BRANIA

Security, Hosting & Support Policy

Version 1.0 | Effective August 7, 2026 | https://www.brania.ai/legal/security

This policy describes BRANIA's standard operational practices for security, hosting, maintenance and support of subscribed BRANIA Services. It applies when incorporated by an Order Form or the MSA. It should be read with the DPA and any customer-specific SOW.

1. Security Program

- BRANIA maintains a risk-based security program appropriate to the nature and scale of its Services and may use the security capabilities of specialized cloud, platform and communications providers.
- Access to production Customer environments and Customer Personal Data is restricted to personnel and contractors with a business need, subject to confidentiality obligations.
- BRANIA uses role-based or least-privilege access practices where supported by the applicable systems and periodically reviews privileged access.
- Multi-factor authentication is used for privileged BRANIA accounts where the applicable provider supports it and it is operationally appropriate.
- Customer Data transmitted between supported web clients and hosted services is protected using industry-standard encrypted transport where supported by the applicable provider.
- Data-at-rest protections rely in part on encryption and security controls supplied by the applicable cloud/platform provider. BRANIA does not represent control over underlying provider encryption implementations beyond BRANIA's contractual/technical rights.
- BRANIA maintains incident-response procedures, vendor management practices and change-management practices appropriate to its operations.

2. Hosting and Third-Party Infrastructure

BRANIA may host, operate or deliver Services using third-party cloud, platform, communications, database, AI and infrastructure providers. Processing locations and direct subprocessors are maintained at https://www.brania.ai/legal/subprocessors. BRANIA may replace providers under the MSA and DPA, provided contractual protections are maintained.

Customer acknowledges that availability of communications channels, telephony, messaging, email, third-party APIs and customer-controlled systems depends on external networks and providers outside BRANIA's direct control.

3. Backups, Resilience and Recovery

BRANIA uses commercially reasonable recovery practices and relies on backup, redundancy and recovery capabilities of applicable hosted providers. Backup scope and retention vary by Service and provider. Unless a SOW expressly states otherwise, Customer is responsible for maintaining copies of data held in Customer-controlled systems and for exporting data needed for its own independent retention obligations.

4. Security Incident Management

BRANIA maintains a process to investigate suspected security events, contain confirmed incidents, coordinate with affected providers, remediate identified issues and notify Customers as required by the DPA and applicable law. Security incident communications will be directed to the Customer contacts designated in the Order Form or provisioning information.

5. Vulnerability and Change Management

BRANIA applies commercially reasonable processes to address material vulnerabilities and security updates within components under its control. Underlying providers manage vulnerabilities and patches within their infrastructure according to their own programs. BRANIA may update software, configurations, models or providers to address security or operational risk.

6. Customer Security Responsibilities

- Protect User credentials and endpoints; enforce appropriate passwords and MFA where available.
- Restrict User access by role and promptly remove access for departed or reassigned personnel.
- Use secure networks and devices and maintain Customer-controlled systems, APIs and integrations.
- Notify BRANIA promptly of suspected compromise, credential misuse or unauthorized access.
- Avoid submitting credentials, secrets or sensitive data into fields not intended for that purpose.
- Comply with applicable data-retention, consent, recording, patient/privacy and security obligations for Customer's business.

7. Maintenance

BRANIA may perform routine maintenance and deploy product updates without advance notice when they do not materially disrupt Service. For maintenance reasonably expected to cause material interruption, BRANIA will use commercially reasonable efforts to provide advance notice when practicable. Emergency maintenance may occur without prior notice when necessary to address security, availability or provider issues.

8. Support Services

Standard platform support is included unless an Order Form states otherwise. BRANIA provides first-line triage for subscribed Services and may escalate provider-dependent incidents through the support channels available from the applicable Third-Party Service. Support excludes new scope, custom development, Customer-controlled systems, data cleanup, new integrations, training beyond the SOW and enhancement requests. BRANIA does not guarantee a third-party provider's response or restoration time.

Severity	Definition	BRANIA operational response target
S1 – Critical	Production Service materially unavailable for most authorized users, or confirmed critical security issue with no reasonable workaround.	Priority acknowledgement and triage during Support Hours; prompt provider escalation when applicable. No resolution-time guarantee.
S2 – High	Major function materially impaired for multiple users; significant business impact; workaround limited.	Same-business-day acknowledgement and triage during Support Hours; provider-dependent restoration remains upstream-dependent.
S3 – Normal	Non-critical defect, question or limited impairment with a reasonable workaround.	Target initial response: 1 business day.
S4 – Request	How-to request, enhancement request, cosmetic issue or general guidance.	Target initial response: 2 business days.

Standard Support Hours: Monday-Friday, 9:00 a.m.-6:00 p.m. Mexico City time, excluding BRANIA-observed holidays, unless an Order Form or SOW states otherwise. Requests may be submitted outside those hours, but staffed BRANIA response is not guaranteed. Response targets mean acknowledgement and triage, not resolution, and do not create service-credit obligations.

9. Availability and Upstream Service Levels

Unless an Order Form expressly states otherwise, BRANIA does not provide a percentage uptime guarantee or service credits for Bedrock or other functionality materially dependent on Third-Party Services. For BRANIA-controlled components, BRANIA will use commercially reasonable efforts to maintain availability and restore material interruptions. For provider-dependent incidents, BRANIA will use commercially reasonable efforts to monitor, triage, escalate and communicate status, but restoration remains dependent on the applicable provider. No BRANIA commitment for a Third-Party Service exceeds the corresponding provider commitment, if any.

10. Support Exclusions

- issues caused by Customer Data, Customer configuration outside agreed procedures, unauthorized modifications or Customer-controlled integrations;
- Third-Party Service outages or policy/API changes outside BRANIA’s control;
- Customer network, device, endpoint or credential compromise;
- use outside Documentation or contracted scope; and
- feature requests, bespoke development or operational consulting not included in the SOW.

11. Policy Updates

BRANIA may update this policy to reflect security practices, provider capabilities, law, technology and operational improvements. Updates will not materially reduce the overall level of contractual security protection during an active Initial Term. Material versions will be dated and archived at https://www.brania.ai/legal/archive.

12. Security Contact

Until BRANIA publishes a dedicated security contact, Customers may report suspected security incidents to hello@brania.ai with “SECURITY” in the subject line. BRANIA may publish a dedicated contact through the Legal Center without requiring an amendment.