Restricted Purpose Agreement - Abliterated Models Program

This Restricted Purpose Agreement (this "Agreement") is entered into by Boundless Networks, Inc. ("Boundless") and the customer identified in the Order Form (the "Customer"), and supplements the Boundless Platform Services Terms (the "Customer Terms" available at https://inference.boundless.network/terms).

Recitals

A. Boundless makes available, to a limited set of customers and on a per-customer basis, certain open-weight models that have been modified to remove or reduce refusal behavior (commonly referred to as "abliterated" models).

B. Boundless grants access to these models only to customers that complete a diligence review to Boundless's satisfaction and commit to the restrictions in this Agreement.

C. The Customer has requested access to one or more such models solely for Defense Purposes, and Boundless is willing to grant access in reliance on the Customer's representations, warranties, and covenants in this Agreement.

The parties agree as follows:

1. Definitions

1.1 "Affiliate" means any entity that controls, is controlled by, or is under common control with the Customer.

1.2 "Defense Purposes" means use of the Restricted Models exclusively for defensive or protective applications, and never for offensive, malicious, or harmful purposes. Defense Purposes are limited to: (a) defensive cybersecurity, meaning the monitoring, detection, investigation, containment, mitigation, remediation, and protection of networks, systems, software, and data against threats, including identifying vulnerabilities and developing, testing, and validating patches, detections, and countermeasures; (b) defensive malware and threat analysis, reverse engineering, and threat intelligence; (c) security testing, red teaming, control validation, and exercises, in each case conducted only where the owner of the systems in scope has authorized the testing in writing, including the use of abliterated models, and within the authorized scope; (d) research, development, and evaluation in support of the activities in (a) through (c), conducted in controlled environments.

1.3 "Misuse" means any use of the Restricted Models (a) outside the Defense Purposes, (b) in breach of this Agreement or the Customer Terms, or (c) that constitutes a Prohibited Use.

1.4 "Order Form" means the customer-specific schedule executed by you, that identifies the Restricted Models and the term.

1.5 "Permitted Users" means the Customer personnel whom the Customer authorizes to access the Restricted Models, and for whom the Customer is fully responsible under Section 4.5.

1.6 "Prohibited Uses" means the activities listed in Schedule 1.

1.7 "Restricted Models" means the open-weight models identified in the Order Form that have been modified to remove or reduce refusal behavior, together with their associated endpoints and documentation.

1.8 "Vetting Information" means the information the Customer provides to Boundless in connection with the diligence review described in Section 4.

1.9 Capitalized terms not defined in this Agreement have the meanings given in the Customer Terms.

2. Grant of Access

2.1 Grant. Subject to this Agreement and the Customer Terms, Boundless grants the Customer a limited, non-exclusive, non-transferable, non-sublicensable, revocable right to access the Restricted Models through the Services, solely for Defense Purposes, solely through Permitted Users, and, except as permitted under Section 1.2(c), solely for the Customer's internal use.

2.2 Per-customer clearance. Access is granted only on a per-customer basis, and only after (a) the Customer completes Boundless's diligence review under Section 4 to Boundless's satisfaction, (b) the parties execute an Order Form, and (c) Boundless activates access in writing. Boundless may decline, condition, or defer access in its discretion, and no access exists unless and until activated.

2.3 No transfer. The Customer shall not share, resell, sublicense, or otherwise make the Restricted Models available to any third party, including its Affiliates, without Boundless's prior, informed, written consent. Access credentials are issued per Permitted User and shall not be shared.

2.4 API access only. The Customer receives API access only. The Customer shall not attempt to extract, reconstruct, or otherwise obtain the weights, architecture, or other internals of any Restricted Model, and shall not use outputs of the Restricted Models to train or improve any other model, except as expressly permitted by Boundless in writing or as required by the applicable Model Terms.

2.5 Changes. Boundless may modify, replace, or withdraw any Restricted Model, and may suspend or terminate access under Section 6.

3. Restricted Purpose Covenant

3.1 Covenant. The Customer represents, warrants, and covenants that it shall use the Restricted Models solely for Defense Purposes, and shall not, and shall not permit any Permitted User or any third party to, use the Restricted Models for any other purpose or in connection with any Prohibited Use.

