy v1.1 (section 4)
Security contact	security@xtra-dev.com (monitored group address)
Review cycle	At least annually, after any security incident, and whenever a role, system or integration changes

1. Purpose and scope

This policy defines who may access the production systems and data of the Xtra-dev platform (xtra-dev.com), including its internal finance module MyXCapital and the consumer financial data it receives from data aggregators (Plaid, SimpleFIN), and how that access is granted, verified, reviewed and removed. It covers people, service accounts and integrations, and the virtual infrastructure the platform runs on. Wyxloop Corp ("Wyxloop") has no on-premise servers.

2. Principles

- **Least privilege:** every account, key and integration receives only the permissions its function needs, for as long as it needs them.
- **Deny by default:** an API route is unreachable unless it is explicitly granted; unknown pages and endpoints return "not found".
- **Need to know:** consumer financial data is visible only to the account owner it belongs to.
- **Strong authentication everywhere:** multi-factor authentication for every administrative identity; tokens or keys, never passwords, for machines.
- **Accountability:** security-relevant actions are logged with the acting identity and reviewed.

3. Roles and permissions (role-based access control)

Role	Who	What it can reach
ADMIN	The founder and any administrator the founder provisions	The administration console; each capability is gated by a named permission (analytics, mailbox, chat, clients, users, websites, billing, security, custom PCs, media library, giveaways) checked on the server for every request
CAPITAL	People an administrator invited to MyXCapital	MyXCapital only (/capital , /api/capital/*): their own workspace and nothing else; no administration console, no client portal
ADMIN or CLIENT with MyXCapital access	Existing administrators or customers an administrator gave MyXCapital access to	What their own role reaches, plus MyXCapital under the same rules as a CAPITAL user
CLIENT	Customers of Xtra-dev	The client portal: their own profile, sessions, chat, invoices and payment methods, never other customers' data
Website API key	A customer website integrated with the platform	Only the endpoints and the single website the key was issued for; keys are rotated automatically and revoked on request
Anonymous	Public visitors	Public pages and the public API only, rate-limited

MyXCapital is a separate, multi-user module. Access exists only through an administrator's invitation (a new email) or grant (an existing account). Each person reaches only their own workspace: the server derives the workspace from the signed-in identity on every request, never from the browser. Multi-factor authentication is mandatory for every MyXCapital session. Administrators can list who has access and remove it at any time; removal signs the person out everywhere and keeps their workspace data, so access can be given back later.

Permissions are defined in one place in the codebase and enforced by server-side middleware; the user interface hides what a role cannot use, but the server is the authority.

4. Authentication

- **Passwords** are hashed with bcrypt and never stored or logged in clear text. New passwords must be at least 12 characters; a password change invalidates every other session of that user.
- **Multi-factor authentication (MFA)** with a time-based one-time password (TOTP) is mandatory for every ADMIN account and every MyXCapital user; administrative routes and MyXCapital refuse requests from sessions that have not completed MFA. Recovery codes are issued once and stored hashed.
- **Trusted devices**: a new browser must be confirmed before it can be trusted for MFA; trust expires after 30 days.
- **Sessions**: administrator and MyXCapital sessions expire after 6 hours of validity, customer sessions after 14 days; a session can be locked and requires re-authentication to unlock. Session cookies are

HTTP-only and secure.

- **Abuse protection:** login, password reset and MFA endpoints are rate-limited; state-changing requests require a CSRF token bound to the session; an administrator login that bypasses MFA raises a security alert.

5. Account lifecycle

- **Provisioning:** only the ISO creates administrator accounts or sends invitations (the `users.invite` permission); MyXCapital access is given only by an administrator, by invitation or grant. New accounts start with the minimum permissions for their function and must enrol in MFA at first login.
- **Changes:** when a person's function changes, permissions are adjusted the same day.
- **Removal:** when a person's relationship with Wyxloop ends, the ISO deactivates the account, revokes its sessions and rotates any shared credential the person could have known, before the end of that day. Removing someone's MyXCapital access ends their sessions and remembered devices at once.
- **Review:** the ISO reviews all accounts, MFA status, integration keys and aggregator connections at least quarterly and removes anything no longer needed; the review and its outcome are noted in the operations log.

6. Infrastructure and administrative access

- Production runs on virtual servers at a cloud hosting provider; there is no physical infrastructure to protect beyond the provider's data-center controls.
- Server access is over SSH with a personal key as a non-root user; root login is disabled; SSH is rate-limited at the firewall. Password login over SSH is not permitted.
- The firewall exposes only SSH, HTTP and HTTPS. The hosting control panel and its API are reachable only from the server itself or over an authenticated tunnel, never from the public Internet.
- The database accepts connections only from the application container on a private container network; it has no public port.
- Secrets (database credentials, API keys, encryption keys, aggregator credentials) live in the deployment platform's secret store and are injected at runtime. They are never committed to source control, printed in logs or pasted into chat tools.
- Workstations used for administration must use full-disk encryption, an automatic screen lock and a password manager for credentials.

7. Non-human access (services, keys, tokens)

- Service-to-service authentication uses OAuth 2.0 client credentials (Microsoft Graph), provider API keys (Stripe, hosting platform) or provider access tokens (Plaid, SimpleFIN), always over TLS. Shared passwords are not used for machine access.

- Aggregator access tokens and SimpleFIN access URLs are encrypted at rest with AES-256-GCM and decrypted only in memory at the moment of use; they are never returned by any API.
- Keys are scoped to the minimum: Plaid is requested for the Transactions product only; website API keys are bound to a single website and rotated automatically by a scheduled job; hosting-platform tokens are limited to the application they manage.
- Inbound webhooks (Plaid, Stripe, Microsoft Graph) are accepted only after their signature or shared secret is verified.
- Any credential suspected of exposure is rotated immediately and the exposure is handled as a security incident.

8. Logging, monitoring and audit

- Logins, MFA events, trusted-device confirmations, administrative actions, key rotations and integration changes are written to the security event log and retained for 180 days.
- Failed and suspicious events raise alerts to the operations channel monitored by the ISO.
- Access logs never contain passwords, tokens or financial transaction data.

9. Exceptions

Exceptions to this policy require the ISO's written approval, a stated reason, a compensating control and an expiry date, and are recorded in the operations log. Temporary elevated access is removed as soon as the task is complete.

10. Policy maintenance

This policy is stored under version control alongside the platform's source code and reviewed as stated above. 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

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