INFORMATION SECURITY PROGRAM

Information Security Policy

A written information security program for the themassis accounting and reconciliation platform, including Shopify payout processing, QuickBooks Online journal entries, and Plaid bank-feed connections.

Document	Information Security Policy (Infosec Program)
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/security
PDF	https://themassis.com/policies/information-security-policy.pdf
Related	Privacy Policy, Terms of Service, Data Retention and Disposal Policy
Contact	security@themassis.com (incidents) · privacy@themassis.com · support@themassis.com

This document is the comprehensive written information security program required of themassis as a Plaid client and as a provider that receives customer financial information. It is approved by senior management. It is designed to meet or exceed the control objectives of the AICPA Trust Services Criteria for Security, NIST SP 800-53 / NIST Cybersecurity Framework, and ISO/IEC 27002, and to satisfy the FTC Safeguards Rule (16 CFR Part 314), the Plaid Master Services Agreement information-security and breach-notification clauses, and the Plaid Developer Policy.

1. Purpose and policy statement

themassis operates an accounting and reconciliation service that splits Shopify payouts into their components (gross sales, fees, refunds, shipping, tax, and adjustments), drafts balanced QuickBooks Online journal entries through a clearing account, and holds exceptions for human review. Optionally, a merchant may connect a bank account through Plaid so that Shopify deposits can be matched to the bank feed. Nothing risky posts to the ledger without an authorized accountant's approval.

The purpose of this policy is to protect the confidentiality, integrity, and availability of information themassis owns, manages, or processes — including End User Data received from Plaid, Shopify payout data, QuickBooks connection tokens, account credentials, and journal-entry workpapers — against unauthorized access, use, disclosure, alteration, destruction, or loss.

Senior management commits that security is a precondition of the product, not an afterthought. We will not collect bank login credentials. We will not sell customer data. We will not use customer books to train unrelated models or to advertise. We will notify affected parties, and Plaid, of a Security Breach on the timelines in Section 16. We will dispose of data as required by the Data Retention and Disposal Policy. There is no unwritten exception to these rules.

2. Scope

This policy applies to all themassis systems, personnel, contractors, processes, and subprocessors that collect, process, store, transmit, or dispose of company or customer information, including:

- The themassis web application, API, databases, backups, logs, and supporting infrastructure.
- Shopify, QuickBooks Online, Plaid, Stripe, and email/hosting integrations.
- Laptops, workstations, mobile devices, and cloud consoles used to operate the service.
- Source code, secrets, configuration, and CI/CD pipelines.
- End User Data as defined by Plaid, nonpublic personal information under the Gramm-Leach-Bliley Act, and personal information under applicable privacy laws.
- Paper or exported files (CSV, XLSX, PDF statements) that leave the production system.

It applies to employees, contractors, accountants operating on the platform, and any third party with access to themassis systems. Customer-side QuickBooks companies and Shopify stores remain the customer's systems; this policy governs how themassis connects to them.

3. Roles and responsibilities

Senior management approves this program, provides resources, and is accountable for its effectiveness. A Qualified Individual is designated to oversee, implement, and enforce the program (FTC Safeguards Rule § 314.4(a)). If that function is performed in part by a service provider, themassis retains responsibility and a senior person directs the provider.

Everyone with access to themassis systems must follow this policy, complete security and privacy training before receiving access to customer financial data, report suspected incidents immediately, and use only approved tools.

Merchants may view their own store, connections, payouts, and status. They cannot approve or post journal entries. Accountants may review exceptions, approve or reject drafts, and post to QuickBooks. There is no standing product-admin role with blanket access to all customer ledgers. Support access to a customer's data is granted only for a ticket the customer opened, is time-bounded, is logged, and is revoked when the ticket closes.

4. Risk assessment and governance

themassis maintains a written risk assessment covering reasonably foreseeable internal and external risks to customer information, including unauthorized access to Plaid End User Data, token theft, mis-posting, insider access, vendor failure, ransomware, and insecure disposal. The assessment identifies safeguards for each risk, the residual risk, and the owner.

The assessment is reviewed at least annually, after a Security Breach, after a material system change (new processor, new data type, production Plaid access), and when a law or partner contract so requires. Findings feed the control set in this policy. Controls that cannot be operated as written are treated as incidents, not as silent exceptions.

5. Data classification

All information is classified. Handling requirements follow the highest classification of any field in a record or export.

Class	Examples	Handling
Restricted	Plaid access tokens and item IDs; Shopify and QuickBooks OAuth access and refresh tokens; password hashes; encryption keys; Plaid client secret; Stripe secret keys.	Encrypt at rest and in transit. Store only in the secrets manager or the encrypted connection store. Never log, email, commit, or put in tickets. Access only by production runtime and named operators under break-glass.

