

Your financial data. Handled with care.

GreenFlow connects to QuickBooks Online to help your business forecast cash flow. Here is how we protect that connection, keep business data separate, and give you control over your information.

Your QuickBooks records stay unchanged

GreenFlow reads accounting data to build forecasts. Its integration does not create, edit, or delete entries in QuickBooks. You connect through Intuit's own authorization screen, so GreenFlow never sees or stores your QuickBooks password.

Each business has its own access controls

GreenFlow checks which businesses a user is allowed to access. Database-level rules add another layer of protection by limiting the records the application can retrieve for each business. The application's database account is configured so it cannot bypass those rules.

Sign-in has an extra layer of protection

Your account requires an additional verification step beyond your password, helping protect access even if your password is compromised. Sign-in is handled by a dedicated identity service, and GreenFlow does not store your login password. Access is assigned by business and role, so viewing a forecast does not automatically grant permission to change settings or manage connections.

Data is encrypted and backed up

GreenFlow is hosted on Amazon Web Services in the United States. Browser and database connections are encrypted, as are the database and its backups. The database is not publicly accessible. Automated backups support recovery within a 14-day retention window.

Security information as of October 14, 2026. This overview describes the controls reported in GreenFlow's security materials; it is not an independent audit or a guarantee against every security incident.

Your connection. Your choice.

You can stop the QuickBooks connection and request deletion of your business's data.

Disconnect whenever you choose

You can disconnect QuickBooks from inside GreenFlow, which revokes the connection with Intuit and removes the active connection credentials. You can also revoke GreenFlow's access through your Intuit account. Disconnecting stops future access; it does not by itself delete data already imported.

Request deletion from inside GreenFlow

A business owner can request deletion. The business is disconnected and hidden immediately, followed by a 30-day recovery window in case the request was a mistake. After that window, GreenFlow purges the business's application records, reporting data, synchronized files, and connection credentials.

Encrypted database backups expire on the separate 14-day retention cycle. Billing records and a de-identified audit trail are retained for legal and financial recordkeeping.

Where we stand on independent assurance

A formal SOC 2 audit is on GreenFlow's roadmap. GreenFlow has not yet completed that audit. This overview is a description of current safeguards, not a SOC 2 or SOC 3 report.

Questions are welcome

Contact info@greenflowforecast.com with security questions or to report a suspected issue. We can walk through the safeguards described here with you or your IT advisor.

Security controls

Implementation details for your IT team. Controls described in GreenFlow security materials as of October 14, 2026.

CONTROL	IMPLEMENTATION
Data isolation	PostgreSQL row-level security across application, raw, and reporting schemas: 97 tenant tables, 286 policies. Application role: NOSUPERUSER, NOBYPASSRLS; owns no tables.
Request scope & roles	Transaction-scoped business and user context; reapplied after commit or rollback. Missing context returns no rows. Per-business capabilities checked before client-scoped queries.
Authentication	Clerk-managed identity; MFA required for all users. Short-lived RS256 JWTs verified against JWKS, with issuer, subject, issued-at and expiry checks. Invitations expire after 7 days.
QuickBooks integration	OAuth 2.0; accounting scope only. Accounting data requests use HTTP GET. POST requests are limited to OAuth token exchange, refresh and revocation. Single-use OAuth state expires after 10 minutes.
Credentials	AWS Secrets Manager with KMS encryption. One QuickBooks token secret per business; separate application credentials. Tokens stored outside source code and the application database.
Hosting & network	AWS us-east-1. RDS PostgreSQL 16: not publicly accessible; port 5432 restricted to internal ranges. ECS Fargate and Lambda in private subnets, without public IPs; outbound traffic via NAT.
Encryption	CloudFront: HTTPS redirect and minimum TLSv1.2_2021. Database requires SSL. RDS and backups encrypted with KMS; S3 default encryption and all four Block Public Access settings enabled.
Recovery	Automated RDS backups with 14-day point-in-time recovery retention. Database deletion protection enabled.
Logging & detection	Multi-region CloudTrail with log-file validation; GuardDuty active. 13 CloudWatch alarms notify operations through SNS. Key application changes record actor, business, time and before/after values.
Data integrity	Nightly synchronization and post-load comparison of bank and cash balances with QuickBooks; \$0.01 alert threshold. Exports include actuals and books freshness dates.
Development & releases	Approximately 4,500 automated tests; required secret scan; weekly dependency checks. Protected branches and SHA-pinned workflow actions. Release tags deploy immutable image digests with a rollback anchor.
Data lifecycle	Owner-initiated deletion: immediate disconnect and hiding, 30-day recovery window, then purge of business records, files and credentials. Backups expire on a 14-day cycle; billing records and a de-identified audit trail retained.
Service providers	AWS: hosting and storage. Intuit: accounting connection. Clerk: identity. Stripe: billing; GreenFlow stores no card numbers. GitHub: code and releases.
AI processing	Anthropic interprets free-text planning notes. Note text is sent for processing; ledger records, vendor lists and balances are not included separately. Information entered in a note is part of that text.
Independent assurance	Formal SOC 2 audit planned; not yet completed. This overview is not a SOC 2 or SOC 3 report.