3.2 Prohibited Uses. The Customer shall comply with Schedule 1 (Prohibited Uses). Boundless may update Schedule 1 from time to time as required by applicable law or to address emerging risks, effective upon notice to the Customer.

3.3 No circumvention. The Customer shall not circumvent, disable, or attempt to defeat any safety, security, or access-control feature of the Services, and shall not use the Restricted Models to develop or improve safeguard-circumvention techniques for use outside the Defense Purposes.

3.4 Compliance with law. The Customer shall comply with all applicable laws in connection with its use of the Restricted Models, including computer-misuse, export-control, and sanctions laws, and shall not export, re-export, or provide access to the Restricted Models in violation of those laws.

3.5 No authorization. For clarity, Boundless's grant of access does not constitute authorization for any security testing of any system. The Customer must obtain all authorizations required for its activities itself.

3.6 Material covenants. The covenants in this Section 3 are material to Boundless's grant of access. Any breach involving a Prohibited Use is a material breach that terminates this Agreement immediately and is not subject to cure.

4. Diligence, Eligibility, and Ongoing Obligations

4.1 Eligibility. The Customer represents and warrants that: (a) it is an organization (and not an individual) engaged in legitimate defensive-security or security research activities; (b) the Vetting Information it has provided is true, accurate, and complete; (c) neither it nor its Permitted Users is a Sanctioned Person or located in a Restricted Territory (each as defined in the Customer Terms); and (d) the individual executing this Agreement is authorized to bind the Customer.

4.2 Reliance. Boundless has granted access in reliance on the Vetting Information and the covenants in this Agreement.

4.3 Notification. The Customer shall promptly notify Boundless, and in any event within five business days, of any material change to the Vetting Information, including any change in ownership or control, any change in sanctions status, and any Misuse or suspected Misuse.

4.4 Re-verification. Boundless may request additional information and re-verify eligibility at any time. The Customer shall respond within ten business days. Failure to respond is grounds for suspension.

4.5 Permitted Users. The Customer controls its Permitted Users and is fully responsible for them. The Customer shall (a) limit access to Permitted Users; (b) ensure that each Permitted User is bound by written obligations at least as protective as this Agreement; (c) train Permitted Users on this Agreement and Schedule 1; and (d) promptly revoke access for any Permitted User who breaches this Agreement. Boundless does not approve or supervise Permitted Users, and the Customer may add, remove, or replace them at its discretion. The Customer bears full responsibility and liability for its Permitted Users'

choices, security practices, acts, omissions, and mistakes, including any Misuse, as if they were the Customer's own.

4.6 Certifications. As a condition to any renewal, an officer of the Customer shall certify in writing that the Customer has remained in compliance with Sections 3 through 5 during the period then ended.

4.7 KYC/KYB. Before activation and on an ongoing basis, the Customer shall pass Boundless's KYC/KYB review under, and remain in compliance with, Boundless's KYC/KYB policy as updated from time to time, and shall provide the information and documentation reasonably required for that review. Failure to pass or remain in compliance is grounds for declining, suspending, or terminating access.

5. Controls, Monitoring, and Reporting

5.1 Customer controls. The Customer shall maintain, and verify upon Boundless written request, reasonable administrative, technical, and physical safeguards for its use of the Restricted Models, including per-user access controls, logging of Restricted Model usage, protection of outputs consistent with their sensitivity, a designated security contact, and an internal acceptable-use policy consistent with Schedule 1.

5.2 Monitoring. The Customer acknowledges that Boundless may monitor usage metadata, such as request volumes, error patterns, and abuse indicators, for security and abuse-prevention purposes, and may act on reports and lawful requests, consistent with the Customer Terms.

5.3 Reporting. The Customer shall report any Misuse or suspected Misuse, and any incident that could reasonably lead to Misuse, promptly and in any event within twenty-four hours of becoming aware, and shall reasonably cooperate with Boundless's investigation.

5.4 Records. The Customer shall maintain records of its use of the Restricted Models sufficient to demonstrate compliance with this Agreement for at least five years and shall make them available to Boundless upon reasonable request.