Class	Examples	Handling
Confidential — financial	Shopify payout components, bank-deposit amounts, journal lines, chart-of-accounts mappings, exceptions, audit logs of posting, Plaid transaction data used to match deposits.	Encrypt in transit. Restrict by tenant and role. No use for marketing, model training outside the customer's tenant, or resale. Dispose per the retention schedule.
Confidential — personal	Account email, name, store domain, support correspondence, IP addresses in auth logs.	Need-to-know. Disclose only as described in the Privacy Policy. Honor deletion and access requests.
Internal	Architecture notes, non-secret configuration, aggregated operational metrics that cannot identify a customer.	Limit to personnel. Do not publish.
Public	This policy, the Privacy Policy, Terms, marketing site.	May be published. Still change-controlled.

6. Plaid, bank feeds, and End User Data — mandatory rules

These rules are mandatory. They close the gaps Plaid and banking partners treat as deal-breakers. They are not optional product features.

6.1 What we never collect or store

- Bank, credit-union, or card login credentials (username, password, PIN, knowledge-based answers, OTP/MFA codes, session cookies of the financial institution).
- Full payment-card PAN, CVV, or magnetic-stripe data. Card payments for themassis subscriptions are handled by Stripe; themassis does not store card numbers.
- Plaid Link UI in a modified, scraped, or proxied form. Customers authenticate inside Plaid Link / OAuth at the institution.
- End User Data beyond what is required to match Shopify payouts to the connected deposit account and to operate the customer's reconciliation.

6.2 What we may store, and how

After a customer completes Plaid Link, Plaid returns a short-lived public_token. themassis exchanges it server-side for an access_token and item_id. Only those values, plus the Plaid account identifier needed to select the deposit account, are stored — encrypted at rest using authenticated encryption (Fernet, AES-128-CBC with HMAC-SHA256, key derived from the production secret). The Plaid client_id and secret live in the production secrets store, not in source control, not in the browser, and not in application logs.

Plaid transaction data is requested only for the connected deposit account(s) the customer selected, and only in the amount and window needed to match Shopify payouts. We do not pull unrelated accounts (for example credit cards or loans) when the product only needs the payout landing account. We do not retain raw bank-transaction dumps longer than the retention schedule.

6.3 Use limitation

- End User Data is used solely to provide the reconciliation the customer requested, to prevent fraud or abuse of that connection, to comply with law, and to support a customer-initiated ticket.
- We do not sell, rent, or barter End User Data or nonpublic personal information.
- We do not use End User Data for cross-context behavioral advertising.

- We do not disclose End User Data to other merchants, data brokers, or AI training corpora.
- We do not use anonymized End User Data for a secondary purpose unless that purpose is disclosed in the Privacy Policy before the data is used. Default: we do not.
- Employees access End User Data only with a business need. Access is logged.

6.4 Disconnect, revocation, and Plaid item removal

When a customer disconnects Plaid, closes the account, or we terminate the connection for cause, themassis will, within 24 hours: (a) call Plaid's item/remove (or successor) API so the access_token is revoked at Plaid; (b) delete the encrypted access_token, item_id, and cached bank-transaction payloads from the primary store; (c) cease new pulls. Backup copies expire on the backup rotation in the Data Retention and Disposal Policy and are not restored into production except for disaster recovery under legal hold.

6.5 Plaid credentials and Developer Policy

- Plaid Dashboard credentials, client_id, and secret are confidential Account Information. They are not published, committed, or shared except with Authorized Users who have a legitimate need.
- Production Plaid access is used only for the customer application described to Plaid (Shopify payout reconciliation to QuickBooks).
- Security events involving Plaid Account Information or End User Data are reported to security@plaid.com as required in Section 16, and in any event within 12 hours of becoming aware of a Security Breach as defined in the Plaid MSA.

7. Shopify, QuickBooks Online, and other connections

Shopify and QuickBooks Online are connected through OAuth 2.0. Access and refresh tokens are stored encrypted at rest on the customer's Connection row. Tokens are never returned to the browser. Scopes are limited to what the product needs (payout/settlement read on Shopify; chart of accounts and journal entry write on QuickBooks). We do not request unrelated scopes as a convenience.

Journal entries post to QuickBooks only after an authorized accountant approves. Merchants cannot post. This is an access-control control as well as a product rule: unauthorized posting is a security incident.

Customers may disconnect Shopify or QuickBooks at any time. On disconnect or account deletion we revoke tokens with the provider where an API exists and delete stored tokens within 24 hours.

