CaughtUp Security and Privacy Program

Information security, access control, data protection, incident response, vulnerability management, and deletion procedures

Owner: CaughtUp owner and operator

Security and privacy contact: support@getcaughtup.io

Effective date: August 10, 2026

Review cycle: At least annually and after material changes

Information Security Program

Policy owner: CaughtUp owner and operator

Effective date: August 10, 2026

Purpose and scope

CaughtUp maintains a risk-based information security program appropriate to an owner-operated creator inbox and affiliate opportunity service. The program applies to company endpoints, source code, production services, user data, administrative accounts, vendors, and the public website.

Security objectives

- Protect the confidentiality, integrity, and availability of CaughtUp data.
- Limit access to the minimum necessary for an approved operational purpose.
- Prevent secrets, OAuth tokens, and personal data from entering source code,

public logs, documentation, or unapproved communication channels.

- Preserve creator control over drafts, sending, account connections, and data

deletion.

- Detect, contain, investigate, and communicate security incidents.

Governance

The owner and operator is accountable for this program and acts as Security and Privacy Lead. Security concerns are reported to support@getcaughtup.io. Policies are reviewed at least annually and after a material product, provider, legal, or security change. Material exceptions must be documented with their reason, duration, risk, and compensating safeguards.

Risk management

Security decisions consider data sensitivity, Internet exposure, tenant impact, provider dependency, likelihood of misuse, and the effect of loss or unauthorized disclosure. High-risk changes involving authentication, sending, secrets, personal data, or production access require explicit verification before release.

Personnel and vendor responsibilities

Only authorized persons may access administrative systems. Unique accounts and multi-factor authentication are required wherever supported. Service providers are selected for necessary capability and reviewed for security, privacy, access, retention, and incident-notification commitments appropriate to the data they process.

Compliance and review

CaughtUp maintains a public Privacy Policy and a process for access, correction, deletion, security, and complaint requests. The program does not represent that CaughtUp holds an independent certification unless one is formally obtained.

Network and Endpoint Security Policy

Policy owner: CaughtUp owner and operator

Effective date: August 10, 2026

Network protection

CaughtUp uses managed cloud services to separate public delivery, application processing, database and private storage, authentication, and secret management. Public requests use HTTPS. Administrative database access requires authenticated provider access. Application endpoints perform their own authorization and do not rely on network location alone.

The public site uses Cloudflare edge protection and restrictive response headers. Backend data is protected through authenticated APIs, owner scoping, row-level security, private storage, and service-only roles. Direct inbound services are limited to those required for the product. New public endpoints must have a documented purpose, authentication decision, input validation, and logging plan.

Monitoring

Application failures, authentication failures, service errors, and provider security notices are reviewed during operations and incident investigation. Unexpected access patterns, secret exposure, authorization failures, or public data exposure are treated as security events.

Endpoint baseline

Company endpoints must use supported operating systems, automatic security updates, antivirus with real-time protection, an enabled host firewall, screen locking, device encryption where supported, and unique password-protected user accounts. Administrative work must not be performed from shared or unmanaged accounts. Lost or compromised devices must be reported immediately and relevant sessions or credentials revoked.

Daily operating baseline

Administrative accounts must use unique credentials and multi-factor authentication wherever available. Screens must be locked when unattended. Sensitive information must not be left visible or printed without an operational need. Secrets must be kept in approved secret stores and must not be copied into source code, tickets, chat, screenshots, or public documents.

Access Control Policy

Policy owner: CaughtUp owner and operator

Effective date: August 10, 2026

Principles

Access to systems and personal data is granted according to least privilege, need to know, unique identity, and separation between public clients and privileged services. Shared administrative accounts are prohibited when a unique account is available.

User and service access

User requests require authenticated identity and are scoped to the owning user. Privileged server operations use controlled service credentials. Public clients must never contain service-role credentials, refresh tokens, or secret keys. Service-only database tables use row-level security and restricted role grants. Private files are delivered only through authorized application flows.

Administrative access

Administrative access is limited to the owner and any specifically approved person with an operational need. Multi-factor authentication is required where supported. Privileged access is not used for ordinary browsing or communication. Production data is not copied to local files unless required for a documented support or security task and protected throughout that task.

Access lifecycle

Access is approved before use, reviewed at least quarterly, and reviewed again after any role, provider, device, or security change. Unnecessary access is removed promptly. Sessions and credentials are revoked when a person, device, integration, or contractual relationship no longer requires access.

Logging and exceptions

Authentication events, privileged changes, and relevant application operations are retained through available provider and application logs. Any exception to this policy must be documented, time limited, and protected with compensating controls.

Data Classification and Encryption Policy

Policy owner: CaughtUp owner and operator

Effective date: August 10, 2026

Classification levels

Public data is approved for public release, such as website content and published policies. Internal data is routine operational material not intended for public release. Confidential data includes user settings, message-derived records, media-kit metadata, support records, and operational logs. Restricted data includes OAuth tokens, secret keys, passwords, privileged credentials, and raw personal data whose disclosure could enable account access or material harm.

