

HotSaus Information Security Policy

See also the HotSaus Data Retention and Disposal Policy (Part B).

Company	HotSaus, LLC (Atlanta, Georgia, United States)
Document owner	Security Lead: Bam Faboyede
Approved by	Kelechi Ajayi, Legal Advisor
Version	1.2
Effective date	October 29, 2026
Review cycle	At least once every 12 months, and after any material change to systems, vendors, or law
Contact	aye@ayehotsaus.com

Part A: Information Security Policy

1. Purpose

This policy sets the controls HotSaus uses to protect the confidentiality, integrity, and availability of the data it handles, including consumer financial data received through Plaid. It is the governing document for how HotSaus personnel, contractors, and systems collect, store, use, share, and dispose of that data.

2. Scope

This policy applies to:

- All HotSaus personnel, contractors, and anyone granted access to HotSaus systems ("Personnel").
- All production and non-production systems that store or process HotSaus data, including the web application (app.ayehotsaus.com), the backend API, cloud infrastructure, third-party service accounts, source code repositories, and the devices used to access them.
- All data HotSaus collects from users, businesses, and service providers, in any form.

3. Roles and Responsibilities

Role	Responsibilities
Security Lead	Owns this policy. Approves access to Restricted data, runs access reviews, leads incident response, maintains the vendor list, and signs off on exceptions.
Engineering	Implements the technical controls in this policy, reviews code changes for security, and reports suspected incidents immediately.
Admin users	Use the HotSaus admin console only for the business task at hand, and never export or copy user data outside approved systems.
All Personnel	Follow this policy, complete security training, protect their credentials and devices, and report suspected incidents to the Security Lead.

4. Systems and Service Providers

HotSaus runs on managed cloud services. HotSaus does not operate its own data centers or physical servers.

System	Purpose	Data handled
Vercel	Hosts the web application and backend API	Application traffic, server logs
Google Firebase (Authentication, Cloud Firestore)	User accounts and primary application database	Account credentials (managed by Firebase), profiles, claims, ledger, Plaid item records
Plaid	Bank account linking and transaction retrieval	Bank account metadata and transactions, with user consent
Stripe	Subscription and business billing	Payment data (card data is held by Stripe; HotSaus never receives full card numbers)
Wasabi (S3-compatible object storage)	Receipt, proof-of-purchase, and profile images	Uploaded images and PDFs
Amazon Web Services (managed MySQL)	Legacy application data	Legacy deal and search data
Resend	Transactional and marketing email	Name and email address
PostHog, Meta	Product analytics and ad measurement	Usage events, hashed identifiers
GitHub	Source code and change history	Source code (no production data or secrets)

The Security Lead keeps this list current. A new service that will receive Confidential or Restricted data requires the review in Section 13 before use.

5. Data Classification

Class	Definition	Examples
Restricted	Data whose exposure could cause direct financial harm or account takeover	Plaid access tokens, bank transaction data, API keys and service secrets, service account credentials, Stripe secrets
Confidential	Personal information about users or businesses	Names, email addresses, phone numbers, payment handles (Cash App, Zelle, Venmo), receipt and proof-of-purchase images, cashout and ledger records
Internal	Non-public business information	Source code, admin reports, aggregate metrics
Public	Approved for public release	Marketing site content, published offers

Restricted and Confidential data must only be stored in the systems listed in Section 4, and must never be placed in source code, tickets, chat messages, email, personal storage, or spreadsheets.

6. Access Control

1. **Least privilege.** Personnel receive only the access their role requires. Production database and infrastructure access is limited to engineering Personnel who need it.
2. **Unique accounts.** Every person uses their own named account on every system. Shared logins are prohibited.
3. **Multi-factor authentication (MFA).** MFA is required on every administrative account for Google Cloud and Firebase, Vercel, GitHub, Plaid Dashboard, Stripe, Wasabi, AWS, Resend, and the domain registrar and DNS provider.
4. **Application authentication.** Every API request that reads or changes user data must carry a verified Firebase ID token, and the server must confirm that the caller owns the record or holds the admin role. Authorization is enforced on the server; client-side checks are for display only.
5. **Admin role.** The admin role in the HotSaus application is granted only by the Security Lead, and is recorded on the user profile. Admin actions that delete accounts record the acting admin.
6. **Automated jobs.** Scheduled jobs authenticate with a dedicated shared secret sent in a request header, stored as an environment secret, and rotated at least annually or immediately if exposed.
7. **Access reviews.** The Security Lead reviews all infrastructure accounts and all application admin accounts every quarter, and removes access that is no longer needed.
8. **Offboarding.** When a person leaves or changes role, their access is removed within one business day, and any shared secrets they could see are rotated.

7. Secrets Management

1. Production secrets (Plaid client secret, Stripe keys, Firebase service account, storage keys, cron secrets) are stored only as encrypted environment variables in the hosting provider.
2. Secrets are never committed to source control. Local `.env` files and service account files are excluded by `.gitignore`.
3. Sandbox and production use separate credentials. Production Plaid credentials are never used in local development.
4. Any secret that is exposed, or suspected to be exposed, is rotated immediately and the event is handled under Section 14.

8. Encryption

1. **In transit.** All traffic between users, HotSaus, and service providers uses HTTPS with TLS 1.2 or higher. Plain HTTP is redirected to HTTPS. The backend accepts browser requests only from HotSaus origins (CORS allowlist).
2. **At rest.** All data stores used by HotSaus encrypt data at rest with AES-256 or an equivalent standard, provided by the service (Firestore, Wasabi, AWS, Stripe, Plaid).
3. **Restricted fields.** Plaid access tokens are held only on the server, are never returned to a browser or mobile client, and are never written to logs.

