ACCEPTABLE USE POLICY (AUP)

DASHAMAP

Table of Contents

AUP

ACCEPTABLE USE POLICY

DASHAMAP

Controlling Version

Last updated: 22 February 2026
Effective date: 22 February 2026

This document (the "AUP" or "Acceptable Use Policy") sets forth the permitted and prohibited use rules for the DashaMap platform and related services (the "Service"). The AUP is an integral part of the Terms of Service (the "ToS") and applies to all persons who access or use the Service, including individual users, registered accounts, authorized users of business customers, tenant administrators, staff, white-label customers, invited persons, visitors who use protected or interactive features, and third parties who interact with Service features.

The AUP applies regardless of the active plan, duration of use, access channel, device, or geographic area. Use of the Service must comply with the ToS, the Disclaimer, the Privacy Policy, the Cookie Policy, the AI Notice (AI Transparency & Compliance Notice), and any other policy or annex referenced in the contractual documents.

Service Owner (Provider)
GLOBAL MOUNTAIN GROUP LLC
30 N Gould St #47047, Sheridan, Wyoming 82801-6317 – U.S.A.
Company ID: 2023-001208525 | EIN: 61-2074460
Email: info@globalmountain.group
Website: www.globalmountain.group

---

1. Purpose of the AUP, Scope, and General Principles

1.1 Objective of the AUP

The AUP aims to:
a) protect the security, availability, integrity, continuity, and operational reliability of the Service;
b) prevent technical, economic, contractual, and legal abuses (including scraping, circumvention, fraud, reverse engineering, attacks, misuse of credits and premium features);
c) protect user data, infrastructure, the technology supply chain, third-party providers, and the Provider's rights;
d) ensure use consistent with the nature of the Service, including the symbolic/edutainment component and any AI functions for text generation or reformulation;
e) preserve infrastructure resources and operating costs (AI/LLM, compute, storage, exports, shareable links, premium features, security and anti-fraud);

f) support a proportionate, documentable enforcement framework consistent with applicable laws.

1.2 Scope of application

The AUP applies to any use of the Service, including, by way of example:
a) browsing protected areas;
b) creating and managing accounts/tenants/profiles;
c) entering data, notes, content, "Souls," or third-party profiles;
d) generating reports, outputs, exports, PDFs, shareable links, or AI functions;
e) integrations, automations, or business/white-label/client portal features;
f) activities performed directly by the user or indirectly through the user's employees, contractors, consultants, agents, scripts, tools, or systems.

1.3 Acceptance and contractual incorporation

The AUP is incorporated into the ToS and forms part of the Service contractual framework. The user accepts the AUP in the manner provided by the ToS (including, where applicable, clickwrap/checkbox mechanics, account registration, plan activation, use of protected features, or continued use after effective updates properly published and communicated to the extent required by law).
The Company may retain evidence of acceptance, applicable version, timestamps, and consent/acceptance events for contractual, anti-fraud, audit, legal defense, and compliance purposes, in accordance with the Privacy Policy and applicable laws.

1.4 Enforcement guiding principles

Interpretation and application of the AUP shall occur, to the extent permitted by law, according to criteria of:
a) proportionality;
b) severity and risk;
c) urgency;
d) recurrence;
e) impact on other users, the Service, or the technology supply chain;
f) reasonable technical or contractual evidence available at the time of the decision.

1.5 Nature of the Service (reference)

DashaMap operates in a symbolic/edutainment context and may integrate AI functions for text generation or reformulation. The Service must not be used as a sole or automated decision engine for high-impact decisions (medical, legal, financial, employment, credit, insurance, or equivalent), except with competent human review and in compliance with applicable laws and contractual documents.

