AI SERVICES ADDENDUM

This AI Services Addendum (the "**Addendum**") forms part of the Agreement between Borg and Customer and applies to Customer's access to and use of AI-enabled, automated, or agentic Services (including, without limitation, Asset Discovery Services, and Penetration Testing Services) made available by Borg from time to time to Customer (collectively, the "**AI Services**"). By requesting or initiating any AI Services, Customer acknowledges and agrees to be bound by this Addendum. Capitalized terms used but not defined in this Addendum have the meanings given in the General Terms.

1. PRODUCT SCOPE MODELS AND RELATED WARRANTIES

1.1 **Scope of Asset Discovery Services.** Customer acknowledges and agrees that Asset Discovery Services are designed to identify and surface Discovered Assets. Discovered Assets identified through Asset Discovery Services form part of the output of the relevant AI Services and may be displayed, mapped, analysed, categorized, or otherwise processed by Borg as part of providing those Asset Discovery Services.

1.2 **Scope of Penetration Testing Services.** Customer acknowledges and agrees that Penetration Testing Services are limited to Selected Assets. The identification, display, inference, import, or discovery of an asset by or through the AI Services (e.g., through Asset Discovery Services) does not by itself authorize Borg to validate, test, exploit, or otherwise actively engage with that asset through Penetration Testing Services.

1.3 **Excluded Assets May Be Indirectly Affected.** Customer acknowledges and agrees that, although Excluded Assets are not intended to be actively targeted through Penetration Testing Services, such services directed at Selected Assets may nonetheless incidentally, indirectly, transitively, or unavoidably interact with, traverse, reach, query, affect, or test Excluded Assets as part of identifying, validating, reproducing, or demonstrating a vulnerability, exploit path, privilege escalation path, trust relationship, dependency, or other security issue affecting a Selected Asset. Designating an asset as an Excluded Asset does therefore not guarantee that such Excluded Asset will not be affected by Penetration Testing Services performed against Selected Assets.

1.4 **Dynamic Scope.** Customer acknowledges and agrees that the scope of authorized activity under this Addendum is dynamic and is established through the Odin platform and other Borg-provided workflows. The authorized scope for any given AI Services activity consists solely of: (i) for Asset Discovery Services, the assets, environments, repositories, integrations, credentials, and materials made available by or on behalf of Customer for discovery or analysis; and (ii) for Penetration Testing Services, the Selected Assets that have been made available by or on behalf of Customer, that have not been designated as Excluded Assets (without prejudice to Section 1.3), and that remain subject to the applicable platform controls, credential scopes, environment settings, exclusions, rate limits, safety restrictions, and other constraints then in effect.

1.5 **No Automatic Testing of Discovered Assets.** Unless and until a Discovered Asset becomes a Selected Asset in accordance with this Addendum, it shall be treated as informational only for purposes of Penetration Testing Services and outside the scope of active testing, validation, exploit verification, or other active offensive activity.

1.6 **Customer Warranty as to Scope.** Customer represents, warrants, and agrees that all Selected Assets are, at all relevant times, owned or controlled by Customer or otherwise subject to all rights, permissions, consents, approvals, and other legal authority necessary for Borg to provide the applicable AI Services. Customer further represents, warrants, and agrees that it has obtained all necessary internal approvals and all necessary third-party permissions, consents, and authorizations required for Borg to provide the AI Services.

1.7 **Customer Warranty as to Authorizations.** Customer represents, warrants, and agrees that all Authorizations issued by or on behalf of Customer are valid, accurate, and authorized instructions from Customer, and that they accurately reflect Customer's intended scope selections, exclusions, and permissions for the AI Services. Customer shall ensure that no person submits Authorizations on Customer's behalf unless duly authorized to do so.

1.8 **Customer Responsibility for Third-Party Restrictions.** Customer represents, warrants, and agrees that its use of the AI Services, and Borg's performance of the AI Services with respect to the relevant Discovered Assets and Selected Assets, does not violate any applicable law or any terms, policies, restrictions, or requirements applicable to any third-party provider, platform, cloud environment, repository, API, host, or connected system used in connection with the AI Services.

1.9 **Production Election.** Borg strongly recommends that Customer first use Penetration Testing Services or similar AI Services which may materially stress or otherwise impact the Customer's environments and/or systems (including, without limitation, cloud auditing services) in non-production, staged, sandboxed, or otherwise isolated environments where feasible. If Customer elects to use any AI Services against live, production, production-connected, or otherwise sensitive systems, Customer does so at its sole risk and remains solely responsible for all resulting operational, technical, legal, and commercial consequences.

