BrowserStack Security Exhibit for Customers

Customer Security Exhibit

Please read this Security Exhibit carefully. It is part of the [INSERT NAME OF AGREEMENT] (“Agreement”) between BrowserStack and (“Customer Name”).

1.0 Information Security Program

BrowserStack agrees to implement and maintain a comprehensive written Information Security Program that shall include administrative, technical, and organizational measures, documented processes, and policies according to the current commercially reasonable industry standards to protect Customer confidential information, including personal data.

1.1 Security Policies

BrowserStack agrees to maintain documented policies or standards appropriate to maintain its Information Security Program and govern Confidential Customer Information in compliance with this Exhibit.

1.2 Security Awareness Training

BrowserStack agrees to train its employees on a no less than annual basis on BrowserStack’s Information Security Program. Such training shall, at minimum, include the following: instructions regarding the unauthorized collection, use, sharing, retention, destruction, and other inappropriate or prohibited use of Customer Confidential Information; training on BrowserStack’s security policies, including acceptable use, password protection, data classification, incident reporting, the repercussions of violations, awareness of common attack mechanisms and tips on how to identify them, and brief overviews of applicable geographical regional laws and regulations including data privacy and protection.

1.3 Personnel Security

BrowserStack agrees to and is solely responsible for conducting reasonable and necessary background checks consistent with local industry practice and compliant with applicable law for all BrowserStack Employees.

1.4 Conditions for Access

Access to BrowserStack systems containing Customer Confidential Information shall not be granted to BrowserStack's Employees, unless: (i) access is necessary to perform Services under the Agreement and access is limited to what is required to perform their job function; (ii) they are trained in the proper handling of Confidential Information under the Information Security Program in Section 1.2; (iii) they are subject to an obligation to handle Customer Confidential Information in ways at least as restrictive as those practices outlined in this Exhibit; (iv) their access can be uniquely identified (e.g., by a unique User ID), (v) they are required to use a password or other authorizing token configured to meet industry best practice standards, (vi) the date, time, requestor, and nature of the access (i.e. read-only or modify) has been recorded in a log file which is maintained and preserved according to applicable data protection law(s) and industry best practice standards and (vii) access is only granted on least privilege/need-to-know basis.

1.5 Storage

BrowserStack agrees to store Confidential Customer Information with adequate security controls following industry best practices with access to such data-limited per Section 1.4.

1.6 Segregation of Data

To the extent BrowserStack is permitted to store or retain Customer Confidential information under the Agreement, BrowserStack will logically separate and segregate data from its other clients' data, including the use of unique encryption keys where appropriate. BrowserStack may use customer Confidential Information solely to provide the Services to the Customer.

1.7 Encryption

BrowserStack agrees to (i) adopt then-current commercially reasonable industry best-practices concerning encrypting Customer Confidential Information to safeguard Customer Confidential Information in BrowserStack's systems from retrieval by unauthorized persons; (ii) transmit data over secure and encrypted connections using industry-standard encryption techniques.

1.8 Use of Single Sign-On

BrowserStack shall provide Single Sign-On (SSO) feature to the Customer as part of the Enterprise offering.

1.9 Backup

Where permitted or required by the Agreement, BrowserStack shall backup Customer Confidential Information in a secure manner and retain as per the BrowserStack's retention period or as required by applicable Data Protection Law(s). BrowserStack may use any backup of Customer Confidential Information solely to provide the Services to the Customer. BrowserStack shall not commercialize, rent, sell, monetize, distribute, manipulate, and/or otherwise use the data in any other way for itself or any third party.

1.10 Vulnerability Scans

Where applicable, BrowserStack shall run web application scans, and network vulnerability scans at least monthly.

1.11 Network Security

BrowserStack shall have appropriate Network perimeter defense solutions in place, such as Intrusion Detection System (IDS)/ Intrusion Prevention System(IPS) and firewalls to monitor, detect, and prevent malicious network activity and restrict access to authorized users and services. BrowserStack shall have appropriate monitoring in place to detect and take appropriate action. BrowserStack shall have processes to review Firewall configurations and rules at least annually, and any significant changes to firewall rules follow a documented change management process.

1.12 Secure Development

BrowserStack shall have a Software Development Lifecycle (SDLC) methodology in place that governs the acquisition, development, implementation, configuration, maintenance, modification, and management of BrowserStack's infrastructure and software components as applicable. BrowserStack agrees that before executing the Agreement, it shall have defined secure coding guidelines based on leading industry standards, and developers receive annual secure code training. BrowserStack's SDLC program shall include secure code reviews, vulnerability scanning, and security architecture reviews as appropriate.

1.13 Change Management

BrowserStack shall follow documented change management policies and procedures to request, test, and approve the application, infrastructure, and product-related changes. Changes shall be subject to review and testing before implementation or deployment. The move to production of any approved code shall be performed solely by authorized BrowserStack Employees. BrowserStack shall have separate environments for development, testing, and production.

1.14 Third-Party Risk Management

BrowserStack shall have a Third-party Risk Management Program in place to assess the operational and security risks associated with new and existing third-party vendors. BrowserStack shall communicate and ensure any third-party vendor complies with all security and confidentiality requirements under this Agreement and operational responsibilities through contractual agreements no less restrictive than those contained in this Exhibit.

1.15 Security Patches

BrowserStack agrees to install any security-related patches identified by their hardware or software vendors related to Customer Confidential Information or as required for operational and business purposes.

1.16 Auditing Key Controls, Systems, and Procedures

BrowserStack shall conduct internal and third-party security audits to ensure that the information security program's critical controls, systems, and procedures are appropriately implemented, effectively addressing the threats. The risks identified incorporate reasonable industry-standard security safeguards.

