

Information Security Policy

Effective date	July 2, 2026 (v1.1 revised July 3, 2026)
Policy owner	Elizabeth Peterson, Owner — ekathleen@lotusbloomllc.com
Review cadence	Annually, or upon material change to systems or vendors
Scope	All LotusBloom LLC production systems, including lotusbloomllc.com, the Credit Hub application, RepoLens, and supporting infrastructure.

1. Purpose and Scope

This policy documents how LotusBloom LLC identifies, mitigates, and monitors information-security risks across its products and infrastructure. It covers all systems that store or process user data: the production web application (Vercel), the production database (Neon PostgreSQL), payment processing (Stripe), financial-data aggregation (Plaid), and transactional email (Resend).

2. Governance

The Owner is the designated resource responsible for information security, vendor review, incident response, and this policy's maintenance. Security-impacting changes — new vendors, new data categories collected, or new integrations — require Owner review before deployment.

3. Data Classification and Handling

- **User credentials:** Passwords are hashed with bcrypt before storage. Plaintext passwords are never stored or logged.
- **Financial-institution tokens (Plaid access tokens):** Encrypted at rest with AES-256-GCM using a dedicated encryption key held only in the production secret store.
- **User financial data:** Stored per-user in the production PostgreSQL database (Neon), encrypted at rest by the provider, with TLS in transit.
- **Payment card data:** Never touches LotusBloom systems. All payment processing is delegated to Stripe-hosted checkout (a PCI DSS Level 1 service provider).
- **Guest-mode data:** Credit Hub's guest mode stores data exclusively in the user's own browser (localStorage); it is never transmitted to or stored on LotusBloom servers.

4. Identity and Access Management

- Production infrastructure (Vercel, Neon, Stripe, Plaid, Resend, domain registrar) is accessible only to the Owner. There are no shared accounts.
- Access to each provider is protected by a unique, strong password, with multi-factor authentication enabled where the provider supports it.
- Application secrets (API keys, database credentials, signing secrets, encryption keys) are stored as encrypted environment variables in Vercel's secret store — never committed to source control and never embedded in client-side code.
- Session management uses HMAC-SHA256-signed, httpOnly cookies with a cryptographically random signing secret and 30-day expiry.
- Internal scheduled endpoints (cron) are protected by bearer-token secrets.

5. Application Security

- All traffic is served exclusively over HTTPS/TLS.
- Authentication endpoints are rate-limited (per-IP and per-account) to resist credential-stuffing and brute-force attacks.
- Webhook endpoints verify cryptographic signatures (e.g., Stripe webhook signature verification) before processing.
- Payment entitlements are granted only server-side upon verified webhook events; client-supplied state is never trusted for authorization.
- Password reset uses single-use, hashed, time-limited (one-hour) tokens.

6. Vendor Management

LotusBloom relies on SOC 2-audited infrastructure providers: Vercel (hosting), Neon (database), Stripe (payments), Plaid (financial-data aggregation), and Resend (email). Vendor security posture is considered before adoption, and the number of vendors with access to user data is deliberately kept minimal.

7. Data Retention, User Rights, and Deletion

- Users may export all of their data at any time via a self-service export endpoint.
- Users may delete their account at any time; deletion cascades to all associated records (accounts, snapshots, receipts, assessments, tokens).
- Users may disconnect linked financial institutions at any time, which revokes and removes stored access tokens.
- The public privacy policy (lotusbloomllc.com/privacy) discloses data practices and includes CCPA provisions.

8. Risk Identification and Monitoring

- Deployment logs and function logs are retained and reviewable in Vercel.
- Payment and webhook activity is monitored via the Stripe dashboard.
- Database access and usage are monitored via the Neon console.
- Dependency updates are applied as part of routine development; production frameworks and libraries are actively maintained releases.

9. Incident Response

Upon discovery of a suspected security incident, the Owner will: (1) contain the issue — rotate affected credentials and disable affected endpoints; (2) assess scope and affected users; (3) remediate the root cause; (4) notify affected users and applicable authorities as required by law, including CCPA and state breach-notification statutes; and (5) document the incident and corrective actions taken.