9. Plaid and Consumer Financial Data

1. **Consent.** Users connect a bank only through Plaid Link, which presents Plaid's disclosures and obtains the user's consent before any data is shared with HotSaus. HotSaus never sees or stores the user's bank login credentials.
2. **Purpose limitation.** Bank data is used only to find the user's own Zelle, Cash App, and Venmo payments and let the user turn selected payments into cashback claims. It is not sold, not shared for advertising, and not used for credit decisions.
3. **Minimum product scope.** HotSaus requests only the Plaid Transactions product, US institutions only.
4. **Data minimization.** HotSaus stores the account name, type, and last four digits (mask). It does not store full account or routing numbers. Transactions retrieved during a scan are processed in memory; only transactions identified as peer-to-peer payments are saved.
5. **Feature access.** Bank linking is available only to eligible members as controlled from the admin console. Any user can view and unlink their connected banks at any time.
6. **Unlinking.** When a user unlinks a bank, HotSaus calls Plaid's item removal endpoint to revoke access and deletes the stored access token.
7. **Plaid policies.** HotSaus complies with its agreement with Plaid and Plaid's developer policies, and notifies Plaid of any incident affecting Plaid data as Section 14 requires.

10. Secure Development

1. All code changes go through version control on GitHub. Changes to authentication, authorization, payments, or Plaid handling require review before deployment.
2. Every new or changed API route must enforce authentication and ownership checks as described in Section 6.4.
3. Request input is validated against typed schemas on the server.
4. New features that touch Restricted data are tested in the Plaid sandbox, or an equivalent non-production environment, before release.
5. Production data is not copied into development or test environments.

11. Vulnerability and Patch Management

1. Dependencies are monitored with automated vulnerability alerts (for example GitHub Dependabot and `npm audit`).
2. Remediation targets from the date a vulnerability is known: Critical within 7 days, High within 30 days, Medium and Low in the normal release cycle.
3. Hosting, database, and storage infrastructure are managed services patched by their providers.
4. The Security Lead runs a review of authentication and authorization on all API routes at least annually and before each production Plaid launch.

12. Logging and Monitoring

1. The hosting platform records application and access logs. Logs are reviewed when investigating errors or suspected incidents.
2. Logs must not contain passwords, ID tokens, Plaid access tokens, API secrets, full bank transaction details, or payment card data.
3. Automated jobs send completion and failure alerts to the engineering notification channel.

13. Vendor Management

1. Before a vendor receives Confidential or Restricted data, the Security Lead confirms the vendor maintains an independent security attestation (such as SOC 2 Type II or ISO 27001) or an equivalent written security commitment, and that the contract restricts the vendor's use of the data.
2. Vendor attestations are reviewed annually.
3. When a vendor is retired, HotSaus deletes its data from that vendor and revokes all credentials.

14. Incident Response

A security incident is any actual or suspected unauthorized access to, use of, or loss of HotSaus data or systems.

1. **Report.** Anyone who suspects an incident reports it to the Security Lead immediately at aye@ayehotsaus.com.
2. **Contain.** Revoke exposed credentials, rotate secrets, disable affected accounts or features, and preserve logs.
3. **Assess.** Determine what data and which users are affected, and how.
4. **Notify.** Notify affected users and regulators as required by applicable state and federal law. Notify Plaid without undue delay, and within any period its agreement requires, when Plaid data or credentials may be affected. Notify other affected vendors under their agreements.
5. **Recover and review.** Restore normal operation, fix the root cause, and write a post-incident review within 10 business days.

15. Business Continuity

1. Production data lives in managed, replicated cloud services.
2. HotSaus maintains backups or point-in-time recovery for its primary database, and tests a restore at least annually.
3. Backups are encrypted and subject to the retention limits in the Data Retention and Disposal Policy.

16. Personnel and Devices

1. Personnel sign a confidentiality agreement before receiving access to Confidential or Restricted data.
2. Personnel complete security awareness training at onboarding and annually, covering phishing, credential handling, and incident reporting.
3. Devices used to access HotSaus systems must have full-disk encryption, a screen lock, current operating system updates, and a password or biometric login. Lost or stolen devices are reported immediately so access can be revoked.

Part B: Data Retention and Disposal

17. Data Retention and Disposal Policy

How long HotSaus keeps each kind of data, how it is disposed of, and what happens when an account is deleted are set by the separate **HotSaus Data Retention and Disposal Policy**, which forms part of this policy. In summary:

1. Raw bank transactions are never stored, and bank connections are revoked at Plaid when a user unlinks a bank or deletes their account.
2. Users can delete their account in the app or by email. Deletion removes the login, profile, content, bank connections, subscription, and marketing contact; financial records are kept for 7 years

under a legal exception.

3. A daily job enforces the retention schedule and reports its results to engineering.

Part C: Administration

18. Exceptions

Exceptions to this policy require written approval from the Security Lead, a stated reason, compensating controls, and an expiry date no longer than 12 months.

19. Enforcement

Violations of this policy may result in loss of access and disciplinary action up to termination of employment or contract.

20. Related Documents

- HotSaus Data Retention and Disposal Policy
- HotSaus Privacy Policy (</legal/privacy>)
- HotSaus Terms of Service (</legal/terms>)

21. Revision History

Version	Date	Author	Change
1.0	October 15, 2026	Engineering	Initial draft for legal review
1.1	October 19, 2026	Engineering	Part B moved to the standalone Data Retention and Disposal Policy
1.2	October 29, 2026	Bam Faboyede	Approved by Kelechi Ajayi, Legal Advisor, and published