8. Access control

Access is granted on least privilege and need-to-know. Production data is segmented by tenant (user_id). A merchant cannot read another merchant's payouts, tokens, or journals. An accountant sees only assigned clients.

- Authentication is required for all non-public endpoints. Sessions are server-side; the browser holds only an opaque session identifier in an HttpOnly cookie.
- Passwords are stored with scrypt (per-user random salt, constant-time compare). Plaintext passwords are never logged or stored.
- Login is rate-limited. CSRF tokens are required on state-changing requests.
- Session lifetime is finite. Expired sessions are deleted. Logout invalidates the server session.
- Joiner-mover-leaver: access is provisioned on role, reviewed on role change, and revoked the same day on termination or contract end. Shared logins are prohibited.
- Privileged (production console, database, secrets) access uses unique identities, MFA on the cloud/identity provider, and is logged.

- Service accounts are unique per system, minimally scoped, and rotated after personnel changes and at least annually.
- Default deny on administrative APIs. No undocumented back doors.

9. Encryption and key management

Data in transit: all customer and partner HTTP(S) endpoints require TLS 1.2 or higher with a valid certificate from a public CA. Plain HTTP is not accepted for authentication, tokens, or End User Data. Plaid, Shopify, Intuit, and Stripe APIs are called only over TLS.

Data at rest: OAuth and Plaid tokens are encrypted with Fernet (AES and HMAC). Production databases, object storage, and backups are encrypted at rest using the cloud provider's AES-256 (or equivalent) volume/object encryption. Secrets are not stored in source control.

Keys: the application encryption key is derived from a production secret that is unique per environment, stored in the host secrets mechanism, restricted to the runtime and named operators, and rotated when personnel with knowledge of the secret leave, when compromise is suspected, and at least annually. Development and mock modes use separate keys and must not contain production End User Data.

10. Application and network security

The application is designed so that financial posting cannot happen without an authorized human. Input is validated. SQL is parameterized. Secrets are filtered from logs. Error messages shown to users do not include tokens or stack traces.

- Production systems sit in a professionally managed cloud environment. Management ports are not exposed to the public internet.
- Workstations used to access production have full-disk encryption, automatic screen lock, current OS patches, and current anti-malware / EDR.
- Up-to-date antivirus and anti-malware tools are required on endpoints that can reach customer data, as required by the Plaid MSA.
- Dependencies are pinned and reviewed. Known-vulnerable packages are patched on a risk-based SLA: critical within 72 hours of a usable fix, high within 14 days, others on the next scheduled cycle.
- Changes to authentication, encryption, Plaid scopes, or posting authorization require review before production.

11. Logging, monitoring, and audit

themassis logs authentication events, connection create/disconnect, token refresh failures, payout processing, journal approve/reject/post, and privileged access. Logs include time, actor, tenant, and action, and do not include secrets, passwords, or raw tokens.

Audit logs of journal posting and exception resolution are retained for seven years so that a customer or regulator can reconstruct who posted what. Security logs are reviewed on an ongoing basis and after anomalies. Clock time is UTC.

12. Vulnerability management and testing

themassis tracks vulnerabilities in application code, dependencies, and infrastructure. We welcome good-faith reports to security@themassis.com. We do not run a public bug-bounty program as of this version; reports are still investigated.

Before production Plaid access and at least annually thereafter, themassis will obtain an independent penetration test or equivalent third-party security assessment of the customer application, remediate critical and high findings, and retain the executive summary for partner diligence. This policy does not claim SOC 2 or ISO 27001 certification unless a current

report is published at themassis.com/security. If we obtain such a report, this section will be updated with the date and scope.

13. Secure development

Production secrets are not committed. Mock mode is the default for local development and uses synthetic data. Feature work that touches money uses exact decimal arithmetic; journals must balance before they can be marked ready to post.

Pull requests that change authentication, authorization, encryption, Plaid handling, or posting controls require review. Test suites covering authz (merchant cannot post; accountant can) and token encryption are part of the definition of done for those areas.

14. Third parties, subprocessors, and vendors

themassis does not share customer financial data with a vendor unless the vendor is needed to provide the service, is under contract, and is held to security and disposal terms no weaker than this program. Vendors that receive End User Data or tokens are reviewed before onboarding and at least annually.

Party	Role	Data involved
Shopify	Payout source the customer connects	Payout and settlement components; OAuth tokens
Intuit QuickBooks Online	Ledger the customer connects	Chart of accounts; journal entries the accountant posts; OAuth tokens
Plaid	Bank-feed connection the customer opts into	Link session; access_token / item_id; selected-account transactions
Stripe	Subscription billing	Customer email, plan, Stripe customer/subscription IDs. Card data stays with Stripe.
Cloud infrastructure / email	Host the app, database, backups, and transactional email	Application data and logs under this policy

A current subprocessor list is maintained with the Privacy Policy. Adding a subprocessor that will receive End User Data or tokens requires a written security review and, where contractually required, customer or Plaid notice. themassis remains responsible for subprocessors.

