Taxable

POSTMAC VENTURES PRIVATE LIMITED

SECURITY STATEMENT

This document states what Taxable does to protect your books, and what we ask of you.

Document	Security Statement
Version	2.3
Effective date	24 November 2026
Operated by	Postmac Ventures Private Limited
Registered office	3rd Floor, Orchid Center, Golf Course Road, Sector-53, Gurugram, Haryana – 122002
CIN	U66190HR2025PTC129138
GSTIN	06AAPCP5039G1Z7
Governing law	Laws of India; courts at Gurugram

CONTENTS

1. Definitions and interpretation
2. How we think about security
3. Where Taxable runs
4. Encryption and secrets
5. Signing in
6. Sessions and devices
7. Who can see what
8. Approvals and AI assistants
9. The Tally connector
10. Records, logs and locks
11. Backups and recovery
12. How Taxable is built
13. Our people and your documents
14. Why the signature is not ours
15. If something goes wrong
16. What you can do
17. What we do not claim

Schedule 1: Controls at a glance
Schedule 2: Lifetimes
Schedule 3: Roles
Schedule 4: If there is an incident

1. DEFINITIONS AND INTERPRETATION

1.1 In this statement the following words have the meanings given to them below.

1.2 **"Assistant"** means an AI assistant, built into Taxable or connected by a User, such as Claude, ChatGPT or Gemini.

1.3 **"Company"** means a business whose books are kept in Taxable.

1.4 **"Connector"** means the program that links Tally to Taxable: the Taxable Tally Connector for Windows or Connector Lite.

1.5 **"Customer Data"** means everything you put into Taxable or sync from Tally.

1.6 **"Prepared change"** means a change to the books that an Assistant has proposed and that waits for a person to approve it.

1.7 **"Session"** means the period during which a browser or app stays signed in after you sign in.

1.8 **"User"** means a person who signs in to Taxable.

2. HOW WE THINK ABOUT SECURITY

2.1 Your books are your business, and keeping them safe is part of the product, not an add-on. This page says plainly what Taxable does, how it is built to limit harm when something goes wrong, and what we ask of you.

2.2 We follow a few simple rules: give each person and each assistant the least access they need, make every change visible, put a human approval in front of anything an AI prepares, and keep the moving parts few so that there is less to attack.

2.3 We describe what exists today. Where something is not in place, we say so, because a security page that only lists strengths is not worth reading.

2.4 Security is shared. We look after the platform, the code and the way access is checked. You look after who you give access to, how you keep your passwords, and what you approve. This page explains both halves.

2.5 We build on the services of Google Cloud, which provides the data centres, the network and the managed database and storage. We rely on Google’s security for those layers and add our own controls above them.

2.6 Words with capital letters have the meaning given in the definitions at the start. The schedules at the end summarise the controls, the lifetimes of tokens and links, the roles and the steps we follow in an incident.

3. WHERE TAXABLE RUNS

3.1 The Taxable application and its database run in Google Cloud’s Mumbai region (asia-south1), in a project that we control. We use Google Cloud’s managed services, so the physical security of the data centres and the platform underneath is Google’s, to the standard Google publishes.

3.2 Files and backups are kept in Google Cloud Storage in the same project. Nothing is stored on a laptop or a desktop in an office, and the desktop apps keep your books in your account in the cloud, not on the computer.

3.3 The websites are static pages delivered over HTTPS through Google’s hosting network. They load no scripts, fonts or trackers from other companies, and they are sent with a strict content security policy, a ban on being framed, and a policy of sending no more of the page address to other sites than is needed.

3.4 The application runs as a managed service that restarts itself if it fails, and we run one copy in a single region so that the data is in one place. Because there is one copy of the running program, limits such as rate limits are exact, not approximate.

3.5 Changes to the live service are made by releasing a new version through our deployment process. We do not edit the live service by hand.

3.6 The desktop applications for Windows and Mac are your books in a window: they show what is in your account and do not keep a second copy of your books on the computer.

4. ENCRYPTION AND SECRETS

4.1 Every connection to Taxable uses HTTPS, and the sites tell browsers to use only HTTPS in future (HSTS). Data you send to Taxable is encrypted in transit.

