Vulnerability and Threat Management 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

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.