1.17 Publicly Accessible Networks

Except as restricted by applicable Data Protection Law(s), BrowserStack shall not electronically transmit (via email or otherwise) Customer Confidential Information over publicly accessible networks without using industry-standard encryption in transit.

1.18 Penetration Testing

BrowserStack shall complete penetration testing at least once annually by a recognized independent third party. BrowserStack shall provide a summary of the results of the tests upon the Customer’s request.

2.0 Assessments, Audits, and Remediation

2.1 Assessments

BrowserStack shall maintain records to demonstrate compliance with this Exhibit and then-current applicable Data Protection Law(s) and provide relevant summary reports to Customer upon request. BrowserStack shall complete any data protection questionnaire provided by the Customer within two weeks.

2.2 Remediation

BrowserStack shall correct any demonstrable security issue as agreed between both the parties, even if such problem does not rise to the level of a “Security Incident,” affecting Customer Confidential Information and customer. If action is not promptly taken to Customer’s satisfaction, Customer may terminate the Agreement and any or all Statements of Work at Customer’s discretion for a cause.

2.3 Secure Disposal

Customer Confidential Information in any form contained in shall be securely disposed and/or deleted, at Customer’s sole discretion or as per BrowserStack's data retention period whichever is earlier during the Term of the Agreement upon Customer’s written request if such information is no longer reasonably required to perform the Services. A copy of any such retained Customer Confidential Information shall be returned to Customer before disposal upon customer’s written request. When disposing of Customer Confidential Information, BrowserStack agrees to (i) destroy and/or irreversibly delete such data from any applicable media (including back-up copies) such that the media contains no residual data and (ii) Written confirmation of secure disposal/ deletion shall be provided to the Customer upon customer’s written request.

2.4 Security Incident

2.4.1 Security Incident Procedure

BrowserStack shall deploy and follow policies and procedures to detect, respond to, and otherwise address: any unauthorized disclosure of Customer Confidential Information to a third party vulnerability, breach, penetration, or other malicious activity related to Customer Confidential Information, including procedures to (i) monitor systems and detect successfully attempted attacks on or intrusions into Customer Confidential Information (ii) identify and respond to suspected or known Security Incidents, (iii) mitigate the effects and minimize any damage resulting from a Security Incident, (iv) document Security Incidents and their outcomes, and (v) restore the availability or access to Customer Confidential Information promptly. Furthermore, BrowserStack shall make all reasonable efforts to retrieve and/or prevent continued or future disclosure of Customer Confidential Information that may have been disclosed to third parties and cooperate fully with the Customer in its efforts to prevent any further disclosure.

2.4.2 Notice

In the event of an actual Security Incident, BrowserStack shall provide the Customer with prompt written notice, without undue delay and within the time frame required under applicable Data Protection Law(s) (in any case within 72 hours of becoming aware of a Security Incident). Such notice will be made to the Customer via email at **(email address)**. It shall include all available details required under applicable Data Protection Law(s), including without limitation to elements of the nature of the Security Incident (including the categories and number of individuals concerned and the categories and number of records involved), any impact to Customer SLAs or Service, any impact and consequences to Customer Confidential Information, as well as details of any remediation steps taken or planned to allow Customer to comply with its notification obligations to regulatory authorities or individuals affected by the Security Incident. BrowserStack shall provide regular updates to the Customer on the status of the Security Incident.

2.4.3 Remediation

The customer shall be notified about the response plan of the security incident. BrowserStack shall cooperate fully to investigate and remedy any harm or potential harm caused by the Security Incident. BrowserStack shall indemnify and reimburse Customer for any applicable damages, losses, fees, or costs incurred from such Security Incident if the Security Incident arises from BrowserStack's gross negligence or material omission.

3.0 Termination Obligations

3.1 Termination

Any breach of this Exhibit will be deemed a material breach under the Agreement.

3.2 Business Continuity

3.2.1 Business Continuity Plan

BrowserStack shall be responsible for establishing, implementing, testing, and maintaining an effective business continuity plan (including disaster recovery and crisis management procedures) to provide continuous access to and support solely to provide the Services to the Customer. At a minimum, BrowserStack shall: (i) back up, archive, and maintain a duplicate or redundant systems that can fully recover the Services and any data required to perform such Services daily (per Section 1.6 (Data Segregation) and 1.9 (Backup) of this Exhibit); (ii) establish and follow procedures and frequency intervals for transmitting backup data and systems to BrowserStack's backup location (per Section 1.6 (Data Segregation) and 1.9 (Backup) of this Exhibit); and (iii) demonstrate that the Services, products, and/or support capabilities can be recovered within BrowserStack's defined recovery time objective ("RTO") and recovery point objective ("RPO") timeframes.

3.2.2 BCP Test

Not less than annually following the Continuity Plan's adoption, BrowserStack shall conduct a test of the Business Continuity Plan.

4.0 Contact Information

BrowserStack shall designate a Data Privacy and Security Team. This team will: (i) maintain responsibility for applying adequate protections to Customer Confidential Information, including the development, implementation, and maintenance of its Information Security Program, (ii) oversee the application of BrowserStack compliance with the requirements of this Exhibit, and (iii) serve as a point of contact for internal communications and communications with Customer about this Exhibit and compliance with or any breaches thereof.

4.1 Sub-processors

BrowserStack shall maintain and update a record of the BrowserStack's key sub-processors that access and store Customer Confidential Information. BrowserStack's Sub-processors list is maintained at https://www.browserstack.com/sub-processors.