2. AUTHORIZATION METHODS

2.1 **Root Domain Verification.** Where Customer connects a root domain to the Odin platform and completes TXT record verification or another Borg-approved domain verification method, Customer represents, warrants, and agrees that such verification constitutes a valid and authorized instruction for Borg to perform AI Services and related scope management in relation to that root domain and related internet-visible assets associated with it.

2.2 **Cloud and Infrastructure Connections.** Where Customer connects a cloud tenant, project, subscription, account, service account, role, API credential, or other authenticated cloud or infrastructure integration through the Odin platform, Customer represents, warrants, and agrees that such connection constitutes a valid and authorized instruction for Borg to perform the applicable AI Services within the scope of that connected environment, subject to the relevant selections, exclusions, settings, and limitations then in effect.

2.3 **Repository and Integration Connections.** Where Customer connects repositories, code hosts, SaaS systems, APIs, or other integrations through Odin, Customer represents, warrants, and agrees that such connection and authorization flow constitutes a valid and authorized instruction for Borg to access and process such connected resources to the extent necessary to provide the applicable AI Services.

2.4 **Dashboard Scope Authorization.** Where Customer affirmatively selects, enables, approves, or launches Penetration Testing Services against assets in Odin, Customer represents, warrants, and agrees that those in-product actions constitute Customer's express instruction and authorization to perform the relevant Penetration Testing Services against those Selected Assets.

2.5 **Least-Privilege Access.** Customer shall provide only the minimum credentials, permissions, roles, scopes, and access tokens reasonably necessary for the relevant AI Services. Customer is solely responsible for determining whether any credentials, tokens, service accounts, repository access, cloud permissions, or other access methods are over-privileged, excessive, production-scoped, or otherwise inappropriate for the intended use. Borg has no duty to assess or reduce the privilege level of access provided by Customer.

2.6 **Express Instruction for AI Services.** Customer acknowledges and agrees that each Authorization, including root-domain verification, repository connection, cloud connection, integration authorization, scope selection, and run-launch action, constitutes Customer's express request and instruction to Borg to perform the applicable AI Services against the relevant in-scope assets.

3. CUSTOMER MONITORING AND INCIDENT REPORTING

3.1 **Customer Monitoring Responsibility.** Customer is solely responsible for monitoring its own systems, environments, and Selected Assets while AI Services are in use, including while Penetration Testing Services are running or otherwise active, and for maintaining personnel and emergency contacts capable of responding to operational issues – and may utilize the suspension/stop functionality for a given AI Service within the Odin platform if needed.

3.2 **Notification to Borg.** If Customer believes that AI Services are causing instability, disruption, or unintended consequences, or otherwise materially adversely impacting any person, system, or data, Customer may notify Borg through the channels designated by Borg.

3.3 **Borg Limitation Efforts.** Following such notice, Borg shall use commercially reasonable efforts to limit, restrict, or suspend the applicable AI Services activity as soon as reasonably practicable. However, Customer acknowledges that Borg cannot guarantee that any applicable AI Services activity can be paused, limited, or suspended immediately or effectively in all circumstances, and that in-flight requests, queued jobs, already-triggered processes, passive or background processes, and related logging, shutdown, audit, or incident-handling processes may continue briefly or continue to generate metadata after Customer's intervention or request, or Borg's attempted intervention. Borg therefore strongly advises that Customer ensure monitoring in accordance with Section 3.1, and uses the stop/suspension functionality within the AI Services as available to Customer.

4. RECORDS AND HUMAN ACCESS RESTRICTIONS

4.1 **Technical Records.** Customer acknowledges and agrees that Borg may collect, generate, retain, and display logs, screenshots, request and response fragments, code snippets, configuration details, metadata, findings, reproducibility information, and related technical records reasonably necessary to provide the AI Services, validate findings, support remediation, maintain an audit trail, investigate abuse, preserve service integrity, and defend legal claims.

4.2 **Authorization Records.** Customer acknowledges and agrees that records of Authorizations, including verification events, integration authorizations, workspace settings, selections, exclusions, credentials, launch actions, stop or pause requests, and written instructions, may be retained by Borg as evidence of Customer's authorization, instructions, and scope selections.

4.3 **Restricted Human Access.** Notwithstanding anything to the contrary in the Agreement, no Borg employee or team member shall access or review the substantive contents of Customer's internal files, repositories, databases, applications, environments, or other information residing within Customer's systems in connection with the provision of AI Services without Customer's prior explicit consent, except to the extent required by applicable law. For the avoidance of doubt, this restriction does not prevent Borg personnel from accessing credentials, logs, metadata, Findings, operational telemetry, audit records, screenshots, or other technical records generated by or through the AI Services to the extent reasonably necessary to operate, support, secure, audit, troubleshoot, or improve the AI Services, provided that such access does not involve review of the substantive contents of Customer's internal files, repositories, databases, applications, environments, or other information residing within Customer's systems.