Handling rules

Public data may be distributed through approved channels. Internal data is limited to operational use. Confidential data requires authenticated access and must not be placed in public repositories or unapproved services. Restricted data must remain server-side in approved secret or protected data stores and must never be written to source code, public logs, screenshots, documentation, chat, or client-side persistent storage.

Encryption

Internet traffic carrying account or personal data uses HTTPS and TLS. Sensitive configuration and OAuth credentials use server-side protected storage. Managed database and storage providers supply encryption at rest for hosted data. Company endpoints must use device encryption where supported when they store company information.

Data minimization and disposal

CaughtUp collects and processes only data required for the user-selected workflow, security, support, or legal obligations. Temporary exports and local copies must be avoided. When required, they must be access restricted and securely removed when the task is complete. Production secrets are rotated after suspected disclosure.

Incident Response and Breach Notification Policy

Policy owner and Incident Lead: CaughtUp owner and operator

Reporting channel: support@getcaughtup.io

Effective date: August 10, 2026

Reporting and scope

Suspected unauthorized access, personal-data exposure, malware, credential loss, service compromise, material availability loss, or policy violation must be reported promptly through the security channel. Reports should not include passwords, refresh tokens, secret keys, or unnecessary personal data.

Response process

The Incident Lead records the report, time, affected systems, reporter, known facts, and immediate risks. The incident is triaged by potential impact and urgency. Response activities include containment, preservation of relevant evidence, credential or session revocation when appropriate, investigation, remediation, recovery validation, and documented closure.

Roles

The owner and operator acts as Incident Lead, coordinates technical response, determines whether personal data or external systems are affected, preserves the incident record, and manages required communication. Relevant providers are contacted when their systems or evidence are required.

Notification

When an incident affects TikTok Shop, a seller, a creator, or personal data, CaughtUp will notify the affected party and any required authority without undue delay and within applicable legal or contractual deadlines. Notifications will describe the known nature of the incident, affected data or services, mitigation steps, user actions when relevant, and a contact channel. Facts will be updated as the investigation develops.

Post-incident review

Material incidents receive a documented review of root cause, control failures, remediation, notification decisions, and follow-up owners. Policies, monitoring, tests, credentials, or provider configurations are updated when needed to reduce recurrence.

Vulnerability and Threat Management Policy

Policy owner: CaughtUp owner and operator

Effective date: August 10, 2026

Identification

CaughtUp reviews application code, authentication boundaries, dependencies, provider advisories, error reports, and public exposure for vulnerabilities and threats. Reviews occur at least monthly, after material releases, and when a relevant provider or dependency publishes a security advisory.

Prioritization

Findings are prioritized using exploitability, Internet exposure, data sensitivity, tenant scope, privilege gained, and operational impact. Suspected secret exposure, authentication bypass, cross-user access, unauthorized sending, or public personal-data exposure is treated as urgent.

Remediation targets

Urgent findings are contained immediately and fixed or mitigated as soon as practicable. High-risk findings target remediation within 30 days. Lower-risk findings are scheduled according to exposure and product risk. If a target cannot be met, the reason, risk, compensating safeguards, and new target are documented.

Secure change process

Security changes are kept narrow, reviewed for sibling weaknesses, tested using the cheapest decisive verifier, committed before production deployment, and verified after deployment. Production secrets, user tokens, billing, and sending settings are not changed during testing without explicit authorization.

Reporting and records

Security reports are accepted at support@getcaughtup.io. Findings, decisions, verification evidence, and remediation status are recorded without including live secrets or unnecessary personal data.

Personal Data Protection and Deletion Policy

Policy owner and Privacy Lead: CaughtUp owner and operator

Request channel: support@getcaughtup.io

Effective date: August 10, 2026

Principles

CaughtUp processes personal data lawfully, transparently, and only for the user-selected product, security, support, or legal purpose. Personal data is minimized, access restricted, protected according to sensitivity, and retained only while necessary for those purposes.

Individual and seller requests

Users, sellers, creators, and TikTok Shop may request access, correction, restriction, export, or deletion through the request channel. CaughtUp verifies identity and authority before disclosing or changing data. Requests are tracked and completed within applicable legal or contractual timeframes. If a request cannot be fulfilled, the reason and available next steps are communicated.

Retention and deletion

Account settings, connection records, media kits, workflow records, drafts and edits, and related data are retained while needed to provide the active service. After a verified deletion request or the end of the applicable relationship, CaughtUp removes customer data from active systems without unreasonable delay, except where limited retention is required for law, security, fraud prevention, dispute handling, or provider backup recovery cycles. Data restored from a backup remains subject to the deletion requirement and is not returned to ordinary use.

Processors and transfers

CaughtUp uses providers needed for hosting, authentication, email integration, marketplace authorization, and bounded language processing. Provider access is limited to the service purpose. Data may be processed in the United States and other locations where authorized providers operate, as described in the public Privacy Policy and applicable provider terms.

Complaints and changes

Privacy complaints are recorded, investigated, and answered through the request channel. This policy and the public Privacy Policy are reviewed at least annually and after material changes to processing, providers, law, or the product.