SECURITY

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

Security Procedures

Product: Pinch

Operator: Joshua Lipton (sole owner and employee)

Contact: josh@5ls.us

Version: 1.0

Effective date: September 15, 2026

Last reviewed: September 15, 2026

These procedures operationalize the Information Security Policy. They are written for a sole-operator product: clear enough for diligence and day-to-day use, without inventing a large security organization or tools that are not in use.

---

0. Consumer authentication (Supabase)

Pinch is backed by **Supabase** (auth, database, edge functions). It is **not** a local-only app.

Consumer account methods:

1. Sign in with Apple
2. Passkeys via Supabase
3. Email / password
4. Required MFA

Operational checks when changing auth:

1. Confirm MFA enforcement remains required for consumer accounts

2. Smoke-test Apple Sign In, passkey, and email/password paths in staging when available
3. Verify Plaid Link still requires an authenticated session (and device unlock if enabled)
4. Watch Supabase Auth logs for anomalies after releases

Face ID / passcode may lock the app UI after login; do not treat Face ID as the account identity provider.

---

1. Onboarding and offboarding (solo operator)

1.1 Onboarding (new access for the operator)

When setting up or expanding production access:

1. Create or use a dedicated operator identity per vendor (Supabase, Plaid, hosting, source control, secret vault)
2. Enable MFA on every portal that supports it
3. Store credentials and API secrets only in vaulted / platform secret storage
4. Confirm least-privilege roles (no broader admin rights than required)
5. Verify TLS endpoints and that production secrets are not present in client source or public repos
6. Record which systems were enabled (informal checklist is sufficient for a solo operator)

There are no additional employees to onboard. If a contractor is ever used, they must receive the minimum access required, under NDA/contract as appropriate, with MFA, and this procedure must be updated before access is granted.

1.2 Offboarding (solo model)

Offboarding in a one-person company primarily means **credential and device loss scenarios** (or voluntary wind-down):

1. Immediately rotate all production secrets (Plaid, Supabase service keys, hosting tokens, vault credentials)

2. Revoke active sessions / refresh tokens on vendor platforms where available
3. Remove local copies of secrets from devices being retired
4. Confirm no production secrets remain in email, chat, or unencrypted backups
5. If the product is shut down, revoke Plaid access, delete or dispose of retained server-side data per retention policy, and update public privacy disclosures

---

2. Secret rotation

2.1 When to rotate

Rotate secrets when any of the following occur:

- Suspected or confirmed compromise
- Device loss or unauthorized physical access
- Accidental exposure (commit, screenshot, support ticket, logs)
- Operator decision during scheduled hygiene
- Vendor notification requiring rotation

2.2 What to rotate

Priority order for Pinch:

1. **Plaid** credentials and access tokens (vaulted Plaid tokens)
2. **Supabase** service role / privileged keys and related backend secrets
3. Hosting / deploy tokens
4. Any other API keys used by Pinch backend functions

2.3 How to rotate (high-level)

1. Generate new secret in the vendor console or vault
2. Update vaulted storage and production runtime configuration
3. Redeploy or reload services that consume the secret
4. Invalidate the old secret at the vendor
5. Smoke-test critical paths: auth, Plaid link/exchange/sync as applicable

6. Note the rotation date privately (do not store the secret value in the note)

Never commit secrets to git. Never paste production secrets into untrusted tools or public channels.

---

3. Production access

3.1 Who

Only Joshua Lipton has production administrative access.

3.2 Systems in scope

- Supabase MultiProject (Pinch-related backend, database, edge functions, auth as configured)
- Plaid Dashboard and Plaid API credentials
- Hosting for pinch.5ls.us
- Source control and deploy pipelines for Pinch
- Secret vault / platform secret stores holding Plaid tokens and other production secrets

3.3 Rules of use

- Use MFA-backed sessions
- Prefer read-only exploration when diagnosing issues; make write/destructive changes deliberately
- Avoid using production credentials on untrusted networks or shared machines
- Do not grant temporary shared logins; if emergency help is ever needed, create time-limited, least-privilege access and revoke immediately after

3.4 Change hygiene

Before changes that touch auth, Plaid flows, token storage, or authorization:

1. Understand blast radius
2. Prefer staging or isolated testing when available
3. Deploy with a rollback path in mind

4. Watch logs / monitoring after deploy

---

4. Monitoring triage (Claude hourly security bot)

Pinch runs an **hourly Claude-based security monitoring bot** that reviews signals for:

- Authentication anomalies
- Suspected data-exfiltration patterns
- RBAC / unauthorized access attempts
- Related security issues

4.1 Triage workflow

1. **Receive** — Review the bot's hourly findings (or digests / alerts as configured)
2. **Classify**

- **False positive / noise** — Document briefly if useful; no further action

- **Needs investigation** — Correlate with platform logs (Supabase, hosting, Plaid)

- **Confirmed issue** — Begin containment per Incident response below

1. **Act** — Rotate secrets, revoke sessions, patch config/code, or tighten RBAC as appropriate
2. **Verify** — Confirm the anomalous pattern has stopped
3. **Close** — Note outcome for the next review cycle

4.2 Severity guidance (practical)

Severity	Examples	Target response
Critical	Confirmed token theft, unauthorized production admin access, active exfiltration	Immediate containment; rotate secrets; assess user impact
High	Clear auth bypass attempt that succeeded; exposed privileged key	Same day containment and rotation

Severity	Examples	Target response
Medium	Repeated failed auth anomalies; suspicious but unverified patterns	Investigate within 1–2 days
Low	Isolated noise; informational advisories	Batch into routine review

The bot is a detection aid. Absence of a finding does not prove absence of risk; presence of a finding requires human judgment.

---

5. Patching

1. Apply security-relevant updates to dependencies and platforms in a timely manner, prioritizing issues that affect auth, cryptography, or data exposure
2. Review Supabase (and similar) security advisories when assessing backend posture
3. After patching production, verify Pinch critical paths (app auth, Plaid link, sync/webhook handlers as applicable)
4. Do not leave known critical vulnerabilities unaddressed without a written compensating control and a remediation date

---

6. Backup assumptions

Pinch uses **Supabase** for auth and server-side data. The iOS client may cache UI locally after login. Backup expectations:

- **User device data** — Protected by iOS settings and optional Face ID/passcode app unlock after an authenticated Supabase session
- **Server-side / Supabase** — Relies on platform-managed durability and recovery capabilities of Supabase MultiProject as configured; the operator does not claim a separate custom off-site backup appliance unless one is later implemented and this procedure is updated
- **Secrets** — Vault configuration and recovery methods must themselves be protected; losing vault access without recovery is treated as an operational emergency

- **Marketing site** — Static site content is recoverable from source control / deploy history

These assumptions should be revalidated at each annual policy review.

---

7. Reporting security issues

Email: josh@5ls.us

Please include:

- A clear description of the issue
- Steps to reproduce (if applicable)
- Affected component (iOS app, pinch.5ls.us, backend/API, Plaid-related flow)
- Your contact information for follow-up
- Whether you believe user data was accessed or exposed

7.1 What to expect

- Acknowledgement as promptly as a sole operator can manage
- Good-faith investigation and remediation when a valid issue is confirmed
- Notification to affected parties when required by law, contract, or responsible disclosure practice

7.2 Please do not

- Access or exfiltrate user data beyond what is needed to demonstrate a issue
- Perform destructive testing against production without prior written coordination
- Publicly disclose before allowing a reasonable window to remediate (unless users are at imminent risk and delay would increase harm)

Pinch does not currently operate a paid bug bounty. Responsible reports are appreciated.

---

8. Incident response (operational steps)

Aligned with the high-level ISP process:

1. **Detect** — Bot alert, vendor notice, user report, or operator observation
2. **Contain** — Rotate credentials; revoke sessions; disable vulnerable endpoints if needed
3. **Investigate** — Scope systems, time window, and data categories (especially Plaid tokens / transaction data)
4. **Remediate** — Fix root cause; patch; re-deploy; re-enable only when safe
5. **Communicate** — josh@5ls.us is the contact; notify users/partners as required
6. **Post-incident** — Short written notes on cause, impact, and control changes; update ISP/procedures if material

---

9. Vendor-specific notes

Plaid

- Treat access tokens as highly sensitive; keep vaulted
- Use Plaid only for authorized account/transaction retrieval for Pinch features
- Do not use Plaid to move money or initiate payments
- Follow Plaid Dashboard security settings (MFA, team access limited to the owner)

Supabase MultiProject

- Restrict dashboard access to the owner with MFA
- Prefer authenticated, least-privilege patterns for sensitive edge functions and data access
- Review platform advisors periodically as part of vulnerability management

---

10. Review

These procedures are reviewed at least annually and when material changes occur, together with the Information Security Policy.

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