4.4 **Controlled Access if Consent Granted.** If Customer grants consent under Section 4.3, any access by Borg personnel to the substantive contents of Customer's internal files, repositories, databases, applications, environments, or other information residing within Customer's systems shall be limited in time, closely monitored by Borg, and used solely for the express purpose for which access has been granted – and, for the avoidance of doubt, be subject to the duty of confidentiality under the General Terms.

4.5 **No General Human Review Obligation.** Unless otherwise is agreed, Customer acknowledges that Borg is not obliged to human-review all AI Services activity, outputs, findings, evidence, logs, screenshots, request or response fragments, or other technical records. Borg personnel may instead rely on automated workflows, system-generated telemetry, metadata, and selective review processes in operating, supporting, securing, auditing, troubleshooting, or improving the AI Services.

5. SAFETY CONTROLS AND TESTING RESTRICTIONS

5.1 **Safety Controls.** Customer acknowledges and agrees that the AI Services may be subject to technical and operational controls implemented through Odin or otherwise by Borg, including scope restrictions, exclusions, environment designations, testing windows, blackout periods, rate limits, concurrency limits, credential restrictions, and other safety controls reasonably designed to manage risk and operational impact.

5.2 **Customer-Configured and Default Controls.** Where Customer has configured safety controls, testing windows, blackout periods, or other operational restrictions in Odin, such controls shall govern the applicable AI Services activity. Where Customer has not configured any such controls, Borg may apply reasonable default controls and may restrict or limit higher-risk AI Services activity until appropriate constraints are established – but is under no obligation to do so.

6. ASSUMPTION OF RISK AND LIMITATION OF LIABILITY

6.1 **No Guarantee of Coverage or Accuracy.** Without limiting the General Terms, Customer acknowledges and agrees that AI Services are inherently non-deterministic, probabilistic, and operationally risky. Outputs may be incomplete, inaccurate, inconsistent, hallucinated, non-reproducible, delayed, or difficult to explain, and AI Services may fail to identify vulnerabilities, may generate false positives or false negatives, may execute unintended sequences of actions, and may produce outputs or recommendations that are unsafe, misleading, or operationally harmful. Borg does not guarantee that AI Services will not affect live systems, alter data, trigger alerts, cause lockouts, create instability, or otherwise interfere with Customer's systems, environments, or data.

6.2 **Assumption of Risk.** To the maximum extent permitted by law, Customer knowingly assumes the risks associated with Customer's configuration, authorization, selection, enablement, launch, and use of the AI Services, including risks associated with Customer's use of Penetration Testing Services in relation to live, production, production-connected, or otherwise sensitive Selected Assets.

Customer is therefore strongly advised to back up all data and systems within the target environment before initiating Penetration Testing Services, and to ensure that appropriate restore mechanisms and contingency plans are in place for the target systems.

6.3 **No Liability for Authorized AI Services Activity.** To the maximum extent permitted by law, and without limiting the General Terms, Customer shall not hold Borg liable for downtime, degradation, delays, data loss, data corruption, inaccurate outputs, missed findings, or other operational consequences arising from Borg's provision of AI Services in accordance with the Agreement.

6.4 **No Liability for Unintended AI Actions.** Customer acknowledges that, despite safeguards, AI Services may issue requests, exploit attempts, configuration changes, write actions, deletions, data mutations, or other operations that alter, corrupt, expose, lock, degrade, or otherwise affect Customer's systems, applications, environments, or data. To the maximum extent permitted by law, Customer assumes these risks where Customer has configured, authorized, enabled, launched, or otherwise used the relevant AI Services.

6.5 **Excluded Assets Risk Allocation.** To the maximum extent permitted by law, Customer assumes the risk that Penetration Testing Services performed against Selected Assets may incidentally, indirectly, or transitively affect Excluded Assets, cf. Section 1.3. If Customer wishes to eliminate or reduce such risk, Customer is solely responsible for removing, isolating, segmenting, disabling, disconnecting, or otherwise protecting the relevant Excluded Assets from the applicable environment before initiating the relevant Penetration Testing Services. Borg shall have no liability for any effects on Excluded Assets, connected infrastructure, third-party infrastructure, or proprietary infrastructure arising use of the Penetration Testing Services, except to the extent such liability cannot lawfully be excluded.

