Pinch

SECURITY

Download PDF · Access Control Policy · Security Procedures · Privacy Policy

# Information Security Policy

**Product:** Pinch

**Operator:** Joshua Lipton (sole owner and employee)

**Contact:** josh@5ls.us

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

**Version:** 1.0

**Effective date:** September 15, 2026

**Last reviewed:** September 15, 2026

---

## 1. Purpose

This Information Security Policy (ISP) describes how Pinch protects information assets—especially consumer financial data obtained through Plaid—across the Pinch iOS app, the public site at pinch.5ls.us, and supporting backend systems. It is written for a sole-operator product: practices are real, proportionate, and documented without claiming certifications (for example SOC 2 or ISO 27001) that Pinch has not obtained.

The goals of this policy are to:

- Identify and reduce information security risks relevant to Pinch
- Protect confidentiality, integrity, and availability of user and system data
- Align operational security with Pinch's published Privacy Policy
- Provide clear diligence material for partners (including Plaid Production review)

---

## 2. Scope

This policy applies to:

| Asset / system | Description |
|---|---|
| **Pinch iOS app** | Consumer client; authenticates via Supabase; may cache UI locally after login |
| **pinch.5ls.us** | Public marketing website and related static hosting |
| **Backend** | Server-side components used for bank linking and related operations |
| **Supabase (MultiProject)** | **Primary backend** for Pinch: Auth, database, edge functions, and server-side storage (not a local-only architecture) |
| **Plaid** | Bank connection provider used when a user chooses to link an institution; Pinch does not use Plaid to move money or initiate payments |

This policy covers people (the sole operator), processes, and technology under Joshua Lipton's control. Third-party platforms (Plaid, Supabase, hosting providers) are governed by their own terms and security programs; Pinch's obligations are to configure and use them responsibly and to limit data shared with them to what the product requires.

---

## 3. Roles and responsibilities

| Role | Person | Responsibilities |
|---|---|---|
| **Owner / Information Security Lead** | Joshua Lipton | Owns this policy; risk decisions; access control; secret management; monitoring triage; incident response; vendor diligence; annual (or event-driven) review |
| **Sole operator** | Joshua Lipton | All development, production access, support, and security operations |

There are no other employees. Contractors or additional staff, if ever engaged, will be brought under this policy before receiving access, and this document will be updated

accordingly.

---

### 4. Risk management

Pinch manages risk in a lightweight, continuous manner appropriate for a sole-operator consumer finance app:

1. **Identify** — Threats and weaknesses related to Plaid tokens, auth, API exposure, client data handling, and vendor dependencies
2. **Assess** — Likelihood and impact relative to user harm, regulatory expectations, and partner requirements
3. **Treat** — Prefer prevention (least privilege, encryption, vaulted secrets, secure defaults); accept residual risk only consciously
4. **Monitor** — Logging, platform advisories, and the hourly Claude security monitoring bot (see §8)
5. **Review** — At least annually, and whenever a material change occurs (new vendor, architecture change, significant incident)

Risk decisions are made by the Information Security Lead. Material residual risks are recorded informally and revisited at review time.

---

### 5. Access control

- Production and administrative access is limited to Joshua Lipton
- Access follows least privilege: only accounts and roles needed to operate Pinch
- Shared credentials are avoided; where a platform requires a single owner account, MFA is enabled where available
- Service accounts and API keys are scoped to the minimum permissions required
- Offboarding is immediate by nature of a solo operator model: if access must be revoked (compromised credential, device loss), the operator rotates secrets and disables sessions as described in the Security Procedures

User data access within the product is constrained by Supabase Auth sessions and backend authorization controls (including role-based and authenticated access patterns

where implemented), plus optional device unlock on iOS after login.

---

## 6. Authentication and multi-factor authentication (MFA)

### 6.1 Consumer authentication (Supabase)

Pinch consumer accounts authenticate through **Supabase Auth** (backend is Supabase—not local-only). Supported methods:

1. **Sign in with Apple**
2. **Passkeys** via Supabase
3. **Email and password**
4. **Required MFA** for consumer accounts

Session tokens and server-side account data are handled by Supabase. Secrets and privileged keys are not embedded in client builds beyond public client configuration.

### 6.2 Device unlock (after login)

After an authenticated session exists, the iOS app may require **Face ID or passcode** as a local device unlock before showing sensitive spend UI or initiating Plaid Link. Face ID supplements the authenticated session; it does not replace Apple / passkey / email-password + MFA account auth.

### 6.3 Operator / administrative MFA

- Administrative console access (Supabase, Plaid Dashboard, hosting, source control, and related vendor portals) uses strong unique passwords and MFA wherever the vendor supports it
- Failed or anomalous authentication patterns are in scope for monitoring (see §8)

---

## 7. Encryption

### 7.1 In transit

- External network traffic for Pinch services is protected with **TLS 1.2 or higher**

- Plaid and Supabase API calls use HTTPS as provided by those platforms
- The public site pinch.5ls.us is served over HTTPS

### 7.2 At rest

- Sensitive server-side data relies on encryption-at-rest capabilities of the hosting platforms in use (including Supabase storage/database encryption as provided by the platform)
- On-device app data is protected by iOS platform storage and device security features
- Plaid access tokens and related secrets are not stored in plaintext in source control or local notes; they are kept in vaulted / platform secret storage (see §8 Secrets)

