

FinanceDeck Information Security Policy

Owner: Digital Block Enterprises (12192934 Canada Inc.)

Effective: August 19, 2026

Review cadence: annually, or immediately following any material security incident or architecture change.

1. Purpose and Scope

This policy governs how FinanceDeck ("the application," operated at myfinancedeck.com) identifies, mitigates, and monitors information security risk relevant to the consumer financial data it handles, including data received via Plaid.

2. Responsible Party

The individual(s) responsible for information security are listed in the project's operational contacts. Security concerns, including responsible disclosure of vulnerabilities, should be sent to support@myfinancedeck.com (see also /.well-known/security.txt on the production domain).

3. Access Control

- Access to production infrastructure (hosting, database, payment processor, and bank-data provider dashboards) is limited to designated administrators only, on a least-privilege basis.
- Multi-factor authentication (MFA) is required on all accounts with access to production infrastructure that stores or processes consumer financial data (hosting provider, database provider, payment processor, and Plaid dashboard).
- Credentials and API secrets are never committed to source control and are managed via the hosting provider's encrypted environment variable store.

4. Data Encryption

- All data in transit between clients and servers is encrypted using TLS 1.2 or higher.
- Sensitive account identifiers (bank name, account name, and free-text notes) are encrypted at the application layer using AES-256-GCM before being written to the database.
- Underlying database storage is encrypted at rest by the database provider's infrastructure.
- Plaid access tokens are encrypted at the application layer before storage and are never logged or exposed to client-side code.
- Plaid access is used strictly in read-only mode. The application never initiates payments, transfers, or writes to a connected bank account.

5. Vulnerability Management

- Automated dependency vulnerability scanning (GitHub Dependabot) is enabled on the application repository, covering both application dependencies and CI/CD workflow dependencies.
- Identified vulnerabilities are patched within a defined SLA based on severity:
 - Critical and High severity: patched within 7 days of alert.

- Medium and Low severity: patched within 30 days of alert.
- Security-relevant dependency updates are reviewed and merged in a timely manner following automated alerts.
- As the team grows, this policy will be extended to include scheduled scanning of employee and contractor endpoint devices.

6. Development Practices

- Code changes are tracked through version control with a documented commit history.
- Continuous integration checks (type-checking, linting, and automated tests) run on changes before they are merged.

7. Privacy and Consumer Data Rights

- The application maintains a public Privacy Policy (myfinancedeck.com/privacy) describing what data is collected, why, and which third parties process it.
- Consent to data collection and processing is captured and timestamped at account creation.
- Users may permanently delete their account and all associated data at any time from Settings. Deletion requests are processed immediately.
- Data retention: account and financial data is retained only while the account is active, and is deleted upon user-initiated account deletion. This retention practice is reviewed as part of the annual policy review described above.

8. Incident Response

In the event of a suspected security incident involving consumer data:

1. The responsible party (Section 2) investigates and contains the issue.
2. Affected third-party providers (e.g., Plaid, Stripe) are notified as required by their respective agreements.
3. Affected users are notified without undue delay, consistent with applicable privacy law (including PIPEDA).
4. A post-incident review is conducted and this policy is updated if gaps are identified.

9. Third-Party Sub-processors

See myfinancedeck.com/security for the current, maintained list of third-party service providers with access to application data and what each one can see.