



Information Security Program

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: 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.