---

2. Operational Definitions (for purposes of the AUP)

For purposes of this AUP:

a) **“Abuse”** means any use of the Service that violates applicable contractual documents or that, based on reasonable technical/contractual indicators, risks security, availability, integrity, continuity, compliance, operating costs, or rights of the Provider, users, or third parties.

b) **“Scraping / Crawling / Data Mining”** means automated, systematic, or semi-systematic extraction of data, pages, outputs, reports, metadata, assets, or patterns from the Service, even if partial, through bots, scripts, agents, browser automation, extensions, unauthorized APIs, or equivalent techniques.

c) **“Reverse Engineering”** means any attempt to reconstruct code, logic, algorithms, prompts, pipelines, models, architectures, methods, structures, or internal behaviors of the Service, including systematic tests aimed at inferring implementation or operation.

d) **“Circumvention”** means any attempt to bypass, evade, or neutralize plan limits, quotas, credits, rate limits, paywalls, access controls, anti-bot/anti-fraud protections, watermarks, link expirations, export controls, security controls, or compliance measures.

e) **“AI Misuse”** means use of the Service or its outputs for model training, creation of datasets/corpora/benchmarks, extraction of patterns or behaviors, manipulation of safety filters, malicious prompts, unauthorized competitive benchmarking, or other uses contrary to contractual documents or applicable AI rules.

f) **“Prohibited Content”** means illegal, fraudulent, abusive, harmful, defamatory, deceptive, or otherwise prohibited content under the ToS, this AUP, or applicable laws.

g) **“Authorized User”** means a natural person authorized by a business customer to use the Service within the relevant tenant/environment.

h) **“Shareable Link” / “Magic Link”** means any URL or mechanism generated by the Service for access, viewing, or sharing of content, reports, or resources, with or without expiration, and with or without additional controls.

i) **“Credits”** means consumption units, quotas, or contractual limits provided by plan, add-ons, promotions, or Service functions (e.g., AI, export, PDF, tokens, activations, seals, or equivalents).

j) **“Suspected Violation”** means a situation where reasonable signals, patterns, or evidence indicate a possible violation of the AUP, even prior to full ascertainment.

k) **“Confirmed Violation”** means a violation supported by reasonable technical, contractual, documentary, or behavioral evidence.

l) **“Material Violation”** means a violation that, due to severity, risk, or impact, may justify immediate limitations, suspension, or termination (e.g., attack, mass scraping, data exfiltration, fraud, systematic circumvention, severe unlawful use of the Service).

m) **“White Label”** means features allowing brand customization, output redistribution, or delivery to end customers via portal, reports, or customized channels, within the limits of the activated plan.

---

3. Permitted Use (Baseline)

3.1 General rule

DashaMap may be used solely for lawful purposes, contractually permitted purposes, and purposes consistent with the nature of the Service.

3.2 Examples of permitted use (non-exhaustive)

Generally permitted, subject to plan, credits, quotas, and applicable policies:
a) creating and managing profiles, settings, preferences, and “Souls”;
b) consulting timelines, calculations, reports, and outputs of the Service;
c) generating outputs, documents, exports, and PDFs via official functions;
d) saving notes, journals, tags, and lawful content;
e) sharing outputs through official functions (download, expiring links, magic links) with authorized recipients;
f) using the Service for lawful personal or professional purposes, provided such use is not prohibited by the ToS, Disclaimer, Privacy Policy, Cookie Policy, AI Notice, or this AUP.

3.3 General user responsibility

The user remains responsible for:
a) use of the user’s account, credentials, sessions, and devices;
b) lawfulness, accuracy, and legitimacy of entered data, including third-party data;
c) compliance with applicable laws in the user’s jurisdiction;
d) compliance with the Service contractual documents;
e) use and sharing of outputs with third parties, end customers, or the public.

---

4. Main Prohibitions (Prohibited Use)

4.1 Violations of law and third-party rights

It is prohibited to use the Service to:
a) engage in illegal activities, fraud, scams, phishing, money laundering, impersonation, deception, or fraudulent conduct;
b) infringe intellectual property rights, trade secrets, copyrights, trademarks, image rights, privacy, confidentiality, or other third-party rights;
c) defame, harass, threaten, stalk, intimidate, or discriminate against third parties;
d) collect, process, or share third-party personal data without an adequate lawful basis, title, or authorization;

e) use Service outputs to create false statements, fictitious testimonials, deceptive content, or untrue attributions to real persons/entities.