6.6 **Remediation Suggestions and Code Changes.** Where AI Services generate remediation suggestions, code changes, patches, pull requests, retesting actions, workflow automations, or similar outputs, such outputs are suggestions only unless expressly agreed otherwise in writing. Customer is solely responsible for reviewing, validating, approving, testing, and deciding whether to implement or deploy any such output. Borg shall have no liability for any consequences arising from Customer's reliance on, implementation of, or failure to review such outputs.

7. INDEMNIFICATION

7.1 **Indemnity Obligation.** Without limiting Customer's indemnification obligations under the General Terms, Customer shall defend, indemnify, and hold harmless the Borg Indemnified Parties from and against any and all third-party claims, investigations, fines, penalties, regulatory actions, losses, liabilities, costs, and expenses arising out of or relating to Customer's configuration, authorization, selection, enablement, launch, or use of the AI Services. For the avoidance of doubt, this indemnity obligation shall not be subject to any limitations of liability under the General Terms.

Such claims include, without limitation, claims arising from unauthorized targeting, Customer's lack of authority for any Selected Asset or other connected or selected asset or environment, Customer's use of the AI Services in breach of third-party provider terms, third-party rights or applicable law, Customer's breach of any warranties in this Addendum, Customer's use of the AI Services against live or production environments, or Customer's failure to maintain appropriate safeguards, approvals, backups, restoration capability, monitoring, or incident response capability.

7.2 **Additional Customer Indemnity for Data and Content Risks.** Without limiting the foregoing, Customer shall defend, indemnify, and hold harmless the Borg Indemnified Parties from and against any and all claims, investigations, regulatory actions, fines, penalties, losses, liabilities, costs, and expenses arising out of or relating to (i) Personal Data, illegal content, or regulated data present in Customer's systems, repositories, environments, findings, or other Customer-provided or Customer-connected content, (ii) Borg's Processing of such data in accordance with the Agreement and Customer's instructions, or (iii) Customer's failure to implement appropriate safeguards, notices, permissions, legal bases, or restrictions in relation to such data.

8. GENERAL

8.1 **Incorporation into Agreement**. This Addendum is an integral part of the Agreement and is considered a Service Appendix. All terms and provisions of the General Terms (including confidentiality, governing law, dispute resolution, indemnification, and data protection) apply to this Addendum, except as specifically modified and/or supplemented herein. In the event of a conflict between this Addendum and the General Terms, this Addendum controls with respect to the AI Services.

9. PRODUCTION RISK AND CUSTOMER RESPONSIBILITIES

9.1 **Production Risk.** Customer acknowledges that AI Services may occur against live, internet-facing, production or production-connected systems selected by Customer and that such activity may involve active interaction with running systems.

10. DEFINITIONS

10.1 In addition to definitions elsewhere in this Addendum, the following definitions shall apply:

Asset Discovery Services	means the AI Services used to identify, infer, import, surface, display, map, analyse, or otherwise make visible assets associated with Customer, including external, non-authenticated, authenticated, or integration-based discovery and analysis – which as of the Effective Date includes the Huginn and Muninn services within the Odin platform.
Penetration Testing Services	means the AI Services used to perform active validation, penetration testing, exploit verification, authenticated security testing, limited proof-of-concept activity, provision of Findings related thereto, and related offensive security actions permitted under this Addendum – which as of the Effective Date includes the Mjolnir service within the Odin platform.
Discovered Assets	means any access points, assets, resources, environments, components, repositories, services, or other targets identified, inferred, imported, surfaced, displayed, or otherwise made visible by or through the AI Services, whether through Asset Discovery Services, Customer submissions, Customer integrations, connected repositories, connected cloud environments, connected SaaS systems, Customer-provided credentials, uploaded materials, or other analysis performed by or through the Services. Discovered Assets may include, without limitation, root domains, subdomains, IP addresses, URLs, APIs, web applications, code repositories, cloud assets, workloads, services, environments, infrastructure components, and similar resources.
Selected Assets	means the subset of Discovered Assets, or other assets, resources, environments, repositories, integrations, credentials, applications, systems, or targets, that Customer affirmatively connects, submits, selects, enables, launches, approves, or otherwise designates for active Penetration Testing Services through the Odin platform or another Borg-approved workflow.
Excluded Assets	means any assets, resources, environments, repositories, integrations, credentials, applications, systems, or other targets that Customer marks, configures, or designates as excluded, disabled, paused, stopped, or out of scope in the Odin platform or otherwise in writing through a Borg-approved workflow.

Authorizations	means the technical and operational actions through which Customer expresses scope, authority, and instructions in relation to the AI Services, including root domain verification, repository connections, cloud tenant or service account connections, integration authorization flows, workspace settings, scope selections, exclusions, run configurations, credentials supplied by Customer, and run-launch actions.