---

## 8. Secrets management

- **Plaid tokens** (and other production secrets) are stored in vaulted or platform-managed secret storage—not in plaintext repositories, chat logs, or unencrypted files intended for long-term retention
- Secrets are rotated when compromised, when personnel/device access changes, or on a scheduled basis as described in Security Procedures
- Client apps receive only the credentials appropriate for a public client (for example publishable keys); privileged secrets remain server-side
- Secret material is excluded from version control via ignore rules and review before commit

---

## 9. Logging and monitoring

Pinch uses a combination of platform logs and automated review:

- **Platform logging** — Supabase, hosting, and related vendor logs for auth, API, and operational events as available
- **Hourly Claude security bot** — An automated hourly review that examines signals for:

- Authentication anomalies

- Suspected data-exfiltration patterns

- RBAC / unauthorized access attempts

- Related security issues relevant to Pinch backend and integrations

Findings from the bot are triaged by Joshua Lipton. Confirmed issues are remediated according to severity (see Incident response and Security Procedures). Monitoring is a detection and triage aid; it does not replace secure design or access control.

---

### 10. Vulnerability management

- Dependencies and platform advisories are reviewed periodically
- Supabase security/performance advisors and similar platform signals are considered when assessing backend posture
- High-severity issues affecting production or user financial data are prioritized for remediation
- Client and server changes that touch auth, tokens, or Plaid flows receive heightened scrutiny before release

Pinch does not claim a formal bug-bounty program; security reports are welcome at josh@5ls.us (see Security Procedures).

---

### 11. Incident response (high-level)

If a security incident is suspected or confirmed:

1. **Contain** — Revoke or rotate affected credentials; disable compromised sessions; limit further exposure
2. **Assess** — Determine scope (systems, data types, users affected)
3. **Eradicate / recover** — Remove cause; restore secure configuration; verify integrity of critical paths (auth, Plaid linking)
4. **Notify** — Inform affected users and partners as required by law, contract, or good faith; contact for reports: josh@5ls.us
5. **Learn** — Document what happened at a high level; update controls and this policy if needed

Detailed operational steps live in Security Procedures. This section is intentionally high-level and does not invent a multi-person CSIRT.

---

## 12. Vendor and Plaid data handling

### 12.1 Plaid

- Users authorize Plaid to retrieve account and transaction information so Pinch can provide spend analysis features
- Pinch uses Plaid for linking and transaction retrieval—not for money movement or payment initiation
- Plaid tokens and related connection data are treated as highly sensitive and vaulted
- Pinch follows Plaid's required security and privacy expectations for Production use, including least-privilege use of Plaid APIs and secure storage of tokens

### 12.2 Supabase (MultiProject)

- Backend functions, database, and auth for Pinch-related workloads use Supabase MultiProject as configured by the operator
- Access to the Supabase project is restricted to the Information Security Lead
- Configuration aims for authenticated, least-privilege access to sensitive operations

### 12.3 Other processors

- Hosting and email (for support contact) are limited to what is needed to run the site and respond to users
- Pinch does not sell personal information and does not share user data with third parties for their advertising

---

## 13. Privacy alignment

This ISP is intended to be consistent with Pinch's Privacy Policy:

**https://pinch.5ls.us/privacy**

Key alignments include:

- Authenticated Supabase backend for accounts and server-side data; device unlock (Face ID/passcode) after login for sensitive UI
- Optional email receipt features only when enabled by the user
- No sale of personal information
- Retention limited to what is needed for the service or legal obligations
- Contact for privacy and security: josh@5ls.us

If this policy and the Privacy Policy ever conflict on a user-facing promise, the Privacy Policy governs user-facing disclosures until both documents are updated together.

---

### 14. Data retention and deletion

- **On-device data** remains until the user deletes it or removes the app
- **Plaid connection tokens and limited server-side data** are retained only as long as needed to provide the service or meet legal obligations
- When data is no longer required, it is securely deleted or disposed of using platform deletion capabilities and operator procedures
- Users may disconnect institutions in the app / through Plaid Portal where available, disable optional email scanning, delete the app, or email josh@5ls.us with privacy requests
- Retention and disposal practices are reviewed periodically by the owner (at least with the annual ISP review)

---

### 15. Policy review cadence

- **Minimum:** Review at least annually
- **Event-driven:** Review when there is a material change (architecture, new sensitive vendor, significant incident, or material product change affecting data handling)
- **Owner:** Joshua Lipton, Information Security Lead
- **Versioning:** Updates increment the version and update the “Last reviewed” date at the top of this document

## 16. Exceptions and honesty statement

Exceptions to this policy require a written note by the Information Security Lead describing the risk and compensating controls.

**Honesty statement:** Pinch is a sole-operator product. This document describes practices actually used or intended for production diligence. It does not claim SOC 2, ISO 27001, PCI DSS, or similar certifications, and it does not invent headcount, tools, or controls that are not in place.

---

## Document control

| Field | Value |
|---|---|
| Document | Information Security Policy |
| Product | Pinch |
| Version | 1.0 |
| Status | Approved for publication |
| Approved by | Joshua Lipton |
| Approval date | September 15, 2026 |
| Related | Security Procedures, Privacy Policy |