4.2 Data stored in Google Cloud’s database, storage and backups is encrypted at rest by Google by default. Credentials that you save in Taxable for other services are additionally encrypted by Taxable before they are stored.

4.3 Passwords are never stored. Each one is stored only as a salted scrypt hash, a slow function chosen so that guessing is expensive, and it is compared in a way that does not reveal how close a guess was. Sign-in tokens, pairing codes and one-time links are stored only as hashes.

4.4 The keys and passwords that Taxable itself needs are kept in Google Secret Manager, not in the code, and are given to the running service only when it starts.

4.5 Passwords, tokens and pairing codes are protected so that even someone with access to the database cannot read them back. A password is not stored; a token is stored only as a hash and compared with the hash of what is presented.

4.6 The keys that protect the credentials you save are not stored beside the data they protect. They are held as secrets of the running service.

5. SIGNING IN

5.1 You can sign in with an email and password, or with Google. An email address can be verified before an account is created, so that nobody can open an account in your name by using your address.

5.2 Repeated wrong passwords are stopped: after eight wrong attempts for an email in fifteen minutes that account is locked for the rest of the window, whoever is trying, and attempts from one address are limited as well. Sign-up, password reset, pairing and assistant sign-in are rate limited in the same way.

5.3 A password reset link works once and expires in an hour. Using it signs out every other session of that person. The reset form gives the same answer whether or not an address has an account, so it cannot be used to find out who is a customer.

5.4 We do not offer two-step verification inside Taxable at present. If you sign in with Google, you can use Google’s own two-step verification to protect your Taxable access, and we recommend that you do.

5.5 When you sign in with Google, Google tells Taxable who you are, and Taxable never sees your Google password. Taxable checks the identity token that Google sends before it trusts it.

5.6 We never ask you for your password by email, by phone or in a message, and neither does our support. If you receive a message that asks for it, it is not from us.

6. SESSIONS AND DEVICES

6.1 When you sign in, Taxable gives your browser a session cookie that cannot be read by scripts on the page (HttpOnly), is sent only over HTTPS (Secure), and is not sent on requests started by other sites (SameSite=Lax). It lasts up to 30 days, and a signed-out or expired session is rejected.

6.2 You can sign out of the browser you are using, or sign out of every other device at once. The second also ends the sign-in of any assistant you connected through a connector, so a lost or shared computer can be shut off quickly.

6.3 A sign-in at one of our front doors opens only that product’s companies: the Tally connector product and the full accounting software have separate sign-in addresses, and a session of one is not accepted by the other.

6.4 A session is tied to a browser. If you sign in on another computer, that is a separate session, and you can end it from the first computer by signing out of every other device.

6.5 On a shared computer, use a private window or sign out when you finish, because a signed-in browser can act as you until the session ends.

7. WHO CAN SEE WHAT

7.1 Access inside a company is set by role, and by branch (Schedule 2 lists the roles). An owner invites people by email with a role, and may limit a person to the branches they should see. Each person sees only what their role allows, and inviting people or changing roles is itself a permission that not every role has.

7.2 There are no shared logins. Everyone has their own, so that the activity log says who did what, and you can remove a person at once when they leave.

7.3 An employee’s login opens only the employee portal, where they can see their own attendance, leave, payslips and declarations, and nothing else in the company.

7.4 Our own staff cannot see your books by default. Platform staff roles are limited, and a staff member who opens a company for support does so in a read-only mode that changes nothing and that cannot make entries or approve anything. If you never engage our services, nobody at Taxable looks at your books.

7.5 If you engage us for expert work, our access is scoped to the engagement and the people who work on it, and ends when it does. Documents are kept only as long as the engagement and the law require.

7.6 Access is checked on the server for every request, not only hidden in the screen. A person who types an address that their role does not allow, or calls the interface directly, is refused.

7.7 The roles are listed in Schedule 3. An Owner can change a person’s role or remove them at any time, and the change applies at once to every device that person is signed in on.

7.8 A Company on the Connect Tally with AI plan can use only the connector, the connection for Assistants, approvals, and billing and profile. That limit is checked on the server, so it does not depend on the menu.