4.2 Scraping, harvesting, and unauthorized automation

It is prohibited to:
a) perform scraping/crawling/data mining on any part of the Service (UI, pages, reports, outputs, exports, links, endpoints, assets, metadata);
b) use bots, agents, browser automation, or scripts to extract outputs at scale or systematically;
c) systematically reproduce, copy, index, or archive pages or reports;
d) bypass anti-bot protections, rate limits, CAPTCHA, authentication systems, or session controls;
e) use the Service as a source to build unauthorized databases, archives, datasets, or corpora;
f) automate requests at scale or systematically without the Provider's written authorization, even where per-request volume appears low but overall behavior is repetitive, coordinated, or suitable to bypass limits/quotas.

4.3 Reverse engineering, probing, and attacks

It is prohibited to:
a) decompile, disassemble, or attempt to reconstruct Service components;
b) perform unauthorized vulnerability scanning, probing, fuzzing, brute-force, credential stuffing, or security testing;
c) attempt injection or exploits (including, by way of example, SQL injection, XSS, SSRF, CSRF, prompt injection, command injection, path traversal, or equivalents);
d) interfere with logging, audit, monitoring, anti-fraud, telemetry, or security controls;
e) attempt unauthorized access to data, tenants, accounts, environments, or resources of other users;
f) conduct denial-of-service, stress testing, artificial load, or activities suitable to degrade the Service without written authorization.

4.4 Bypassing economic limits, credits, plans, and paywalls

It is prohibited to:
a) bypass or manipulate credit/consumption counters (AI, PDF, export, tokens, activations, seals, or equivalents);
b) create multiple accounts, multiple identities, or coordinated schemes to evade plan limits, quotas, blocks, or policies;
c) exploit bugs, race conditions, or system errors to obtain features/outputs without credit consumption or due payment;
d) resell, transfer, exchange, or monetize plan credits/benefits outside official functions (e.g., authorized gift/referral), without written authorization;

e) use abusive chargebacks, bad-faith disputes, or other means to obtain free access to already delivered features.

4.5 Anti-training clause (use of outputs for AI training / datasets)

It is prohibited to:
a) use outputs, reports, texts, timelines, or content generated by DashaMap to train the user's or third parties' AI models;
b) create datasets, corpora, benchmarks, or evaluation sets based on Service outputs;
c) systematically extract outputs to distill behaviors, patterns, prompts, or the Service style;
d) publish or sell prompt packs, report packs, template packs, or materials derived from the Service for commercial purposes without written consent;
e) use the Service for model-evaluation farming or unauthorized competitive benchmarking.

4.6 Unauthorized sharing, links, and access

It is prohibited to:
a) share links, reports, or access with unauthorized parties;
b) publish shareable links on public channels if they contain or may expose personal/confidential data;
c) artificially extend link validity, remove watermarks, alter notices, evade expirations, or bypass access controls;
d) impersonate third parties or use false identities to obtain access to reports/profiles/tenants;
e) transfer accounts or share credentials in violation of the ToS/plan.

4.7 Brand misuse, white-label, and prohibited claims

It is prohibited to:
a) present DashaMap or its outputs as medical, legal, financial, or scientifically certified advice;
b) use white-label functions to deceptively conceal the nature of the Service or to make misleading claims;
c) make claims of guaranteed accuracy, certain predictability, or assured results;
d) use the Provider's name, trademarks, reputation, or references in a misleading or unauthorized manner.

4.8 High-impact uses prohibited as sole/automatic basis

It is prohibited to use DashaMap as a sole or automated basis for:
a) medical/therapeutic decisions;
b) financial investment, credit, or trading decisions;
c) legal decisions or professional compliance decisions;
d) hiring/firing, scoring, ranking, or profiling with significant effects;
e) assessments or decisions producing legal or equivalent effects without competent human review.

