1099 Ops Information Security Policy

Effective date: May 6, 2026 **Last updated:** May 6, 2026 **Contact:** security@1099ops.app / support@1099ops.app

Overview

1099 Ops maintains an information security program designed to protect customer accounts, financial workflow data, connected-account metadata, authentication systems, production infrastructure, and internal operational systems.

Our approach is privacy-minimized: sensitive bank access, payment card handling, authentication, hosting, and other specialized operations are handled by vetted third-party providers. 1099 Ops is designed to store only the information needed to operate the product and support customer-requested workflows.

1. Scope

This policy applies to 1099 Ops application systems, production infrastructure, source code repositories, CI/CD and deployment systems, database and storage systems, customer support workflows, third-party processors, and authorized personnel or contractors with access to 1099 Ops systems.

2. Data Minimization

1099 Ops collects and stores only the data required to provide the Service. We do not intentionally collect Social Security Numbers, NPIs, full bank account numbers, routing numbers, full card numbers, or bank login credentials.

For connected financial accounts, Plaid handles bank credential collection and bank-side access through Plaid Link. 1099 Ops receives limited account and transaction metadata needed for income detection, expense classification, transfer/refund/payment review, tax-reserve estimates, cash-flow summaries, and user review prompts.

3. Third-Party Processors

We use trusted third-party providers for functions such as hosting, database and authentication, payments, email, monitoring, AI assistance, and bank connectivity. These providers process data only for their specific service function. Our public Privacy Policy lists current sub-processors and explains the categories of information handled by each provider.

4. Access Control

Access to production systems, databases, deployment tools, and administrative platforms is limited to authorized personnel with a business need. Administrative access is reviewed periodically and removed when no longer required.

Application data access is scoped by authentication and authorization controls, including database row-level security where applicable. Service-role database access is restricted to server-side routes and backend processes.

5. Credential and Secret Handling

Secrets, API keys, database credentials, Plaid access tokens, webhook secrets, and other sensitive credentials are confidential and must not be committed to source code, exposed in logs, sent to client applications, or included in support messages.

Plaid access tokens are stored server-side only and encrypted before storage using application-level authenticated encryption.

6. Encryption

1099 Ops uses encrypted transmission through HTTPS/TLS. Sensitive provider tokens are encrypted before storage, and production secrets are managed through approved infrastructure and deployment environment controls.

7. Secure Development and Change Management

Production changes are managed through source control, CI/CD checks, testing, type checking, linting, schema checks, and deployment review practices. Security-sensitive changes are reviewed for data exposure, authentication and authorization impact, logging behavior, provider scope, secret handling, privacy-policy alignment, and database/schema impact.

8. Logging and Audit Controls

1099 Ops maintains audit logging for sensitive application events and security-relevant operations where appropriate. Sensitive values, including secrets, tokens, credentials, and sensitive provider data, are scrubbed from logs and audit metadata.

9. Incident Response

1099 Ops maintains procedures for identifying, triaging, containing, remediating, and documenting security incidents. Security concerns or vulnerability reports may be sent to security@1099ops.app.

We aim to acknowledge vulnerability reports within two business days and prioritize remediation based on severity and customer impact.

10. Business Continuity and Recovery

1099 Ops maintains operational runbooks for production recovery, deployment recovery, database availability, and incident response coordination. Our infrastructure providers maintain underlying availability, redundancy, backup, and disaster-recovery controls.

11. Continuous Improvement

Security is treated as a continuously maturing program. Policies, procedures, and controls are updated as product functionality, infrastructure, integrations, provider requirements, customer needs, and risk profiles change.

12. Contact

For security questions or vulnerability reports, contact security@1099ops.app. For privacy or support requests, contact support@1099ops.app.