6. Suspension; Term; Termination

6.1 Suspension. Boundless may suspend or limit access immediately and without liability if it reasonably determines that (a) the Customer's use poses a security, legal, or operational risk; (b) the Customer has breached this Agreement, including any Prohibited Use; or (c) suspension is required by a supplier, court, or governmental authority. No cure period applies to any breach involving a Prohibited Use.

6.2 Term. This Agreement begins on activation and continues for one (1) year, unless earlier terminated under this Section. After that period, this Agreement may be renewed only by mutual written consent for additional one (1) year periods.

6.3 Termination. Either party may terminate this Agreement on written notice. Boundless may terminate immediately upon any breach of Section 3 or Section 4.

6.4 Effect. On termination or suspension, access ends; the Customer shall cease all use, destroy or return any Restricted Model materials it received, and on request certify compliance with this Section. Sections 1, 3, 4, 5.4, 6.4, and 7 survive.

7. Relationship to the Customer Terms; Legal Terms

7.1 Supplement; precedence. This Agreement supplements and is incorporated into the Customer Terms. As to the Restricted Models, this Agreement controls over the Customer Terms in case of conflict; as to all other matters, the Customer Terms control. An Order Form controls only as to the items it expressly varies.

7.2 Disclaimers and liability. The disclaimers, release, and limitations of liability in the Customer Terms (Sections 9 through 11) apply to the Restricted Models and this Agreement. Without limiting the Customer's indemnity in the Customer Terms, the Customer shall indemnify and hold harmless the Released Parties (as defined in the Customer Terms) from and against claims, losses, liabilities, fines, penalties, and costs, including reasonable legal fees, arising from (a) the Customer's breach of Section 3, Section 4, or Section 5, or (b) any Misuse.

7.3 Export and sanctions. Without limiting Section 3.4, the Customer shall not access or use the Restricted Models in or for the benefit of any Sanctioned Person or Restricted Territory, and shall comply with all applicable export-control and sanctions laws.

7.4 Dispute resolution; governing law. The dispute-resolution and governing-law provisions of the Customer Terms (Section 12) apply to this Agreement.

7.5 Notices. Notices are given as provided in the Customer Terms (Section 13.3); notices under this Agreement may also be sent to the contacts identified in the Order Form.

7.6 Entire agreement; amendments. This Agreement, together with the Customer Terms, the Order Form, and the Schedules, is the entire agreement regarding the Restricted Models. Amendments must be in writing and signed by both parties, except that Boundless may update Schedule 1 upon notice as stated in Section 3.2.

7.7 General. Boundless may assign this Agreement as provided in the Customer Terms; the Customer may not assign it without Boundless's prior written consent. There are no third-party beneficiaries. If any provision is held invalid, the remainder stands. This Agreement may be executed in counterparts, including electronically.

Schedule 1: Prohibited Uses

1. Offensive or destructive cyber activity. Developing, deploying, or materially supporting malware, ransomware, exploits, or attacks against any system; unauthorized access; denial-of-service; or destructive operations. Authorized security testing within the Defense Purposes is not a Prohibited Use.

2. Weaponry. Designing, developing, or operating weapons, weapons systems, or autonomous targeting capabilities; or generating content that facilitates chemical, biological, radiological, or nuclear weapons.

3. Child safety. Any content or material that constitutes child sexual abuse material or child sexual exploitation, and any sexualization of minors. Zero tolerance. Suspected material must be reported to the appropriate authorities and to Boundless.

4. Non-consensual intimate imagery. Generating or manipulating intimate depictions of an identifiable person without their consent.

5. Violence and crime. Content or tools that materially facilitate terrorism, violent extremism, trafficking, or other serious crimes.

6. Unlawful surveillance. Surveillance or tracking of individuals, or social scoring, except as lawful, authorized, and within the scope of an approved engagement.

7. Circumvention. Defeating safety, security, or access controls; or using outputs to train or improve other models in violation of Section 2.4.

8. Access sharing. Sharing credentials, reselling access, or making the Restricted Models available to third parties, including Affiliates, without Boundless's written consent.

9. Export and sanctions. Any use in violation of export-control or sanctions laws.

10. Misrepresentation. Misrepresenting authorization, affiliation, or the scope of any security testing.