Information Security Policy and Procedures

Budg!t Pro — Hansgemachter

Effective Date: March 30, 2026

Version: 1.0

Reviewed Annually

1. Purpose

This policy establishes the information security practices and procedures for Budg!t Pro, a locally installed Windows desktop application developed and maintained by Hansgemachter. The purpose is to identify, mitigate, and monitor information security risks relevant to the application and its use of the Plaid API.

2. Scope

This policy applies to all aspects of Budg!t Pro development, distribution, and operation, including source code management, third-party API integrations, application distribution, and consumer financial data handling.

3. Security Architecture

Budg!t Pro is architected to minimize security risk by design:

- The application is entirely locally installed with no cloud backend, no shared servers, and no centralized database. - All consumer financial data remains on the user's own device at all times. - The application has no user authentication system — each installation is inherently single-user. - Network communication occurs exclusively between the local application and Plaid's API endpoints over HTTPS using TLS 1.2 or higher.

4. Access Control

- Source code is stored in GitHub repositories accessible only to the developer with multi-factor authentication (MFA) enforced on the GitHub account. - Plaid API credentials (Client ID and Secret) are never hardcoded in source code and are never committed to version control. - API credentials are stored as environment variables or in a local configuration file outside the application's distributed package. - The Microsoft Store Developer account used for distribution is protected with MFA.

5. Secure Development Practices

- All application dependencies are monitored for known vulnerabilities using GitHub Dependabot and npm audit. - Identified vulnerabilities are remediated within 30 days of discovery for critical/high severity, and 90 days for medium severity. - All code changes are reviewed before release. - The application is built using GitHub Actions in an isolated CI/CD environment with no persistent credentials stored in the pipeline beyond repository secrets. - End-of-life software dependencies are identified and updated as part of each release cycle.

6. Distribution Security

- Budg!t Pro is distributed exclusively through the Microsoft Store, which performs independent security scanning and code signing verification of all submitted packages. - All distributed binaries are produced by the GitHub Actions build pipeline from verified source code. - Application updates are delivered through the Microsoft Store's secure update mechanism.

7. Third-Party API Security

- Plaid integration follows Plaid's security best practices including use of short-lived link tokens, secure storage of access tokens, and read-only API access. - The application requests only the minimum necessary Plaid API permissions (Balance and Transactions). - Plaid access tokens are stored locally on the user's device and are never transmitted to any Hansgemachter-controlled server. - Users can revoke Plaid access at any time by disconnecting their bank account within the application.

8. Incident Response

In the event of a suspected security incident:

- The developer will investigate and assess the scope within 48 hours of discovery. - Affected Plaid access tokens will be revoked immediately if a compromise is suspected. - Affected users will be notified via the Microsoft Store update mechanism and/or application update within 72 hours. - A patched application version will be submitted to the Microsoft Store within 7 days of confirmed incident.

9. Risk Monitoring

- GitHub Dependabot alerts are reviewed weekly for new vulnerability disclosures affecting application dependencies. - Plaid API changelog and security advisories are monitored monthly. - Microsoft Store developer security advisories are monitored as published. - This policy and associated security controls are reviewed annually and updated as necessary.

10. Contact

For security concerns or to report a vulnerability:

Hansgemachter Email: available via the Microsoft Store product listing Application: Budg!t Pro