5. Content and Data: Data Hygiene Rules

5.1 Strictly prohibited data (except where expressly required by dedicated and compliant official functions)

It is prohibited to enter, upload, transmit, or store in the Service:
a) passwords, API keys, access tokens, seed phrases, OTP codes, or security credentials;
b) full payment card numbers or payment data not required by the Service via official payment provider flows;
c) malware, exploits, harmful payloads, or tools intended for attack/sabotage;
d) illegal material, including exploitation or abusive content, illegal material relating to minors, or non-consensual content;
e) content intended to facilitate criminal activity or security violations;
f) third-party data or content where the user knows or reasonably should know they have no title/lawful basis to process it.

5.2 Unnecessary and strongly discouraged data (except where strictly lawful and necessary, under the user/customer's full responsibility)

Entry of the following data is strongly discouraged and, where not strictly necessary, must be avoided:
a) health data, diagnoses, therapies, medical reports, detailed clinical information;
b) data on religion, philosophical beliefs, sexual orientation, political or trade-union affiliation;
c) full identification document numbers, bank accounts, or other sensitive identifiers not required;
d) trade secrets or third-party confidential information not authorized;
e) minors' data without an adequate lawful basis and verifiable authority/consent, where required by law.

Any entry of such data, where deemed strictly necessary by the user/business customer for lawful purposes, occurs under the full responsibility of the user/customer, in compliance with applicable laws, the Privacy Policy, the DPA (if applicable), and the contractual documents.

5.3 Dangerous or prohibited content

It is prohibited to upload, generate, request, or distribute through the Service:
a) content inciting hatred, violence, terrorism, discrimination, or harassment;
b) content promoting self-harm, suicide, or severely dangerous behavior;
c) illegal or non-consensual sexual content;
d) fraudulent, defamatory, or deceptive content;
e) content violating third-party rights or third-party platform terms where the Service is used for distribution/integration to such platforms.

5.4 User warranty regarding entered data and content

The user represents and warrants that the user has the rights, consents, mandate, or lawful bases necessary to enter data and content into the Service, including third-party data. The user remains responsible for consequences arising from data/content entered in violation of law or contractual documents and shall indemnify/hold harmless the Provider within the limits set forth in the ToS for claims attributable to the user.

---

6. Special Rules for Business Customers, White Label, and Staff

6.1 Access and role governance (least privilege)

Business customers are responsible for:
a) assigning minimum necessary permissions (least privilege);
b) revoking or updating access when staff leave or change role;
c) adopting internal security, audit, and access management procedures;
d) defining internal policies for sharing, magic links, exports, retention, and use of third-party data;
e) controlling use of the Service by authorized users within the tenant.

6.2 Third-party data and lawful basis

Where a business customer creates profiles, reports, or outputs for third parties, the customer:
a) must have an adequate lawful basis, mandate, engagement, or title for processing;
b) must provide notices and manage consents/rights under GDPR and applicable local laws;
c) must ensure that reports are not used for prohibited purposes;
d) remains responsible for lawfulness of processing and for instructions given to authorized users.

6.3 White label and communications to end customers

The customer using white-label/client-portal features is responsible for its content, commercial claims, disclaimers, and notices to end customers. In particular, the customer:
a) must not make medical, legal, or financial claims;
b) must not promise guaranteed accuracy or certain results;
c) must ensure appropriate human review where context requires it;
d) must, where applicable, indicate that parts of the content may be AI-assisted;
e) must not use white label to deceptively conceal the nature of the Service.

6.4 Flow-down obligations (minimum downstream obligations)

The business/white-label customer must impose on its authorized users and, where applicable, on its end customers rules compatible with this AUP, at least regarding:
a) prohibition of scraping/systematic extraction;
b) prohibition of unauthorized sharing of links/reports/access;
c) prohibition of high-impact use as sole/automatic basis;

d) prohibition of anti-training/dataset building on outputs;
e) prohibition of deceptive claims or guaranteed-accuracy claims;
f) obligation of lawful use and respect for third-party rights.

6.5 Responsibility for staff and related parties' activities

Unless otherwise provided by mandatory law or written agreement, the business customer is liable to the Provider for activities carried out through its tenant by authorized users, staff, administrators, or persons operating under its control or authorization.

