Security Policy

Last Updated: 2026-04-16 Effective Date: 2026-04-16

1. Hosting and Encryption

1.1. The production infrastructure of the Capawesome Platform is operated with carefully selected infrastructure providers. The current list is set out in the Data Processing Agreement.

1.2. All data in transit is encrypted using TLS 1.2 or higher.

1.3. Data at rest is encrypted using industry-standard methods (encryption at rest).

2. Access Control

2.1. All administrative access to production systems requires multi-factor authentication (MFA).

2.2. Access rights are granted on a least-privilege basis and reviewed on a regular basis.

3. Handling of Customer Data

3.1. **Customer secrets and credentials**: Apple API keys, .p12 certificates, provisioning profiles, and Android keystores are stored encrypted at rest. Access is limited to the automated build and publish pipeline. Credentials are deleted upon account or contract termination.

3.2. **Customer source code**: Source code is processed solely for its intended purpose in isolated build environments. The Provider's personnel shall only access source code in a support case with the express consent of the customer.

3.3. **Code signing for live updates**: The Provider supports code signing for live updates. Customers may sign application bundles with their own RSA key pair. The application verifies the signature before applying the update. The private key remains with the customer.

3.4. **No AI/ML training**: The Provider does not use customer data (including source code, build artefacts, credentials, and end-user SDK data) for training, fine-tuning, or improving AI or ML models.

4. Certifications and External Audits

4.1. The Provider is **SOC 2 Type II** certified. The audit report is available on request under NDA.

4.2. From 2026 onwards, **annual external penetration tests** are conducted. Reports are available on request under NDA.

5. Incident Response

5.1. The Provider maintains a documented incident response process covering detection, containment, remediation, and post-incident review.

5.2. In the event of a security incident affecting customer data, the customer shall be notified without undue delay. For personal data breaches, the notification obligations set out in the Data Processing Agreement apply (48-hour deadline).

5.3. In the event of a security incident affecting confidential customer materials (in particular source code, build secrets, or store credentials), a separate notification shall be provided in accordance with the confidentiality provisions of the Terms of Service, regardless of whether personal data is affected.

6. Vulnerability Disclosure

6.1. The Provider welcomes the responsible disclosure of security vulnerabilities. Reports shall be sent to: security@capawesome.io

6.2. **Testing boundaries**: Security researchers shall observe the following boundaries:

- no denial-of-service attacks against production systems,
- no access to other customers' data,
- no exploitation beyond proof of concept.

6.3. **Safe harbour**: The Provider shall not pursue civil or criminal action against security researchers who act in good faith within the boundaries set out above.

7. Contact

7.1. Security incidents and vulnerability reports: security@capawesome.io

7.2. This document serves transparency and trust-building purposes. It is not contractually binding. The binding technical and organisational measures are set out in the Data Processing Agreement (Annex 2).