Incident Response and Breach Notification Policy

CaughtUp adopted policy

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

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.