---

7. Rate Limiting, Fair Use, and Resource Protection

7.1 Technical and contractual limits

The Service may apply technical and contractual limits on:
a) requests per minute/hour/day;
b) AI generations, exports, PDFs, and premium functions;
c) API/integration usage (if and when available);
d) consumption of AI/PDF/export credits or equivalents;
e) number of active sessions, shareable links, downloads, or other resources.

7.2 Fair use and anomalous usage profile

Abuse includes, even if not expressly listed elsewhere, any use suitable to saturate resources or bypass the Service's economic/technical logic, including:
a) repetitive or artificial generations to saturate AI/compute;
b) mass production of reports to create duplicate archives or datasets;
c) use of the Service as a batch factory outside plans or intended functions;
d) load distribution across coordinated multiple accounts;
e) unauthorized automations that alter the normal usage profile.

7.3 Dynamic protective measures

In case of suspected or confirmed violation, the Company may adopt proportionate technical measures, including:
a) throttling or enhanced rate limiting;
b) temporary blocking of functions (AI, export, upload, links, logins from specific devices/IPs or risk signals);
c) account verification, ownership verification, or additional security checks;
d) suspension or termination, where applicable;
e) introduction or strengthening of anti-fraud/anti-bot controls, to the extent permitted by law.

---

8. Security: Minimum User Obligations

The user agrees to:
a) use strong and unique passwords;
b) enable MFA/2FA where available;
c) not share credentials or sessions;
d) keep device, browser, and software updated;
e) avoid using the Service on compromised networks or devices;
f) log out from shared devices;
g) promptly report suspected unauthorized access, incidents, or credential loss;
h) not bypass security warnings or Service controls.

---

9. Sanctions, Export Control, Restricted Territories, and Geographic Compliance

9.1 Sanctions and export control compliance

It is prohibited to use the Service in violation of laws on economic sanctions, export controls, embargoes, or applicable trade restrictions. The user represents, to the extent permitted by law, that the user is not subject to restrictions that would render use of the Service unlawful.

9.2 Reasonable and proportionate technical screening

For compliance, anti-fraud, and security purposes, the Company may use reasonable and proportionate technical controls, including technical indicators, risk signals, access patterns, approximate geolocation, and other anti-fraud tools, within legal limits and consistently with the Privacy Policy and Cookie Policy.

9.3 Territorial restrictions and blocked access

The Company may limit or block access/provision in territories, networks, or high-risk contexts or those subject to regulatory/compliance restrictions, to the extent permitted by law. Use of VPN/proxy/TOR or masking techniques to bypass geographic or compliance blocks may constitute a violation of this AUP.

---

10. Enforcement: Suspension, Termination, Review, and Remedies

10.1 General enforcement framework

In case of suspected or confirmed violation, the Company may adopt enforcement measures based on severity, risk, urgency, recurrence, and impact. Measures may be progressive or immediate, depending on the case.

10.2 Possible measures (graduation)

To the extent permitted by law and at the Company's reasonable discretion, one or more of the following measures may be adopted:
a) warning and request for remediation/correction;

b) limitation or disabling of specific functions;
c) request for account/identity/ownership verification or security confirmations;
d) temporary suspension of an account or tenant;
e) termination of the account or relationship, pursuant to the ToS;
f) revocation of links, access, exports, or content shared via official functions;
g) blocking of IPs/devices/signals, where lawful, necessary, and proportionate;
h) reporting to competent authorities where required by law or reasonably necessary to protect the Service, third parties, or the technology supply chain.

10.3 Immediate measures without notice

For material violations or imminent risks (e.g., security incident, mass scraping, attack, data exfiltration, fraud, systematic circumvention, severe abuse of the AI/payments supply chain), the Company may apply immediate limitations or suspensions, including without notice, to the extent necessary to contain risk.

10.4 Notice and opportunity to clarify (where reasonably possible)

Where the nature of the risk does not require immediate action, the Company may send a warning or request for clarification/remediation with a reasonable deadline to respond. Failure to respond, inadequate response, or repeated conduct may result in escalation of enforcement measures.

