

BRANIA

Acceptable Use & Supplemental Terms

Version 1.0 | Effective August 7, 2026 | <https://www.brania.ai/legal/acceptable-use>

These terms govern acceptable use of the BRANIA Services and supplement the MSA. Customer is responsible for Users and for ensuring that use of the Services complies with applicable law, channel/provider policies and the Contract Documents.

1. Prohibited Conduct

- illegal, fraudulent, deceptive, defamatory, abusive, harassing or rights-infringing activity;
- sending spam, unlawful marketing, communications without required consent, or content prohibited by applicable carrier, messaging, WhatsApp, email or platform rules;
- uploading malicious code, interfering with availability, bypassing access controls, credential sharing or unauthorized security testing;
- reverse engineering, scraping non-public system logic, attempting to extract confidential prompts/models, or using the Services to develop a competitive product;
- processing Personal Data or sensitive information without legal authority, or using the Services in a way that violates applicable privacy or health-data requirements;
- using AI or automation for prohibited high-impact decisions or as the sole basis for medical diagnosis/treatment; or
- resale, service bureau, sublicensing or third-party access not authorized by an Order Form.

2. Communications Compliance

Customer is the sender/originator of communications initiated through the Services and is responsible for lawful contact lists, opt-in/opt-out rules, required disclosures, call-recording notices, telemarketing restrictions, quiet hours, number registration and compliance with communications-channel policies. BRANIA may implement technical controls or suspend a channel when required by law, a provider or risk-management requirements.

3. Third-Party Feature Terms

Certain optional features may be subject to additional provider or in-application terms. If Customer activates an optional feature, Customer authorizes BRANIA to apply the additional terms necessary for that feature, provided they are presented or referenced before activation when material. Optional paid features require Customer approval as stated in the Order Form.

4. Security Testing

Customer may not conduct penetration testing, vulnerability scanning, load testing, password cracking, network discovery or similar testing against BRANIA or its providers without BRANIA's prior written authorization and an agreed testing plan.

5. Usage Limits and Abuse

BRANIA may enforce reasonable technical or operational limits necessary to protect security, performance, provider policies and fair use. If Customer's use creates unusual risk, material platform degradation or provider sanctions, BRANIA may require remediation, rate limiting, pre-funding, configuration changes or suspension of the affected feature.

6. Remedial Action

BRANIA may remove or disable unlawful content, suspend affected functionality, block abusive traffic, rotate credentials, or take other proportionate action necessary to address a violation, security threat, provider requirement or legal obligation. Where reasonably practicable, BRANIA will notify Customer and provide an opportunity to cure.

7. Updates

BRANIA may update these Terms to reflect changes in law, security, abuse patterns or provider/channel policies. Updates will be versioned and archived. Material changes that affect an active Initial Term will not materially reduce Customer's contractual rights except where required by law or provider rules necessary to continue offering the affected feature.