7.9 A person who manages the books of several Companies as a Practice sees only the Companies that have been added to that Practice, and each client’s Company stays the client’s.

8. APPROVALS AND AI ASSISTANTS

8.1 Taxable’s assistant and the assistants you connect work as the person who asked, with that person’s role and branch access. They cannot see or do more than the person could. An assistant without a write tool cannot propose a change at all.

8.2 Anything an assistant prepares waits in Taxable as a proposal. It becomes an entry only when a person with the right role approves it, and the approval step is enforced by Taxable’s own code, not by the assistant’s good behaviour. A proposal that is not approved within an hour expires.

8.3 Assistants connect with OAuth, with PKCE required, so that Taxable never gives out a password and a stolen sign-in code is of no use on its own. Sign-in codes last ten minutes, access tokens one hour, and the renewal token up to thirty days. You can see and revoke every connection from Taxable.

8.4 A company on the Connect Tally with AI plan gives an assistant a smaller set of tools than a full platform company. This is enforced on the server, not only hidden in the menu, and what Taxable does by itself for you once you approve something is not weakened by it.

8.5 We do not train AI models on your books. The AI providers that process a request are independent companies; the privacy policy says what is sent to them and when, and each assistant you connect is a service you choose, under its own terms.

8.6 The tools that an Assistant can use are a fixed list, and each one is checked against the person's role, the Company's plan and the permission given at connection. A tool that reads is separate from a tool that prepares a change, so an Assistant can be given one without the other.

8.7 The text an Assistant reads from your books is data, not instruction. A document or a ledger name that tells the Assistant to ignore its rules does not change what the Assistant is allowed to do, because the rules are in the program and not in the Assistant's text.

8.8 The prepared change shows what it will do, with the amounts, parties and dates, and a person with the right role approves or rejects it. Changes that alter or remove existing data are held back from bulk approval, so that they are looked at one by one.

8.9 You can see every connected Assistant, when it was last used and what it did, and you can revoke it at once. Revoking ends its access and does not remove what you already approved.

8.10 The Assistant that is built into Taxable runs on the server as the signed-in person. It does not have a separate account with more rights.

9. THE TALLY CONNECTOR

9.1 The connector is paired with a code that you create in Taxable and enter once. After pairing it holds a token for that company only, kept on your computer, and you can revoke it from Taxable at any time.

9.2 Writing Taxable entries into Tally is off until you switch it on for a paired computer. When it is on, each entry is created in Tally as a voucher and is marked done only when Tally says it went in, so a failed write is retried, not forgotten.

9.3 The connector tells Taxable which version it is. Taxable refuses very old versions rather than let them write in an old format, and the Tally Management page shows each connector's version and the last time it was seen.

9.4 The connector talks only to Taxable and to the Tally on your own computer or hosting. Its calls go outward to Taxable, so it does not need you to open a port on your network.

9.5 When the connector sends entries into Tally, Taxable keeps each as waiting until Tally confirms it, so a power cut or a closed Tally does not lose an entry or create a second one.

9.6 The connector tells you in its own window what it is doing, and the Tally Management page in Taxable shows each paired computer, its version and when it was last seen. You can pause write-back or revoke the computer from there.

9.7 The connector never needs your Taxable password. It uses a token for one Company, and revoking it stops the connector at once.

10. RECORDS, LOGS AND LOCKS

10.1 Taxable keeps an activity log of who did what, and when, in each company. Approved actions and changes to entries, roles and settings are recorded in it, so that a correction leaves a trail rather than a silent change.

10.2 You can lock a period so that closed months cannot be changed by mistake. A lock applies to everyone in the company, including assistants.

10.3 Server logs record errors and unusual events, for example an error report from the app, which holds the page, the message and the ids of the user and company, not the content of your books. They are used to find and fix faults.

10.4 When someone signs up, the record that they accepted the legal documents is written once, with a SHA-256 hash of the record as it was written, so that a later change to it can be seen. The record holds the time, IP address, approximate location, browser, the versions of the documents and a fingerprint of each text. The person can see it, and it is available to platform staff in read-only form.

10.5 The activity log is part of the product, not a side file. It records who did what and when, and an Owner can read it. People with access to the Company cannot edit the log.

