

Acceptable Use Policy

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

1. Scope

1.1. This Acceptable Use Policy ("**AUP**") applies to the use of all services provided by Genz IT Solutions GmbH ("**Provider**"), including paid and free offerings.

1.2. This AUP supplements the General Terms and Conditions (GTC). In the event of a conflict, the GTC shall prevail.

2. Prohibited Content

2.1. The Customer shall not distribute, store, or process any content through the Capawesome Platform that:

- contains or distributes malware, viruses, trojans, spyware, ransomware, or phishing components,
- violates applicable law, in particular criminal law, youth protection law, or export control regulations,
- is discriminatory, defamatory, harassing, or glorifies violence,
- infringes copyrights, trademarks, patents, or personality rights of third parties.

3. Prohibited Activities

3.1. The following activities are prohibited when using the Capawesome Platform:

- **Circumvention of app store guidelines:** Using the Capawesome Platform to circumvent review or approval processes of Apple or Google. When using Live Updates, the Customer shall in particular comply with the [Apple App Store Review Guideline 2.5.2](#) and the [Google Play "Device and Network Abuse" Policy](#).
- **Reverse engineering:** Decompilation, disassembly, or other reverse engineering of the Capawesome Platform beyond the extent mandated by applicable law.
- **Unauthorised load and penetration testing:** Conducting load or security tests against the Capawesome infrastructure without prior written approval from the Provider.
- **Resource abuse:** Using the Capawesome infrastructure for purposes that do not correspond to its intended use, in particular crypto-mining, covert data processing in bundles, or other resource-intensive third-party use.
- **Circumvention of billing limits:** Circumventing resource quotas and billing limits (e.g. live update MAU limits, native build concurrency), automated scraping of the platform, account sharing to circumvent limits, or technical circumvention of licence validation mechanisms.
- **Spam:** Sending unsolicited messages or mass communications through the Capawesome Platform.
- **Attacks on third parties:** Using the Capawesome Platform to conduct attacks against third parties or their infrastructure.

4. Customer Obligations

4.1. The Customer shall ensure that its use of the Capawesome Platform complies with all applicable laws and regulations, including the applicable app store guidelines of Apple and Google.

4.2. The Customer is responsible for securing its account and access credentials. The Customer shall notify the Provider without undue delay of any unauthorised use that comes to its attention.

5. Reporting Abuse

5.1. Violations of this AUP may be reported to abuse@capawesome.io. The Provider shall review incoming reports and, where there is reasonable suspicion, initiate the measures described in Section 6.

6. Enforcement

6.1. In the event of violations of this AUP, the Provider shall take graduated measures:

- Warning and request to cease the violation,
- Blocking of individual affected content or features,
- Temporary suspension of the account,
- Termination for cause of the contractual relationship.

6.2. In the event of an acute threat (in particular ongoing distribution of malware, active attacks on third parties, or imminent legal violations), the Provider shall be entitled to take immediate measures without prior warning. The Customer shall be notified without undue delay of the measure taken and the reason for it.

7. Amendments to this AUP

7.1. The Provider may amend this AUP. The amendment procedure, right of objection, and legal consequences set out in the GTC (Section 17) shall apply accordingly.

7.2. In the event of material restrictions under this AUP, the Customer shall have the right to terminate for cause with effect from the date on which the amendment takes effect.