10.5 Review / request for reconsideration

Except in cases of manifest fraud, serious risk, or legal prohibitions, the user may request reconsideration of an enforcement measure by writing to info@globalmountain.group and providing:
a) affected account/tenant;
b) contested measure;
c) approximate date/time;
d) explanation and relevant documents/evidence.
The Company will evaluate the request based on internal priorities, complexity, and risk. Reconsideration does not guarantee reinstatement and does not automatically suspend the adopted measure.

10.6 Effects on credits, subscriptions, and refunds (coordination with ToS / Refund / Billing)

In case of suspected or confirmed violation:
a) the Company may temporarily freeze credits/functions during security or anti-fraud checks;
b) in case of confirmed violation or fraud, it may void credits obtained or used improperly;
c) it may deny refunds to the extent permitted by law and pursuant to the ToS, Refund Policy, and/or Billing/Subscription/Credits Policy (where published);
d) it may dispute chargebacks using technical evidence, logs, and contractual records;
e) suspension/termination for violation does not entitle the user to automatic compensation

for remaining periods, without prejudice to applicable non-derogable rights and any mandatory legal provisions.

In case of a technical error attributable to the Company or an ascertained false positive, any remedies provided under the ToS, Refund Policy, and/or Billing/Subscription/Credits Policy remain applicable.

10.7 No waiver for failure to act immediately

The Provider's decision not to take action in a specific case, or to delay enforcement, does not constitute approval of the relevant conduct, does not create any precedent, and does not limit the Provider's right to take enforcement action in the future.

---

11. Logging, Evidence, and Data Processing for Security/Enforcement

11.1 Data processed for abuse prevention and security

To prevent abuse, ensure security and continuity of the Service, and defend its rights, the Company may process technical and security data, including logs, events, metadata, anti-fraud signals, access/usage patterns, and enforcement records, proportionately and for lawful purposes.

11.2 Consistency with the Privacy Policy and Cookie Policy

Data categories, lawful bases, retention periods, data subject rights, and relevant details are governed by the Privacy Policy and, where applicable, the Cookie Policy. This AUP does not replace or expand beyond legal limits the processing rights set out in privacy documentation.

11.3 Evidence retention

The Company may retain technical and documentary evidence relating to suspected or confirmed violations for security, audit, anti-fraud, legal defense, chargeback/dispute management, and compliance purposes, in accordance with applicable law and privacy documentation.

---

12. Reporting Abuse and Vulnerabilities (Responsible Disclosure)

12.1 Abuse reporting

Email: info@globalmountain.group
Suggested subject: "AUP – Abuse report"
Where available, include: affected account/tenant, date/time, description of facts, links, screenshots, logs, estimated impact.

12.2 Responsible disclosure: general principle

The Company accepts responsible, non-destructive vulnerability reports. However, this AUP does not constitute general authorization to perform security testing on production systems.

12.3 Activities prohibited even in the disclosure context

Absent prior written authorization, it remains prohibited to:
a) access third-party data, tenants, or accounts;
b) exfiltrate credentials, datasets, or confidential information;
c) alter, delete, or destroy data;
d) degrade Service availability;
e) publish exploits or sensitive details without reasonable coordination with the Company.

12.4 Activities permitted only in minimal and non-destructive form (no general safe harbor)

Absent written authorization, only strictly limited, passive, or minimally intrusive, non-destructive checks are permitted, aimed solely at reasonably confirming the existence of a vulnerability, without access to third-party data and without altering the Service. Any doubt shall be resolved conservatively.

12.5 Coordination, remediation, and confidentiality

The Company may request technical details, controlled proofs-of-concept, confidentiality/NDA, and will coordinate remediation based on internal priorities, severity, and resource availability.

12.6 No implied bounty / no unlimited safe harbor

Absent a separate written agreement, this AUP does not establish any bug bounty, compensation, or general/unlimited safe harbor. Any active testing on production systems without written authorization remains prohibited.

---

13. AUP Updates (Amendments, Effectiveness, and Traceability)

13.1 Right to update

The Company may update this AUP for technical, legal, security, anti-fraud, compliance reasons, Service evolution, functional changes, or changes in the technology supply chain.