10. Secure Development Practices

- Source code is version-controlled in a private repository; secrets are excluded from version control.
- Production deploys run through Vercel's build pipeline; database schema changes are applied through versioned migrations.
- New features touching authentication, payments, or financial data receive explicit security review by the Owner before release.

11. Multi-Factor Authentication

- **Internal systems:** All administrator access to systems that store or process consumer data (Vercel, Neon, Stripe, Plaid, Resend, and the root email identity) is protected by multi-factor authentication, including passkeys (phishing-resistant, WebAuthn) and TOTP authenticator apps. Recovery codes are stored in a password manager.
- **Consumer application:** Sign-in to the consumer application requires a second factor: after password verification, a single-use 6-digit code is emailed to the account holder and must be entered before a session is issued. Codes are stored only as SHA-256 hashes, expire after 10 minutes, allow at most 5 attempts, and are rate-limited. A successfully verified browser may be marked trusted for 30 days via a signed, user-scoped, httpOnly cookie. Plaid Link is surfaced only to fully authenticated users.

12. Vulnerability Management and Patch SLA

- **Automated scanning:** A scheduled job runs weekly (Vercel Cron) that checks every production dependency, at its exact resolved version, against the OSV.dev vulnerability database and emails findings to the security contact (admin@lotusbloomllc.com). Scan results are also retained in structured platform logs.

- **Patch SLA:** Identified vulnerabilities are remediated within defined timelines by severity: **Critical — 72 hours; High — 14 days; Medium — 30 days; Low — next routine development cycle.**
- **End-of-life monitoring:** Production frameworks and libraries are kept on actively maintained release lines; end-of-life software is replaced before support lapses.
- **Platform patching:** Underlying infrastructure (compute, database, network) is patched by the SOC 2-audited providers (Vercel, Neon) as part of their managed services. The development workstation runs macOS with automatic security updates and FileVault full-disk encryption enabled.

13. Periodic Access Reviews

The Owner conducts a documented access review at least **quarterly**, covering every system with access to production or consumer data: authorized users and their roles, third-party team members and integrations, MFA status, API keys and tokens (rotating any that are stale or unused), and OAuth grants. Findings and remediation actions are recorded in a dated access-review log retained with company records.

14. Personnel Security and De-provisioning

LotusBloom LLC currently operates with a single principal (the Owner) and no employees or contractors with systems access. Before any employee or contractor is granted access, the following controls take effect: (1) access is provisioned per-person — never shared — at the minimum privilege required; (2) all grants are recorded in the access-review log; (3) upon termination, role change, or contract end, all access is revoked **within 24 hours**, including provider seats, repository access, API keys known to the individual (rotated), and any OAuth grants; and (4) the next scheduled access review verifies completeness of the removal.

15. Zero Trust and Centralized Identity Management

- **No trusted network:** The architecture is fully serverless with no internal network, VPN, or perimeter inside which requests are implicitly trusted. Every request to every service is independently authenticated and authorized: user requests via signed session cookies (issued only after MFA), API requests via secret keys, scheduled jobs via bearer tokens, and webhooks via cryptographic signature verification. Client-supplied state is never trusted for authorization decisions.
- **Centralized identity:** Administrative access to all providers is consolidated under a single owner identity secured with MFA; there are no shared or secondary accounts. Application secrets are centralized in one encrypted store (Vercel environment variables) rather than distributed across configuration files or machines, providing a single point of visibility, rotation, and revocation.
- **Least privilege by construction:** Each credential grants only the scope it needs (e.g., read-only financial data access, per-purpose API tokens), and the consumer application's guest mode operates with no server-side data access at all.

Adoption

This policy was adopted by LotusBloom LLC on July 2, 2026. Revision 1.1 (July 3, 2026) added sections 11–15: multi-factor authentication, vulnerability management and patch SLA, periodic access reviews, personnel de-provisioning, and zero-trust / centralized identity architecture.

Elizabeth Peterson, Owner — LotusBloom LLC

LotusBloom LLC · Woodland, California · lotusbloomllc.com · Confidential