

RECORDS AND DATA LIFECYCLE

Data Retention and Disposal Policy

How themassis retains, deletes, and destroys accounting, reconciliation, and Plaid End User Data — including backups, tokens, and legal holds — with no silent exceptions.

Document	Data Retention and Disposal Policy
Organization	themassis (themassis.com)
Classification	Public — partner and customer diligence
Version	1.0
Effective date	4 September 2026
Next review	On or before 4 September 2027, and after any material change
Owner	Qualified Individual, Information Security
Approved by	Senior management of themassis
Public URL	https://themassis.com/retention
PDF	https://themassis.com/policies/data-retention-and-disposal-policy.pdf
Related	Information Security Policy, Privacy Policy, Terms of Service
Contact	privacy@themassis.com · security@themassis.com · support@themassis.com

This policy exists so that customer financial information is not kept longer than needed, is not kept in backups after it is deleted from production, and is not 'soft-deleted' in a recoverable form unless a closed-list legal hold applies. It is written to satisfy the FTC Safeguards Rule disposal expectations, Plaid MSA proper-disposal of End User Data, NIST SP 800-88 guidelines for media sanitization, and ordinary US recordkeeping for books and tax workpapers.

1. Purpose

themassis retains information only for a documented purpose: to provide the reconciliation service, to keep a reconstructable audit trail of what was posted, to bill, to secure the service, and to meet law. When the purpose ends, we dispose of the information so it cannot be read or reconstructed by an unauthorized person.

This policy answers four questions for every class of data: what we keep, why, how long, and how we destroy it. If a class is not listed, the default is: do not collect; if already collected, delete within 30 days of discovery unless a legal hold applies.

2. Scope

This policy covers all information in production, staging, laptops, tickets, email, exports, logs, backups, and subprocessors. It covers Plaid End User Data, Shopify payout records, QuickBooks tokens and journal workpapers, account data, and operational logs. It applies to employees, contractors, and vendors. Customer copies inside Shopify or QuickBooks are the customer's to retain; disconnecting themassis does not delete the customer's own books at Intuit or Shopify.

3. Principles (no loopholes)

- Purpose limitation. We do not retain data 'because it might be useful later' or for unspecified analytics.
- Data minimization. We collect the least that will match a payout, draft a balanced journal, and operate the account.
- No bank credentials. Bank usernames, passwords, PINs, and MFA codes are never stored, so they have no retention period.
- Closed-list exceptions. The only reasons to keep data past the schedule are listed in Section 8. There is no implied exception for convenience, product research, or model training.
- Deletion means disposal. A status flag of 'deleted' with recoverable ciphertext, files on a shared drive, or an unmanaged laptop copy is not disposal.
- Backups follow production. Deletion from the primary store starts a backup-expiry clock of not more than 90 days.
- Tokens die with the connection. Disconnect or account closure revokes and deletes connection secrets within 24 hours.
- Legal holds freeze, they do not expand. A hold preserves specified records; it does not authorize new collection.
- Customer deletion requests are honored except where Section 8 requires a keep. We explain any refusal in writing.
- Anonymization is not a bypass. We do not convert End User Data into 'anonymous' datasets for reuse unless the Privacy Policy already disclosed that use and the data cannot reasonably be re-identified.

4. Roles

The Qualified Individual owns this policy. Engineering implements deletion jobs, token revocation, and backup expiry. Support accepts deletion and export requests at privacy@themassis.com and authenticates the requester. Accountants and merchants must not download Confidential data onto unmanaged devices; exports they create are their records and should be handled under their own retention program.

5. Retention schedule

Times run from the trigger in the table. 'Account lifetime' means while the themassis account is open and the relevant connection is active. Where two periods could apply, the shorter period applies unless Section 8 requires a keep. Storage is in the United States unless the Privacy Policy states otherwise.

Data class	Trigger / period	Disposal
Bank / card login credentials, OTP, institution session cookies	Never collected. Period = none.	If inadvertently received (paste in a ticket, screenshot), delete from all systems within 24 hours and notify security@themassis.com .
Plaid access_token, item_id, selected account IDs	While the Plaid connection is active. On disconnect, account deletion, or Plaid item error that cannot be repaired: 24 hours.	Call Plaid item/remove (or successor). Then cryptographically delete encrypted token fields. Do not log the token.
Plaid transaction payloads used to match Shopify deposits	90 days after a payout is matched, or 90 days after disconnect, whichever is first. Unmatched transactions: not more than 12 months, then delete unless a legal hold.	Delete from primary store; backup expiry $\leq$ 90 days.
Shopify and QuickBooks OAuth access and refresh tokens	While the connection is active. On disconnect or account deletion: 24 hours.	Revoke at the provider where an API exists. Delete encrypted token fields.
Account email, name, role, password hash, store domain	Account lifetime. After a verified deletion request or closure: 30 days for residual billing/identity, then delete, except Section 8.	Delete user row and session rows. Password hashes are never recovered.