13.2 Publication and traceability

The updated version will be published on the Site/Service indicating “Last updated” and/or “Effective date.” The Company may maintain a changelog or summaries of changes, including separately.

13.3 Material changes and continued use

For material changes significantly affecting usage rules or enforcement, the Company may provide reasonable notices via the Service, account email, or other available channels, to the extent required by law. Continued use of the Service after the effective date constitutes acceptance of the updated version, without prejudice to non-derogable rights and applicable legal obligations.

---

14. Documentary Precedence, Interpretation, and Severability

14.1 Documentary precedence

This AUP supplements the ToS. In case of conflict:
a) the Privacy Policy prevails for data processing/privacy matters;
b) the Cookie Policy prevails for tracking tools, cookies, and consent where applicable;
c) the Disclaimer and/or the AI Notice prevail regarding the nature of the Service, interpretive limits, AI use, and non-reliance;
d) the ToS prevail for contractual rules, billing, licenses, subscriptions, termination, and disputes;
e) this AUP prevails for usage rules, security, anti-abuse, and enforcement.

14.2 Reasonable interpretation and non-exhaustive examples

Examples in this AUP are illustrative and do not limit the scope of general rules where conduct is clearly incompatible with security, compliance, or contractual documents. Application of the AUP shall in any event follow criteria of reasonableness and proportionality.

14.3 No waiver

Except where expressly waived in writing by an authorized representative of the Provider, any failure or delay in exercising any right, power, or remedy under this AUP does not constitute a waiver of that right, power, or remedy.

14.4 Severability

If any provision of this AUP is held invalid, void, or unenforceable, the remaining provisions remain valid and effective to the extent permitted by law.

---

15. Additional Protective Clauses (Enterprise Shield)

15.1 No agency / no partnership / no representation

Nothing in this AUP creates an agency, partnership, joint venture, employment relationship, mandate, or representation between the user/customer and the Provider. The user/customer may not bind the Provider toward third parties.

15.2 No reliance / no duty to monitor

The Company does not guarantee total prevention of abuse, attacks, or improper uses and does not assume a general obligation to monitor in real time all user content or behavior. The user remains responsible for their use of the Service and for verification of outputs in relation to intended use.

15.3 Cost recovery for severe abuse

To the extent permitted by law and without prejudice to remedies under the ToS and/or law, in the event of severe abuse attributable to the user/customer (e.g., mass scraping, attacks, fraud, systematic circumvention), the Company reserves the right to request reimbursement of reasonable costs that are:
a) documented;
b) causally linked to the conduct;
c) reasonably necessary for containment, investigation, remediation, and security/compliance management.
This clause does not exclude further contractual or legal remedies, where applicable.

15.4 Continuous improvement of controls

The Provider reserves the right to improve or modify technical controls, filters, rate limits, anti-abuse systems, and policies, and to block suspicious patterns, to the extent permitted by law and according to necessity/proportionality criteria.

15.5 Survival of relevant clauses

Provisions that by their nature must survive suspension/termination remain effective after account or relationship termination, including by way of example: anti-abuse prohibitions, anti-training, IP, logging/evidence, enforcement, cost recovery, no waiver, severability, contacts, controlling language, and any clause necessary to protect the Provider's or third parties' rights.

---

16. Governing Law and Venue (Reference to the ToS)

Governing law, venue, any dispute resolution procedures, and consumer-right rules are governed by the ToS. In all cases, non-derogable consumer rights and applicable mandatory rules in the user's jurisdiction remain unaffected, where relevant.

---

17. Controlling Language

This AUP may be translated for convenience. In case of interpretive discrepancies, the official English version of the Service shall prevail, if published as the controlling version and made reasonably accessible to users. This Italian version is provided for consultation and internal/commercial operational purposes until publication of the English controlling version, unless the Provider expressly indicates otherwise.

18. Contacts

GLOBAL MOUNTAIN GROUP LLC
Email: info@globalmountain.group
Website: www.globalmountain.group
Registered office: 30 N Gould St #47047, Sheridan, Wyoming 82801-6317 – U.S.A.

END OF AUP DOCUMENT