TRUST CENTER

Information Security Policy

This policy defines how TrendHog protects the systems, credentials, and data used to provide its TikTok Shop intelligence service.

EFFECTIVE

August 11, 2026

VERSION

1.1

OPERATOR

ChessReps LLC

1. Purpose and scope

This policy establishes the information security practices for TrendHog, a service operated by ChessReps LLC. It applies to TrendHog's production application, development environments, source code, cloud services, data stores, integrations, and the people authorized to administer them.

Our objective is to protect the confidentiality, integrity, and availability of information while collecting only the data needed to operate the service.

2. Security responsibility

The managing member of ChessReps LLC is responsible for this security program, approving access, coordinating incident response, and reviewing this policy. Anyone given administrative or contractor access must follow this policy and report suspected security events promptly.

TrendHog follows a shared-responsibility model with its infrastructure providers. Providers secure their managed platforms; TrendHog remains responsible for application code, configuration, credentials, authorized access, and appropriate use of data.

3. Data classification, protection, and minimization

TrendHog classifies information according to its sensitivity and the harm that unauthorized access or disclosure could cause:

- **Public:** information approved for public release, including published website content and public product information.
- **Internal:** nonpublic operational information intended only for authorized maintainers and service providers with a business need.
- **Confidential:** personal data, account information, support content, and nonpublic business records. Access is limited according to least privilege.
- **Restricted:** authorization tokens, API keys, passwords, private signing material, and other credentials. These values receive the strongest access restrictions and must remain server-side.

Confidential and Restricted information is treated as sensitive data. Sensitive data is encrypted in transit using HTTPS and at rest through the encryption controls supplied by TrendHog's managed hosting and database providers.

- TrendHog limits collection and retention to information needed for defined product, security, billing, and support purposes.
- TikTok Shop data and authorization credentials are used only for approved TrendHog functions and applicable API scopes.
- Sensitive values are excluded from client-side code, public logs, source control, and user-facing error messages.

4. Access control and secret management

TrendHog grants production and administrative access only to authorized maintainers with a business need. Access is managed through individual cloud-provider and source-control accounts. Privileged access is reviewed when responsibilities change and at least annually.

- Application secrets are stored in managed server-side environment settings.
- Database service credentials and integration secrets are never intentionally delivered to browsers.
- Internal ingestion and webhook endpoints require secret or signature verification.
- Credentials are revoked or rotated after suspected exposure, loss of access need, or a relevant security incident.

5. Infrastructure and network security

Production is hosted on Vercel, and application data is hosted separately on Supabase. Private development environments are kept separate from production. Logical isolation, authenticated service boundaries, and narrowly scoped credentials limit access between systems.

Vercel terminates HTTPS and places production traffic behind its platform firewall and automatic distributed denial-of-service protections. Supabase provides managed database security controls. TrendHog configures application authorization and protects privileged server operations within those managed environments.

6. Secure development and vulnerability management

- Source changes are tracked in version control and validated with static checks and production builds before release.
- Dependencies are pinned through a lockfile and reviewed for relevant security updates.
- Security-sensitive changes receive focused review of authentication, authorization, input handling, secret exposure, and failure behavior.
- Known vulnerabilities are assessed according to exploitability and potential impact, then remediated on a risk-based schedule.

7. Logging and monitoring

TrendHog uses application and cloud-provider logs to diagnose failures and investigate suspicious activity. Vercel's platform firewall continuously evaluates incoming traffic and applies managed threat protections. Logging is designed to avoid authorization credentials and other secrets.

Operational failures are surfaced rather than silently ignored. Security-relevant events are reviewed based on their severity, affected systems, and potential data exposure.

8. Incident response

When TrendHog identifies a suspected security incident, the responsible operator will:

Assess the event and identify affected systems and data.
Contain the issue, including disabling access or rotating credentials when appropriate.
Preserve relevant evidence and remediate the underlying weakness.
Restore normal operation and monitor for recurrence.
Notify affected parties, service providers, regulators, or platform partners when legally or contractually required.

Suspected vulnerabilities or security incidents involving TrendHog may be reported to hello@trendhog.com.

9. Service-provider security

TrendHog selects service providers according to the function they perform and the sensitivity of the information involved. Current infrastructure includes Vercel for application hosting and Supabase for managed database and authentication services. Other providers may support billing, storage, communications, and approved data integrations.

Provider access is limited through credentials and product configuration. TrendHog reviews material provider changes and removes access when a service is no longer required.

10. Retention and secure disposal

TrendHog retains information only while it supports an active product, contractual, security, or legal need. Authorization tokens are removed or made unusable when an integration is disconnected or access is revoked. Data scheduled for deletion is removed from active systems using the tools provided by the relevant service provider, subject to limited backup and legal-retention periods.

11. Policy review and contact

This policy is reviewed at least annually and after material changes to TrendHog's systems, data use, or legal obligations. Updates are published on this page with a revised effective date or version.

Questions about this policy may be sent to hello@trendhog.com.