Access Controls Policy

Hatch Labs Holdings LLC

Product: AmandasList — Verified Membership Network

Document Version: 1.0 | Effective Date: March 6, 2026

Next Review Date: March 6, 2027

Classification: Confidential

1. Purpose

This policy defines the access control requirements for all systems, applications, and data managed by Hatch Labs Holdings LLC ("Company"). It ensures that access to production assets, consumer data, and sensitive business information is restricted to authorized personnel based on the principle of least privilege and role-based access control (RBAC).

2. Scope

This policy applies to:

- All production systems and databases (Supabase, Cloudflare, GitHub)
- Third-party service provider accounts (Plaid, Mercury Bank)
- Consumer-facing applications (AmandasList web and mobile)
- Internal business systems (Google Workspace, communication tools)
- All employees, contractors, and third parties with access to Company systems

3. Role-Based Access Control (RBAC)

3.1 Defined Roles

Role	Access Level	Systems	Permissions
Owner / CEO	Full Administrative	All systems	Full read/write/admin access to all production and business systems
Developer	Production Limited	GitHub, Supabase (project-level)	Read/write to codebase; read-only to production database; deploy access
Contractor	Project-Scoped	GitHub (specific repos), staging	Read/write to assigned repositories only; no production database access

		environments	
Support	Read-Only	Support tools, limited database views	Read-only access to consumer profiles for support resolution; no financial data access
Consumer	Self-Service	AmandasList application	Access to own profile, verification status, and account settings only

3.2 Role Assignment

- Access roles are assigned based on job function and approved by the CEO/Chief Security Officer
- Each user receives the minimum access necessary to perform their duties (principle of least privilege)
- Role changes require documented approval before implementation
- No shared accounts — every user has a unique, individually assigned account

4. Authentication Requirements

4.1 Password Policy

- Minimum 12 characters for administrative accounts
- Minimum 8 characters for consumer accounts
- Must include a mix of uppercase, lowercase, numbers, and special characters
- Passwords must not be reused across the last 12 password changes
- All passwords stored using bcrypt or Argon2 hashing (never plaintext)

4.2 Multi-Factor Authentication (MFA)

- MFA is **mandatory** for all administrative and production system access
- MFA is **mandatory** for all consumer accounts before accessing Plaid Link or financial data
- Acceptable MFA methods: TOTP (authenticator apps), SMS OTP, email OTP
- See *MFA Implementation Document* for full technical details

4.3 Non-Human Authentication

- Service-to-service communication uses **OAuth 2.0 tokens** or **TLS client certificates**
- API keys are stored encrypted and rotated at minimum every 90 days
- Plaid API tokens are scoped to specific products and stored encrypted at rest (AES-256)
- No hardcoded credentials in source code — all secrets managed via environment variables or secret management services

5. Production Database Access Controls

5.1 Supabase Row-Level Security (RLS)

- Row-Level Security is **enabled on all tables** containing consumer data
- Consumers can only access their own records — enforced at the database level
- Administrative queries require authenticated service role credentials
- All database queries are logged with user identity and timestamp

5.2 Direct Database Access

- Direct database connections are restricted to authorized personnel via secure, encrypted connections (TLS 1.2+)
- Connection credentials are unique per user — no shared database passwords
- Production database access is logged and auditable

6. Access Reviews and Audits

6.1 Periodic Reviews

Review Type	Frequency	Scope	Responsible Party
User Access Review	Quarterly	All production system accounts	CEO / Chief Security Officer
API Key / Token Audit	Quarterly	All API keys, service tokens, Plaid access tokens	CEO / Chief Security Officer
Permission Audit	Semi-Annually	RBAC role assignments, RLS policies	CEO / Chief Security Officer
Third-Party Access Review	Annually	All third-party vendor access	CEO / Chief Security Officer

6.2 Audit Logging

- All authentication events (login, logout, MFA, failures) are logged
- All administrative actions on production systems are logged
- All access to consumer financial data is logged with user identity, timestamp, and action performed
- Logs are retained for minimum 12 months
- Logs are stored separately from production data and protected from unauthorized modification

7. Access Provisioning and De-Provisioning

7.1 Granting Access

- All access requests must be documented and approved by the CEO/Chief Security Officer
- Access is granted based on the principle of least privilege — only the minimum access required
- New accounts are provisioned with MFA enrollment required before first use

7.2 Revoking Access

- Access is revoked within 24 hours of role change or termination
- All active sessions are terminated upon access revocation
- API keys and tokens associated with the departing individual are rotated or revoked
- Access revocation is documented and verified

8. Third-Party Access

Vendor	Access Type	Data Accessed	Controls
Plaid	API Integration	Consumer financial data (identity, income, assets)	OAuth tokens, scoped API permissions, encrypted in transit and at rest
Supabase	Infrastructure Provider	All application data (encrypted)	SOC 2 Type II certified, AES-256 encryption, access via MFA-protected dashboard
Cloudflare	DNS / CDN / WAF	Traffic metadata (no consumer PII)	MFA-protected account, API tokens scoped by zone
GitHub	Source Code Hosting	Application source code (no production data)	MFA required, branch protection rules, code review required for merges

9. Incident Response for Access Violations

- Unauthorized access attempts trigger immediate alerts
- Compromised credentials are revoked immediately upon discovery
- All affected sessions are terminated
- Incident is documented and root cause analysis is performed
- Affected consumers are notified within 72 hours if their data was potentially exposed

10. Policy Review

- This policy is reviewed and updated at minimum **annually**
- Additional reviews triggered by: security incidents, significant infrastructure changes, regulatory updates, or new third-party integrations
- **Next scheduled review:** March 6, 2027

Hatch Labs Holdings LLC | 701 Tillery Street, Suite 12, Austin TX 78702 | amanda@hatchlabs.com

Document Owner: Amanda Bradford, CEO & Chief Security Officer

Approved: Amanda Bradford | Date: March 6, 2026