Security Addendum

This Security Addendum describes the administrative, technical and physical controls applicable to Samsara's storage and processing of Customer Data. This Security Addendum forms a part of Samsara's terms of service or other agreement entered into between Customer and Samsara (the "Agreement"). In the event of any conflict between this Security Addendum and the Agreement, the terms of this Security Addendum shall govern. Capitalized terms that are not defined in this Security Addendum shall have the meaning ascribed to them in the Agreement. For the avoidance of doubt, this Security Addendum does not apply to Non-Samsara Products .

1. Infrastructure and Data Segregation

1.1 Samsara's Hosted Software operates on a multitenant architecture designed to restrict access to Customer Data to only Authorized Users of the Samsara Software.

1.2 Samsara uses infrastructure provided by Amazon Web Services, Inc. ("**AWS**") to host and/or process Customer Data. AWS maintains ISO 27001, SOC 2 Type 2, and other certifications that Samsara monitors on a continuous basis.

2. Audits

2.1 Samsara performs, or retains independent third-party auditors to perform security assessments (e.g. internal audits, architecture review, etc.) on a regular basis as described in this Section 2.

2.2 No less than annually, Samsara's Hosted Software are audited by an accredited independent third-party audit firm against SOC 2 Type 2 and ISO 27001 standards.

2.3 No less than annually, Samsara's Hosted Software undergoes penetration testing from an independent third-party auditor.

2.4 Customer may access the applicable audit report(s) and penetration test summaries on Samsara's Trust Center (http://security.samsara.com), which Samsara will update no less than annually.

3. Technical Security Controls

3.1 Samsara will implement appropriate technical and organizational measures designed to safeguard Customer Personal Data from accidental or unlawful destruction, loss, alteration, and unauthorized disclosure of or access to such Customer Personal Data, including:

(a) Information Security

(i) a security incident response plan in accordance with industry standard security incident management policies and procedures.

(b) Digital Access

(i) controls and mechanisms for Endpoint (Laptop) Management which include modern anti-virus and endpoint management solutions, enforcement of laptop screen lockouts, full disk encryption, and authentication requirements for Samsara employees to access the Samsara network.

(c) Logical Access

(i) auditable Customer activity logs which allows Customer Account administrators to see changes within the Customer's environment and enforce and maintain access restrictions for their Authorized Users;

(ii) processes to allow Customer to ensure assignment of unique IDs, including specific roles and permissions, to each Authorized User;

(iii) mechanisms to allow Customer to configure user authentication and authorization (e.g., Single Sign-On and/or Multi-Factor Authentication) for Accounts created to access the Hosted Software; and

(iv) mechanisms to allow Customer administrators to configure specific retention settings for supported Customer Data types within the Samsara dashboard.

(d) Security Architecture and Design

(i) a system of firewalls configured in accordance with industry practices, using AWS services (e.g. security groups or WAF);

(ii) encryption of Customer Data using industry accepted encryption standards to protect Customer Data in transit (e.g. TLS 1.2); and at rest (e.g. AES 256); and

(iii) mechanisms to keep encryption cipher suites current as industry standards evolve specifically for encryption in transit.

(e) Cloud Host Management

(i) an infrastructure as code management program which allows management of of Samsara infrastructure at scale; and

(ii) mechanisms to keep security patches current.

(iii) procedures to determine potential vulnerabilities including scans on our production hosts no less than monthly and remediation of findings that present a measurable risk within the following time frames:

(1) high vulnerabilities have target remediations of thirty (30) days

(2) medium vulnerabilities have target remediations of ninety (90) days

(3) low vulnerabilities have target remediations of one-hundred eighty (180) days.

(f) Product Security

(i) processes to ensure a thorough review and security testing for all new Samsara Products and Product features, including functionality and design changes; and

(ii) processes to ensure the testing of any Samsara developed code which includes a scan with static analysis software and manual peer review prior to deployment to production.

(g) Bug Bounty Program

(i) operation of a Bug Bounty Program where external researchers are able to responsibly disclose potential vulnerabilities in the Samsara Products.

(h) Infrastructure Monitoring and Logging

(i) maintenance of a centralized logging environment which includes, but is not limited to security, monitoring availability, access and other activities and changes within the Samsara Hosted Software.These logs are further monitored and analyzed by the Samsara security team and anomalous events are triaged accordingly.

4. Administrative Controls

4.1 Personnel Security. Except where prohibited by applicable law, Samsara conducts background checks on all employees before employment where practicable and a generally accepted practice.

4.2 Personnel Training. Employees receive privacy and security training at the time of employee onboarding and as well as on an ongoing basis during their employment.

4.3 Personnel Agreements. All employees are required to read and sign Samsara's comprehensive information security policy covering the security, availability, and confidentiality of the Samsara Services as a part of their privacy and security training.

5. Shared Security Responsibilities

5.1 Customer acknowledges and agrees that protecting Customer Data is a shared responsibility between the Customer and Samsara.

5.2 At a minimum, Samsara will maintain certification standards such as SOC 2 and ISO 27001 and will make available a Customer Responsibility Matrix, a copy of which is available at https://security.samsara.com/resources?s=q78npzq6mxv149ewjz4qd&name=customer-responsibility-matrix-[crm] , that will define Customer's responsibilities around security controls.

6. Incident Management

6.1 Samsara will notify Customer without undue delay upon Samsara becoming aware of any Security Breach affecting Customer Personal Data. For purposes of this Security Addendum, Security Breach shall mean a security breach that Data Protection Laws would require (i) Samsara to report to Customer or (ii) Customer to report to a Supervisory Authority or affected individuals, or to maintain a record of, that involves Personal Data subject to this Security Addendum and the Agreement.

6.2 In the event of a Security Breach as described above, Samsara shall promptly take appropriate measures to address the breach, including measures to mitigate its adverse effects.

6.3 Samsara shall provide Customer timely information about the Security Breach to the extent known by Samsara, including, but not limited to details of a contact point where more

information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

7. Exclusions

For the avoidance of doubt, this Security Addendum does not apply to Non-Samsara Products.