Information Security Policy

Governance, principles, and security commitments for the Splits platform.

Effective	May 19, 2026	**Version**	1.0
Organization	Splits	**Owner**	Mustafa Alhelawe, Founder
Contact	security@splitshq.com	**Review cadence**	Annual

---

1. Purpose and Scope

This Information Security Policy ("Policy") establishes Splits's overall approach to safeguarding the confidentiality, integrity, and availability of information assets used to operate the Splits service (the "Service"). The Service is a personal-finance ledger that tracks IOUs between friends and uses Plaid to detect recurring shared bills.

This Policy applies to all individuals who access systems, data, or development resources owned or operated by Splits, including the founder, contractors, and any future employees. It governs production systems, source code repositories, third-party SaaS accounts used to operate the Service, and developer endpoints used to access them.

2. Roles and Responsibilities

Splits currently operates as a solo-founder organization. The Founder, Mustafa Alhelawe, holds end-to-end responsibility for information security, privacy, vendor management, incident response, and policy maintenance.

As the organization grows, security responsibilities will be reassigned and additional roles (such as a designated Security Officer, Privacy Lead, and Incident Commander) will be appointed. Until then, all such responsibilities default to the Founder.

Security questions, vulnerability reports, and policy inquiries should be directed to security@splitshq.com.

3. Security Principles

Splits' security program is guided by the following principles:

- Least privilege: every person and every service has the minimum access required to perform its function.
- Defense in depth: multiple controls protect each asset, so that the failure of one layer does not result in compromise.
- Secure by default: production code and infrastructure ship with conservative security settings; relaxations require explicit justification.

- Verify, don't assume: authentication is required on every request to user-facing endpoints; trust is never derived solely from network location.
- Transparency: data practices are documented in the Privacy Policy and made available to users.

4. Risk Management

Splits performs an informal risk assessment at least annually and whenever a material change occurs (for example, adding a new vendor that processes consumer data, introducing a new data category, or changing authentication mechanisms). The assessment considers threats to confidentiality, integrity, and availability across the application, infrastructure, vendors, and developer endpoints.

Identified risks are tracked, prioritized, and either mitigated, accepted, or transferred. Accepted risks are reviewed at the next annual cycle.

5. Access Control

Access to Splits production systems, source code, and administrative tooling is governed by the Access Controls Policy. Key commitments include role-based access control (RBAC) enforced at the database layer via Supabase Row-Level Security, multi-factor authentication on all administrative accounts, and phishing-resistant MFA (passkeys / WebAuthn) for end-users prior to bank linking and other sensitive actions.

6. Data Classification and Handling

Splits handles the following categories of information:

- **User account data:** email, hashed password (managed by Supabase Auth), display name, and optional payment-handle identifiers (Venmo / Cash App usernames).
- **Consumer financial data:** bank-account metadata, balances, and transactions retrieved from Plaid; institution names and account masks.
- **Authentication secrets:** Plaid access tokens, MFA factors (TOTP secrets, registered passkeys), and step-up challenge state.
- **Ledger data:** IOU entries, split rules, balances, and payment records between users.

All data categories are treated as confidential by default. Authentication secrets and consumer financial data are treated as the most sensitive and receive additional protections (encryption, restricted access paths, no logging).

7. Encryption

7.1 In Transit

All connections to Splits services are protected by TLS 1.2 or higher. TLS termination is provided by Vercel for the Splits web application and by Supabase for database, authentication, realtime, and storage endpoints. Older protocol versions and weak cipher suites are disabled at the platform level.

7.2 At Rest

All consumer data retrieved from Plaid is encrypted at rest. The Supabase Postgres database that stores user, ledger, and Plaid-derived data is hosted on AWS and encrypted at the storage layer using AES-256. In addition, Plaid access tokens receive application-layer encryption with AES-256-GCM before being persisted, using a key held in the production environment and never written to logs or source control.

8. Network and Infrastructure Security

Splits does not operate its own physical or virtual infrastructure. The Service is hosted on Vercel; data and authentication services are hosted on Supabase; bank-data integration is provided by Plaid; and SMS one-time codes are provided by Twilio. Each vendor is responsible for the physical, network, and host-level security of the infrastructure it provides.

Splits performs the following infrastructure-level controls:

- Production secrets (API keys, encryption keys, OAuth credentials) are stored only in the production environment configuration of each vendor and never committed to source control.
- Database access from application code is mediated by Supabase service keys; per-user access uses short-lived JWTs issued by Supabase Auth.
- Webhook endpoints validate vendor signatures before processing payloads.

9. Vulnerability Management

Splits maintains a documented Vulnerability Management Policy describing scanning, classification, patching SLAs, and end-of-life software monitoring. See the Vulnerability Management Policy for details.

10. Incident Response

If Splits becomes aware of a security incident affecting the confidentiality, integrity, or availability of user data, the following high-level steps are taken:

- Contain the incident by revoking affected credentials, isolating affected systems, or disabling impacted code paths.
- Investigate the scope, root cause, and affected users.
- Notify affected users and relevant data partners (including Plaid, where Plaid-sourced data is involved) without undue delay and in accordance with applicable law.

- Remediate the underlying cause and document lessons learned.

Post-incident reviews are conducted in a blameless manner and produce written findings retained for at least two years.

11. Third-Party and Vendor Management

Splits relies on the following primary vendors for production operations: Vercel (application hosting), Supabase (database, authentication, realtime, storage), Plaid (financial-account connectivity), Twilio (SMS one-time passcodes), GitHub (source code hosting), PostHog (product analytics), and Sentry (application error monitoring).

Each vendor is selected based on its security posture, available compliance attestations, and contractual commitments. Vendor configurations are reviewed at least annually, and any new processor that will handle consumer data is evaluated before onboarding.

12. Privacy and Data Subject Rights

Splits' privacy practices are described in the Privacy Policy, which is published at the Service and reviewed annually. Users may request access to, correction of, or deletion of their personal information by contacting the Founder or by using in-product controls in the Settings area.

13. Data Retention and Disposal

Data retention periods and disposal procedures are described in the Data Retention and Disposal Policy. Key commitments include cascade deletion of user data upon account deletion, prompt revocation of Plaid access tokens upon disconnection, and removal of consumer financial data from backups within the documented backup retention window.

14. Security Awareness

All individuals with access to Splits production systems receive informal security guidance covering phishing, credential hygiene, secret handling, and incident reporting. As the organization grows, formal security-awareness training will be implemented for all personnel with access to production data.

15. Enforcement

Violations of this Policy may result in revocation of access, contract termination, or other corrective action as appropriate. Concerns or suspected violations should be reported to the Founder at the contact email above.

16. Policy Review and Maintenance

This Policy is reviewed at least annually by the Founder, and additionally whenever a material change occurs in Splits' operations, vendors, or regulatory environment. The current version is v1.0, effective May 19, 2026.