Data class	Trigger / period	Disposal
Shopify payout records, split components, mappings, draft and posted journal entries, exception tasks	Account lifetime so history and the review queue work. After closure: 7 years (books and tax workpapers), unless the customer requests earlier deletion and no Section 8 hold applies.	Secure delete of database rows and files. Posted entries that already exist in QuickBooks remain in the customer's QBO company; we do not remotely wipe Intuit.
Audit log of approve / reject / post / connect / disconnect	7 years from the event, including after account closure, because it proves who changed the books. Personal identifiers in the log are limited to user id / email necessary to identify the actor.	Secure delete at 7 years unless a hold. Not used for marketing.
Auth sessions, CSRF cookies, password-reset tokens, OAuth state	Until expiry (sessions: configured days or 90 if remember; reset tokens: short-lived). Expired rows deleted on sight and by a daily job.	Delete. Reset tokens marked used are deleted within 7 days.
Server and security logs (auth, errors, IP)	90 days. Security-incident logs: 3 years.	Log rotation and overwrite. Secrets filtered before write.
Support email and chat	3 years from last message in the thread, or 30 days after account deletion if the customer requests erasure and no hold.	Delete mailbox copies we control. Do not paste tokens into tickets.
Stripe billing identifiers, invoices, plan status	7 years after the last invoice (tax). Card numbers are not stored by themassis.	Delete our copies; Stripe retains what Stripe is legally required to retain.
Backups of any of the above	Rolling 30 days of backup files. A record deleted from production is purged from backups within 90 days.	Encrypted backups; expired backup media overwritten or cryptographically erased.
Source code, mock/synthetic fixtures	Repository lifetime. Must not contain production End User Data.	If production data is found in git, rotate secrets, purge history or invalidate the secret, treat as an incident.
Marketing site analytics / cookies	As described in the Privacy Policy. Essential cookies last for the session or a stated max-age. We do not run third-party advertising cookies on app.themassis.com.	Expire / delete per cookie policy.

6. Plaid End User Data — special rules

Plaid End User Data is retained only while it is needed to provide the bank-match the customer asked for, to debug a failure of that match, or to meet a Section 8 hold. It is not retained 'to enrich the profile,' to sell insights, or to train models.

On disconnect we revoke the item at Plaid and delete our copies on the 24-hour clock in Section 5. If Plaid notifies us that an item is invalidated, we delete our token copy even if the customer has not clicked disconnect.

We do not store End User Data in analytics tools, error trackers, or support desks unless the field is redacted. If a payload is captured in a debug log by mistake, it is purged within 24 hours and the logging rule is fixed.

7. How we dispose (NIST 800-88 aligned)

Disposal method matches media and classification. Restricted and Confidential data is never put in ordinary trash, an unsanitized disk, or a public GitHub gist.

- Database rows: application-level delete of the record, including encrypted token columns. Soft-delete flags are not used for tokens or End User Data.

- Files and object storage: overwrite or provider-side secure delete; bucket versioning that would resurrect the object is disabled for token-bearing prefixes or is included in the 90-day backup expiry.
- Encryption keys: if a key may have wrapped deleted Restricted data and is no longer needed, it is rotated so old ciphertext cannot be read (crypto-shredding) where that is the designed control.
- Backups: time-expire; do not restore a backup into production for convenience if it would reintroduce deleted End User Data. Restore for disaster recovery is followed by re-application of outstanding deletion requests.
- Laptops and disks: full-disk encryption while in use; on retirement, cryptographic erase or physical destruction. Lost devices are an incident.
- Paper: cross-cut shred or equivalent. Do not photocopy token screens.
- Vendors: contract requires return or destruction of themassis data at end of service, with written confirmation on request.

8. Legal holds and other closed-list exceptions

We may retain a specified record past its schedule only if one of the following applies. The hold is documented (what, why, owner, review date) and is released when the reason ends, after which the ordinary schedule runs.

- A statute, regulation, or court order requires retention (for example, a tax audit, a subpoena, or applicable books-and-records rules).
- A reasonable anticipation of litigation, regulatory inquiry, or a customer dispute about a posted journal, limited to the records that are relevant.
- Investigation of fraud, security incident, or abuse, limited to what is needed for the investigation and any related notice.
- Enforcing our Terms or collecting amounts owed, limited to billing and identity records.
- The customer has an active, written request that we preserve a copy (for example, their CPA asked for a seven-year archive).

A hold is not a license to keep Plaid access_tokens active. If we must preserve historical transaction rows, we still revoke live access at Plaid unless the hold expressly requires continued connection, which would be exceptional and customer-directed.

9. Customer deletion, disconnect, and account closure

A customer may disconnect Shopify, QuickBooks, or Plaid in the product or by writing to support@themassis.com or privacy@themassis.com. Disconnect revokes and deletes tokens on the 24-hour clock and stops new collection. Historical payout and journal workpapers remain for the account-lifetime / 7-year schedule unless the customer also requests erasure.

A verified erasure request will delete account data, tokens, Plaid payloads, and support threads we control, subject to Section 8. We will confirm completion or explain any keep within 30 days of verification (sooner where law requires). We will not require the customer to call a phone number or purchase a plan to exercise deletion.

After closure, we do not use remaining workpapers for any purpose except the keep reason. We do not reactivate a Plaid item without a new Link session and customer intent.

10. Exports and accountant copies

The product can export statements and ledgers for the customer's own books. Once downloaded, that copy is the customer's record. themassis cannot dispose of files on the customer's disk. Accountants acting for a merchant are expected to handle exports under the merchant's retention program and not to store them in personal unsanctioned tools.

11. Verification

Deletion jobs are logged (tenant, class, time, operator or system). The Qualified Individual reviews a sample of disconnects and erasure requests at least quarterly to confirm tokens were revoked and rows were removed. Failures are incidents. Partners with a contractual audit right may review this policy, the schedule, and (under NDA) evidence of a sample deletion.

12. Review and contact

This policy is reviewed at least annually and after a material change in systems, law, or partner contracts (including Plaid). The current version is at <https://themassis.com/retention> and <https://themassis.com/policies/data-retention-and-disposal-policy.pdf>.

Requests: privacy@themassis.com. Incidents: security@themassis.com. Operator: themassis, themassis.com.