TABKEEPER SECURITY OVERVIEW

Version 1.1 · Effective Date: July 26, 2026 · Last Updated: August 10, 2026 Security is foundational to Tabkeeper. Our customers trust us with financial information, and we build and operate the Services with that responsibility in mind. This Security Overview describes, at a practices level, how Tabkeeper Inc. ("Tabkeeper," "we," "us") protects the Services and Customer Content. This document is provided for transparency and general information. It is not a contract, does not amend the Terms of Service or any agreement, and does not create warranties or commitments; Tabkeeper's contractual obligations are stated in the Tabkeeper Legal Framework, including Section 35 of the Terms of Service. Capitalized terms have the meanings given in Section 3 of the Terms of Service. Our practices evolve as the platform and the threat landscape evolve.

1. Encryption Customer Content is encrypted in transit between your device and the Services using modern transport-layer security, and encrypted at rest in our production data stores using industry-standard encryption. Encryption key management is handled through our cloud infrastructure providers' managed key services.

2. Financial Account Connections Bank and financial account connections are made through our data aggregation provider, Plaid. When you link an account, your banking credentials are provided directly to the aggregation provider through its secure interface — Tabkeeper does not receive or store your bank login credentials. Connections are read-only: the Services retrieve transactions, balances, and account information, and cannot move money. You can disconnect a linked account at any time.

3. Payments Subscriptions purchased in our iOS app are billed by Apple through In-App Purchase — Tabkeeper receives purchase confirmations and subscription status from Apple, never your payment card details. Where purchases are made directly from Tabkeeper (for example, web checkout or Bookkeeping Services, where offered), payments are processed by Stripe, a PCI-DSS Level 1 certified payment processor, with card details collected through Stripe's secure fields and vaulted by Stripe. In all cases, full payment card numbers are not stored on Tabkeeper's systems.

4. Access Controls Access to production systems and Customer Content is restricted to personnel who need it for legitimate purposes — support, onboarding, bookkeeping engagements, troubleshooting, security, and compliance — under role-based access controls and least-privilege principles. Personnel are bound by confidentiality obligations, and administrative access is logged. Within the product, Customers control access to their own Workspaces through User Roles (Owner, Administrator, Manager, Employee, Viewer, where offered), and audit logging of Workspace activity may be available, where offered.

5. Authentication Passwords are stored using strong one-way hashing — Tabkeeper cannot read your password. Session management includes protections against session hijacking, and additional sign-in protections such as multi-factor authentication may be offered as the platform evolves. We encourage every customer to use a strong, unique password and to enable available security features.

6. Infrastructure The Services run on established cloud infrastructure providers in the United States, benefiting from those providers' physical security, network protections, and compliance programs. Our current infrastructure and service providers are listed in the Tabkeeper Subprocessor List, and each is engaged under agreements with confidentiality and data protection obligations.

7. Backups and Resilience Production data is backed up on a routine, automated basis, with backups retained for up to ninety (90) days. We maintain commercially reasonable business continuity and disaster recovery practices designed to restore the Services in the event of a significant disruption.

8. Monitoring and Secure Development We use logging, monitoring, and error-tracking tooling to detect availability, performance, and security issues. Code changes go through review before deployment, dependencies are updated as vulnerabilities are disclosed, and we assess the security impact of significant changes to the platform.

9. Incident Response We maintain incident response procedures covering identification, containment, remediation, and communication. If an incident affects your unencrypted personal information, we will use commercially reasonable efforts to notify you without undue delay and in accordance with applicable law, as described in the Privacy Policy and Section 35.3 of the Terms of Service.

10. Data Retention and Deletion You can export your data (CSV, PDF, or Excel) at any time. Following account deletion or a verified deletion request, Customer Content is deleted or de-identified within ninety (90) days, with backup copies aging out within a further ninety (90) days, except where law requires longer retention — as described in Section 33 of the Terms of Service and Section 7 of the Privacy Policy.

11. Reporting a Vulnerability We welcome good-faith security research. If you believe you have found a vulnerability in the Services, please email support@tabkeeper.io with the subject line "Security Report" and reasonable detail to reproduce the issue. Please do not access other customers' data, degrade the Services, or publicly disclose an issue before we have had a reasonable opportunity to address it. We will acknowledge good-faith reports and keep reporters informed as we remediate. We do not currently operate a paid bug bounty program.

12. Questions Security questions, due-diligence requests, and vendor reviews: support@tabkeeper.io.