15. Personnel, physical, and acceptable use

Personnel with access to Confidential or Restricted data are bound by confidentiality, trained before access, and removed on the day they leave. Production access from public shared computers is prohibited. Customer data is not copied to personal email, unsanctioned cloud drives, or AI tools that are not an approved subprocessor.

Physical security of production is provided by the cloud data-center operator (badge access, cameras, environmental controls). Office and home workstations that can reach production must lock automatically, encrypt disks, and not leave printed financial exports unattended. Paper with Confidential data is shredded (cross-cut or equivalent).

Use of themassis systems to access another merchant's data, to scrape Plaid or bank properties, or to reverse-engineer connection flows beyond ordinary use, is forbidden and is a Security Incident.

16. Incident response and Security Breach notification

A Security Incident is any attempted or successful unauthorized access, use, disclosure, modification, or destruction of themassis information or systems, or any event that reasonably could lead to that result (lost laptop with production keys, exposed secret in a repository, misdirected export, ransomware).

A Security Breach (for Plaid and customer notice) is a Security Incident that results in, or is reasonably likely to have resulted in, unauthorized access to or acquisition of End User Data, tokens, or other Confidential or Restricted customer information.

16.1 Internal response

- Anyone who suspects an incident reports it immediately to security@themassis.com and does not attempt to conceal it.
- The Qualified Individual (or delegate) triages within one hour of becoming aware during business hours, and as soon as practicable otherwise, not to exceed 12 hours.
- Containment first: rotate secrets, revoke sessions and tokens, disable compromised accounts, isolate systems.
- Preserve evidence (logs, timestamps) before rebuilding.
- Eradicate, recover, write a post-incident report, and feed lessons into the risk assessment.

16.2 Plaid — 12 hour obligation

Upon becoming aware of a Security Breach involving Plaid Account Information or End User Data, themassis will notify Plaid promptly and in no event more than 12 hours later, at security@plaid.com (or any successor address Plaid publishes), with all known facts, the types of End Users affected, what data was involved, containment steps, and any other information Plaid reasonably requests. This timeline is not extended by weekends, incomplete facts, or internal debate. If facts are incomplete, we notify with what we know and update.

16.3 Customers, regulators, and others

Affected customers are notified without unreasonable delay, and in any case within the period required by applicable law (including state breach statutes and, where it applies, the FTC Safeguards Rule). Notice describes what happened, what data was involved, what we are doing, and what the customer should do (for example, disconnect and reconnect Plaid, rotate QBO connections). We will not require a customer to waive claims as a condition of notice.

17. Business continuity and backups

Production data is backed up on a rolling schedule. Backups are encrypted, access-restricted, and tested for restore at least annually. Backups are not an alternate copy of data that escapes the retention schedule: deleted customer data expires from backups within 90 days unless a legal hold applies. Disaster recovery prioritizes integrity of ledgers (no unbalanced journals on restore) and revocation of tokens if keys may have been exposed.

18. Data retention and disposal

Collection is minimized. Retention is purpose-limited. Disposal is secure. The Data Retention and Disposal Policy is part of this program and is incorporated by reference. It specifies schedules, NIST 800-88-aligned destruction, backup purge, legal holds as a closed list of exceptions, and Plaid item removal. Informal 'keep it just in case' retention is a policy violation.

19. Customer and accountant responsibilities

Security is shared. Customers and their accountants must: keep their themassis credentials secret; enable unique users rather than shared logins; connect only stores and books they are authorized to operate; review every draft before posting; disconnect integrations they no longer need; and tell us promptly at security@themassis.com if they believe an account or connection is compromised. themassis is not a licensed CPA firm by virtue of providing software; posting remains a human decision.

20. Exceptions, enforcement, and review

Exceptions to this policy require written approval from the Qualified Individual, a stated duration, compensating controls, and a record. There is no standing exception for Plaid credential storage, for selling data, for skipping breach notice, or for indefinite retention.

Violations may result in removal of access, contract termination, and referral to law enforcement. This policy is reviewed at least annually and after material change. The current version is published at https://themassis.com/security and as a PDF at https://themassis.com/policies/information-security-policy.pdf. Prior versions are retained for seven years.

21. Contact

Security incidents and vulnerability reports: security@themassis.com. Privacy and deletion: privacy@themassis.com. Product support: support@themassis.com. Plaid security notice address (for our notices to Plaid): security@plaid.com.

Controller / operator: themassis, themassis.com.