SECURITY

Download PDF · Information Security Policy · Security Procedures · Privacy Policy

Access Control Policy

Product: Pinch

Operator: Joshua Lipton (sole owner and employee)

Contact: josh@5ls.us

Website: https://pinch.5ls.us

Related: Information Security Policy · Security Procedures

Version: 1.0

Effective date: September 15, 2026

Last reviewed: September 15, 2026

---

1. Purpose

This Access Control Policy defines how Pinch limits access to production systems and sensitive data—especially consumer financial data obtained through Plaid—so that only authorized, authenticated use is permitted.

2. Scope

Applies to:

- Pinch iOS app (consumer-facing)
- Supabase backend (auth, database, edge functions, and related server-side storage for Pinch)

- Operator access to vendor consoles and backends (Supabase MultiProject, Plaid Dashboard, Cloudflare/hosting, source control, secret vaults)
- API credentials, access tokens, and configuration that can affect consumer financial data

Pinch is **not** a local-only product: authenticated sessions and server-side data use **Supabase** as the backend. The iOS app is the primary consumer client.

3. Roles

Role	Person	Access principle
Owner / Information Security Lead	Joshua Lipton	Sole production operator; least privilege consistent with operating the product

There are no additional employees. Any future contractor access requires this policy to be updated before access is granted, with MFA, least privilege, and prompt revocation.

4. Consumer authentication (Supabase)

Consumers authenticate through **Supabase Auth** in the Pinch iOS app. Supported account methods:

1. **Sign in with Apple**
2. **Passkeys** (via Supabase)
3. **Email and password**
4. **Required MFA** on consumer accounts (in addition to the primary sign-in method)

After an authenticated session is established, the app may additionally use **device unlock** (Face ID or passcode) as a local screen/app lock before showing sensitive spend UI or starting Plaid Link. Face ID is **not** the primary account authentication method.

5. Operator / production access

- Unique credentials per vendor; shared passwords are prohibited
- MFA (authenticator, passkey, or vendor-supported phishing-resistant methods) is required on portals that store or process consumer financial data or control

production configuration (including Supabase and Plaid)
- Operator/account access to systems holding consumer financial data uses MFA; passkeys may be used where supported
- Secrets (including Plaid access tokens and Supabase privileged keys) are stored in vaulted / platform secret storage—not in client source or public repositories
- Sensitive edge functions and data paths use authenticated, least-privilege patterns

6. Authorization model

- Access follows least privilege and role-based assignment appropriate to a sole-operator product
- Production admin rights are limited to the owner account
- Periodic access review: at least annually, and after any material change (new vendor, incident, or expanded access)

7. Monitoring

An hourly Claude-based security monitoring bot reviews authentication anomalies, suspected data-exfiltration patterns, RBAC / unauthorized access attempts, and related security issues. Findings are triaged by Joshua Lipton.

8. Violations and exceptions

Suspected unauthorized access is treated as a security incident under the Information Security Policy and Security Procedures. Exceptions to this policy require written acknowledgment by Joshua Lipton and a time-bound remediation plan.

9. Review

This policy is reviewed at least annually and whenever Pinch’s access model or platforms change materially.