Data Classification and Encryption 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: 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.