Points & Prompts — Information Security & Access Control Policy

This document is our Information Security Policy and our Access Control Policy.

Document owner	Jeremy Smith, Founder — privacy@pointsandprompts.com
Version	1.0
Effective date	July 25, 2026
Review cadence	At least annually and upon material change
Classification	Public

1. Purpose and Scope

This policy defines how Points & Prompts ("P&P," "we") protects the information it handles, including consumer data received through the Plaid API. It applies to all systems, code, and personnel involved in operating pointsandprompts.com and its supporting infrastructure (Supabase, Cloudflare, and source control). The guiding principle throughout is **data minimization**: the most effective control is not collecting or retaining data we do not need.

2. Governance and Risk Management

2.1 Ownership. A named owner (the Founder) is accountable for information security and privacy and is the point of contact for any Plaid-identified remediation.

2.2 Policy review. This policy is reviewed at least annually and whenever a material change occurs to the product, its data flows, or its infrastructure.

2.3 Risk approach. Security is evaluated whenever a feature that touches user or financial data is designed or changed, and findings are remediated on a risk-prioritized basis.

3. Data Minimization and Classification

3.1 Bank credentials are entered only within Plaid's secure Link window and are never seen by, transmitted to, or stored by P&P.

3.2 Transactions retrieved through Plaid's read-only Transactions product are aggregated in memory into monthly totals per spending category. Individual transactions, merchant names, and full account numbers are never written to our database.

3.3 We persist only: (a) monthly category totals (overall and per card, current plus up to 12 prior months); (b) the connected institution's name; and (c) the Plaid access token required to refresh those totals.

3.4 Consumer financial data is classified as Confidential and is subject to the access controls in Section 4.

4. Access Control Policy

4.1 Least privilege. Access to production systems and data is granted on a least-privilege basis. Application clients hold only public anon/authenticated keys and have no direct privileges on sensitive tables.

4.2 Role-based access control and row-level security. The database enforces role-based access control (anon, authenticated, service_role) and row-level security (RLS) so that each authenticated user can access only their own records. Every user-data table has RLS enabled with owner-scoped policies.

4.3 Isolation of secrets and tokens. Tables that store Plaid access tokens and audit records carry no privileges for application roles and are reachable only by trusted server-side functions running as the service role. Plaid access tokens are never exposed to the client.

4.4 Non-human authentication. Server-to-server and function-to-database authentication uses scoped tokens and keys transmitted only over TLS; no shared static credentials are embedded in client code.

4.5 Administrative multi-factor authentication. MFA is required for administrative access to every system that stores or processes consumer financial data: the database/auth provider (Supabase), source control (GitHub), and hosting/DNS (Cloudflare). Access to the Plaid Dashboard is federated through Google SSO, which enforces 2-Step Verification.

4.6 Periodic access reviews. An automated access review runs weekly. It re-runs the database security advisors, verifies that RLS and owner-scoped policies remain in force on user-data tables, confirms that token and audit tables remain closed to application roles, checks for newly introduced tables or grants, and reports any regression. The access model and this policy are additionally reviewed at least annually.

4.7 Provisioning and de-provisioning. Access is currently limited to the Founder; any future addition or removal of personnel access is recorded and confirmed as part of the weekly and annual reviews.

5. Consumer Authentication

User accounts are protected by email-based authentication (Supabase Auth) with confirmed-email sign-up, secure session tokens, and server-side authorization checks on every request. Because stored data is read-only, category-level, and non-transactional — the application cannot move money or expose account numbers — consumer MFA is maintained as a roadmap enhancement rather than a requirement before Plaid Link.

6. Infrastructure and Network Security

6.1 Encryption in transit. All traffic between clients and servers uses TLS 1.2 or higher.

6.2 Encryption at rest. Data received from Plaid and stored in our database is encrypted at rest (AES-256) by our infrastructure providers.

6.3 Managed, audited providers. Compute, database, and network infrastructure are operated by managed providers (Supabase, Cloudflare) whose platforms are continuously patched and independently audited (e.g., SOC 2).

7. Development and Vulnerability Management

7.1 Endpoint protection. Developer endpoints run OS-level anti-malware and host firewalls, apply operating-system security updates automatically, use full-disk encryption, and require MFA to reach production systems.

7.2 Dependency management. Application dependencies are monitored for known vulnerabilities and updated as fixes are released.

7.3 Platform patching. Production servers and platform components are continuously patched by the managed providers.

7.4 Change management. Changes are tracked in version control and deployed through an automated pipeline; database schema changes are applied as reviewed migrations.

8. Privacy, Consent, Retention, and Deletion

8.1 A Privacy Policy is published for the application where Plaid Link is deployed (pointsandprompts.com/privacy).

8.2 Connecting a bank is optional and requires explicit consumer consent through Plaid Link.

8.3 Retention. Only monthly category totals for the current and up to the last 12 months are retained; older snapshots are pruned automatically.

8.4 Deletion. Disconnecting a bank removes the connection and instructs Plaid to remove its access; deleting an account removes the user's stored data. Both controls are available to the user in-app.

9. Incident Response

Suspected security incidents are triaged by the owner. Response steps include containing the issue (for example, rotating affected tokens and keys and revoking access), assessing scope, remediating the root cause, and notifying affected parties and Plaid as required. The weekly access review serves as a primary early-detection control for access drift.

10. Contact

Security or privacy questions, and coordination of any Plaid remediation: privacy@pointsandprompts.com.