cappd.

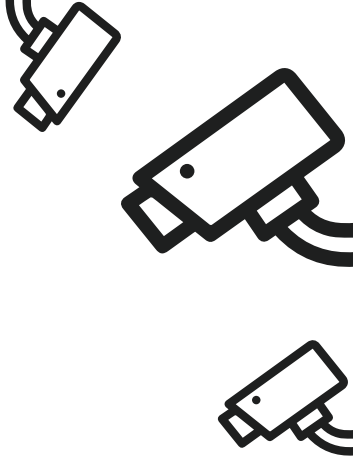
Security taken seriously

At Cappd, we prioritise the security of our web application, and your data, with the utmost seriousness. Our robust security measures are designed to safeguard your information at every level, from application to server, and throughout our development processes.

Our commitment to security ensures that your data is protected from unauthorised access and vulnerabilities, providing you with peace of mind while using our services.

security

security
security



Here's an overview of our commitments, methods, and ongoing focus.

application

1. 2FA should be enabled on all admin accounts, given the wide-ranging access they have. This should be encouraged for owners of any team, even if they don't require it for users.

2. When logged in to the system, every query made is bucketed to the user's team, with access controls at the application and database level to ensure requests can't be altered to access information belonging to another team.

3. Only publicly accessible content (profiles, images) is cached, all internal data such as contacts are queried directly from the database every time, again bucketed by the team's UUID, to eliminate the risk of a cached copy leaking data, or cache poisoning attacks.

4. All authentication and authorisation systems implement rate limiting, including the magic login links, at the application level, protecting from any attempt to brute force authentication.

5. All tokens in the system (such as magic login links) are cryptographically secure, ensuring the token itself cannot be guessed or brute forced.

server

1. The server is both externally and internally firewalled, so that only web and secured shell access is available.

2. All communication into and out of the server require encryption-in-transit, typically via TLS/SSL, even between internal services.

3. All ingress into the system happens via Cloudflare, taking advantage of their DDoS protection, bot mitigation and their web application firewall, which provides automatic protection against critical vulnerabilities the moment they are publicly disclosed.

4. The server itself runs an intrusion detection system to detect and block any scanning or bruteforce attempts that bypass Cloudflare.

5. Security updates to the server are applied automatically. Security updates to the application software are automatically raised and tested before being deployed.

6. Backups are encrypted at rest and stored in SOC 2 Type II and ISO 27001 certified facilities.

development

1. OWASP Secure Coding best practices are followed during development.

2. No real-world data is used during system testing or development.

3. Automated testing is used against all security-related operations at a minimum, to ensure updates and new development work doesn't break the existing security model.