Network and Endpoint Security 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

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.