10.6 A lock on a period stops entries dated in that period from being made or changed, by people and by Assistants, until the lock is lifted by someone with the permission to do so, which is itself recorded.

11. BACKUPS AND RECOVERY

11.1 A consistent copy of the database is taken every day, compressed and kept in Google Cloud Storage, and up to thirty daily copies are kept. If something goes wrong with the live data, we can restore from one.

11.2 Backups are used only to restore the service. A company that you ask us to delete disappears from backups as they are replaced, which takes about a month.

11.3 The service runs in a managed, monitored environment that restarts itself if it fails. Because your books are in the cloud, a lost computer does not lose them.

11.4 A backup is a complete, consistent copy of the database. It is taken while the service is running, without stopping it, and compressed before it is stored.

11.5 We restore from a backup if the live data is damaged. We do not restore a single Company on request except in a case we agree with you, because a restore replaces more than one Company’s data.

11.6 You should not rely only on our backups. Export your reports and entries from time to time, and keep your Tally company backups as you do now.

12. HOW TAXABLE IS BUILT

12.1 The server uses no third-party packages: it is our own code on the standard Node.js runtime, which leaves very little outside code to go wrong or to be tampered with. The website loads nothing from other companies.

12.2 Input is validated on the server and the size of a request is limited, database queries use bound parameters rather than text pasted into a query, and the pages are sent with a strict content security policy that allows scripts only from Taxable itself.

12.3 Every release is tested before it goes live, including tests for permissions: that a person without a role cannot reach what the role protects, that a connector company cannot reach the rest of the product through the open API, and that approvals really gate changes.

12.4 Because the server uses no third-party packages, we do not depend on the update cycle of hundreds of other projects, and a flaw in one of them cannot enter through us. The build step that prepares the web app is separate from the server, and its output is checked before release.

12.5 Releases are made from tested code. The tests include checks that a person cannot see another Company’s data, that a role cannot do what it is not allowed to, that approvals are needed, and that the plan limits hold.

12.6 We keep production secrets out of the code and out of the source repository. They are given to the running service as secrets.

13. OUR PEOPLE AND YOUR DOCUMENTS

13.1 The people who work on your engagement see only what that work needs. We hold documents only for the engagement, not as a general archive of your business, and release or destroy them when the engagement and the law no longer require them.

13.2 Documents you upload, such as bills, bank statements and identity documents, are stored in your company's space and are visible only to people in your company who have the role that allows it.

13.3 Where a document is sent to an AI provider for reading, only that document is sent, for that request, as the privacy policy describes, and you review what is read before it is saved.

13.4 We limit who on our side can reach production systems and data, and a person who leaves our team loses that access when they leave.

13.5 We do not read your books to train anything or to look for anything unrelated to helping you. Where we need to look to fix a fault, we look at the least that will do, and in read-only mode.

14. WHY THE SIGNATURE IS NOT OURS

14.1 A statutory audit, a tax audit or a certificate has to be issued by someone independent of the people who kept the books. We keep the books, so it is not ours to sign: independent practising chartered accountants carry out and sign that work, they are named to you before it starts, and they can disagree with us.

15. IF SOMETHING GOES WRONG

15.1 If we find or are told of a security problem that affects your data, we will act quickly to stop it, find out what happened, and tell you without undue delay with what we know, what we have done and what you should do. We will tell the authorities where the law requires it, including the Data Protection Board of India for a personal data breach.

15.2 Found a vulnerability? Please tell us privately before you tell anyone else, through the contact page with "Security" in the subject, and give us enough detail to reproduce it. We will acknowledge it, keep you informed, and not take action against anyone who acts in good faith and does not access more data than needed to show the problem.

15.3 Please do not test against other customers' data, do not disrupt the service, and do not publish a problem before we have had a reasonable time to fix it.

15.4 Schedule 4 sets out the steps we follow. They are in that order because the first thing is to stop harm, and the last is to make sure it cannot happen the same way again.

15.5 We keep a record of every incident and what we changed because of it, and we use it to decide what to test next.

16. WHAT YOU CAN DO

16.1 Use a strong, unique password or Google sign-in, and keep your own email secure, since a password reset goes to it. Give each person their own login and the smallest role that does the job, and remove people when they leave.

