Access Control 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

Principles

Access to systems and personal data is granted according to least privilege, need to know, unique identity, and separation between public clients and privileged services. Shared administrative accounts are prohibited when a unique account is available.

User and service access

User requests require authenticated identity and are scoped to the owning user. Privileged server operations use controlled service credentials. Public clients must never contain service-role credentials, refresh tokens, or secret keys. Service-only database tables use row-level security and restricted role grants. Private files are delivered only through authorized application flows.

Administrative access

Administrative access is limited to the owner and any specifically approved person with an operational need. Multi-factor authentication is required where supported. Privileged access is not used for ordinary browsing or communication. Production data is not copied to local files unless required for a documented support or security task and protected throughout that task.

Access lifecycle

Access is approved before use, reviewed at least quarterly, and reviewed again after any role, provider, device, or security change. Unnecessary access is removed promptly. Sessions and credentials are revoked when a person, device, integration, or contractual relationship no longer requires access.

Logging and exceptions

Authentication events, privileged changes, and relevant application operations are retained through available provider and application logs. Any exception to this policy must be documented, time limited, and protected with compensating controls.