16.2 Review who has access and which assistants are connected from time to time, revoke what you no longer use, lock closed periods, and approve prepared entries only after reading them.

16.3 Choose a strong, unique password, or use Google sign-in with two-step verification turned on in your Google account. Do not share a login, and do not enter your password on a page that was reached through a link in a message you did not expect.

16.4 Keep your computer and browser up to date, and be careful with browser extensions, because an extension can read what you see.

16.5 If you think your Account has been misused, sign out of every other device, change your password, review who has access and which Assistants are connected, and tell us.

17. WHAT WE DO NOT CLAIM

17.1 We do not claim ISO 27001, SOC 2 or any other certification on this page, and we do not say that Taxable cannot be breached. No system is perfectly secure. We say what we do, we keep doing it carefully, and we will tell you when we change it.

17.2 We say what is in place and we do not claim more. If we add a control, such as two-step verification inside Taxable, we will say so here, and the date at the top will change.

SCHEDULE 1: CONTROLS AT A GLANCE

Area	What is in place
Hosting	Google Cloud, Mumbai (asia-south1); HTTPS only, with HSTS on the websites
Encryption	TLS in transit; encryption at rest by Google Cloud; stored credentials encrypted by Taxable; passwords stored as salted scrypt hashes; tokens and pairing codes stored as hashes
Sign-in	Email and password, or Google; email verification; lock after eight wrong passwords in fifteen minutes; rate limits on sign-up, reset and pairing; reset links work once for an hour
Sessions	HttpOnly, Secure, SameSite=Lax cookie, up to 30 days; sign out here, or everywhere else
Access control	Roles, branch scoping, invitations by email, no shared logins, an employee login that opens the employee portal only
Assistants	Act as the person who asked, with that role and branch; prepare only; a person approves; prepared changes expire in an hour; OAuth with PKCE; revocable connections
Connector	Paired with a code; a token for one Company; write-back off until you switch it on; version check; calls go outward
Records	Activity log; locks on closed periods; changes leave a trail
Backups	A daily copy of the database, up to thirty kept, in Google Cloud Storage
Website	No scripts, fonts or trackers from other companies; strict content security policy; no framing; no sniffing of content types
Code	The server uses no third-party packages; inputs validated; bound parameters in database queries; tests of permissions before each release

SCHEDULE 2: LIFETIMES

Item	Lasts
Browser session	Up to 30 days, or until you sign out
Sign-up verification link	24 hours, used once
Password-reset link	1 hour, used once; using it signs out other sessions
Assistant sign-in code	10 minutes
Assistant access token	1 hour
Assistant renewal token	Up to 30 days, or until revoked
A prepared change waiting for approval	1 hour
Daily database backup	Up to thirty kept; each is replaced in turn

SCHEDULE 3: ROLES

Access inside a Company is set by role and by branch. The roles are:

Role	Purpose
Owner	Full control of the Company, including billing and deletion.
Admin	Full operational control except billing and deleting the Company.
Cross-Branch Manager	Reads and writes across every branch, without administering members or the Company.
Chartered Accountant	An external accountant who runs the books and compliance for the Owner, without changing billing or deleting the Company.
Branch Admin	Administrative control within the branches assigned.
Branch Manager	Runs the branches assigned day to day, without administering access.
Member	Reads, and creates and updates basic records in the branches assigned.
Employee	The employee portal only: own profile, attendance, leave, payslips and tax. No access to the books.

SCHEDULE 4: IF THERE IS AN INCIDENT

These are the steps we follow when we learn of a security problem that may affect Customer Data.

Step	What we do
1. Contain	Stop the problem: close the hole, revoke the access or the tokens involved, and preserve the evidence.
2. Understand	Find out what happened, what was affected and for how long, using the logs and the activity log.
3. Tell	Tell the people affected without undue delay, and the Data Protection Board of India where the law requires, with what we know, what we have done and what they should do.
4. Fix	Repair the cause, restore from a backup if needed, and add a test so that it cannot come back.
5. Learn	Write down what went wrong and what changed, and tell the people affected the outcome.

End of security statement · Version 2.3 · 24 November 2026