StarTree Cloud and BYOC Security Addendum

This Security Addendum is incorporated into and made a part of the written agreement between StarTree and Customer that references this document (the “Agreement”) and any capitalized terms used but not defined herein shall have the meaning set forth in the Agreement. In the event of any conflict between the terms of the Agreement and this Security Addendum, this Security Addendum shall govern.

StarTree utilizes infrastructure-as-a-service cloud providers as further described in the Agreement and/or Documentation (each, a “Cloud Provider”) and provides the Service to Customer using a VPC/VNET and storage hosted by the applicable Cloud Provider (the “Cloud Environment”).

StarTree maintains a comprehensive documented security program under which StarTree implements and maintains physical, administrative, and technical safeguards designed to protect the confidentiality, integrity, availability, and security of the Service and Customer Data (the “Security Program”), including, but not limited to, as set forth below. StarTree regularly tests and evaluates its Security Program, and may review and update its Security Program as well as this Security Addendum, provided, however, that such updates shall be designed to enhance and not materially diminish the Security Program.

1. Hosting Location of Customer Data

1.1. Hosting Location. The hosting location of Customer Data is the production Cloud Environment in the Region offered by StarTree and selected or configured by Customer.

2. Encryption

2.1. Encryption of Customer Data. StarTree encrypts Customer Data at-rest using AES 256-bit (or better) encryption. StarTree uses Transport Layer Security (TLS) 1.2 (or better) for Customer Data in-transit over untrusted networks.

2.2. Encryption Key Management. StarTree’s encryption key management involves regular rotation of encryption keys. Hardware security modules are used to safeguard top-level encryption keys. StarTree logically separates encryption keys from Customer Data.

3. System & Network Security

3.1. Access Controls.

3.1.1. All StarTree personnel access to the Cloud Environment is via a unique user ID, consistent with the principle of least privilege, requires a VPN, as well as multi-factor authentication and passwords meeting or exceeding PCI-DSS length and complexity requirements. For data plane access, StarTree uses just-in-time access with 1 hour tokens.

3.1.2. StarTree personnel will not access Customer Data except (i) as reasonably necessary to provide services under the Agreement or (ii) to comply with the law or a binding order of a governmental body.

3.2. Endpoint Controls. For access to the Cloud Environment, StarTree personnel use StarTree-issued laptops which utilize security controls that include, but are not limited to, (i) disk encryption, (ii) endpoint detection and response (EDR) tools to monitor and alert for suspicious activities and Malicious Code (as defined below), and (iii) vulnerability management in accordance with Section 4.7.3 (Vulnerability Management).

3.3. Separation of Environments. StarTree logically separates production environments from development environments. The Cloud Environment is both logically and physically separate from StarTree's corporate offices and networks.

3.4. Firewalls / Security Groups. StarTree shall protect the Cloud Environment using either 1) industry standard firewall or security groups technology with deny-all default policies to prevent egress and ingress network traffic protocols other than those that are business-required; or 2) deny all public access to the Cloud Environment.

3.5. Hardening. The Cloud Environment shall be hardened using industry-standard practices to protect it from vulnerabilities, including by changing default passwords, removing unnecessary software, disabling or removing unnecessary services, and regular patching as described in this Security Addendum.

3.6. Monitoring & Logging.

3.6.1. Infrastructure Logs. For StarTree Cloud, not StarTree BYOC, monitoring tools or services, such as host-based intrusion detection tools, are utilized to log certain activities and changes within the Cloud Environment. These logs are further monitored, analyzed for anomalies, and are securely stored to prevent tampering for at least one year. For StarTree BYOC, Customer provided Could Environments utilize the corresponding CSP infrastructure logs.

3.6.2. User Logs. As further described in the Documentation, StarTree also captures logs of certain activities and changes within the Account and makes those logs available to Customer for Customer's preservation and analysis.

3.7. Vulnerability Detection & Management.

3.7.1. Anti-Virus & Vulnerability Detection. For StarTree Cloud, not StarTree BYOC, the Cloud Environment leverages advanced threat detection tools with daily signature updates, which are used to monitor and alert for suspicious activities, potential malware, viruses and/or malicious computer code (collectively, "Malicious Code"). StarTree does not monitor Customer Data for Malicious Code.

3.7.2. Penetration Testing & Vulnerability Detection. StarTree regularly conducts penetration tests throughout the year and engages one or more independent third parties to conduct penetration tests of the Service at least annually. StarTree also runs weekly vulnerability scans for the Cloud Environment using updated vulnerability databases.

3.7.3. Vulnerability Management. Vulnerabilities meeting defined risk criteria trigger alerts and are prioritized for remediation based on their potential impact to the Service. Upon becoming aware of such vulnerabilities, StarTree will use commercially reasonable efforts to address private and public (e.g., U.S.-Cert announced) critical and high vulnerabilities within 30 days, and medium vulnerabilities within 90 days. To assess whether a vulnerability is ‘critical’, ‘high’, or ‘medium’, StarTree leverages the National Vulnerability Database’s (NVD) Common Vulnerability Scoring System (CVSS), or where applicable, the U.S.-Cert rating.

4. Administrative Controls

4.1. Personnel Security. StarTree requires criminal background screening on its personnel as part of its hiring process, to the extent permitted by applicable law.

4.2. Personnel Training. StarTree maintains a documented security awareness and training program for its personnel, including, but not limited to, onboarding and on-going training.

4.3. Personnel Agreements. StarTree personnel are required to sign confidentiality agreements. StarTree personnel are also required to sign StarTree’s information security policy, which includes acknowledging responsibility for reporting security incidents involving Customer Data.

4.4. Personnel Access Reviews & Separation. StarTree reviews the access privileges of its personnel to the Cloud Environment at least quarterly, and removes access on a timely basis for all separated personnel.

4.5. StarTree Risk Management & Threat Assessment. StarTree’s security committee meets regularly to review reports and material changes in the threat environment, and to identify potential control deficiencies in order to make recommendations for new or improved controls and threat mitigation strategies.

4.6. External Threat Intelligence Monitoring. StarTree reviews external threat intelligence, including US-Cert vulnerability announcements and other trusted sources of vulnerability reports. U.S.-Cert announced vulnerabilities rated as critical or high are prioritized for remediation in accordance with Section 3.7.3 (Vulnerability Management).

4.7. Change Management. StarTree maintains a documented change management program for the Service.

4.8. Vendor Risk Management. StarTree maintains a vendor risk management program for vendors that process Customer Data designed to ensure each vendor maintains security measures consistent with StarTree’s obligations in this Security Addendum.

5. Physical & Environmental Controls

5.1. Cloud Environment Data Centers. To ensure the Cloud Provider has appropriate physical and environmental controls for its data centers hosting the Cloud Environment, StarTree regularly reviews those controls. Each Cloud Provider shall have a SOC 2 Type II annual audit and ISO 27001 certification, or industry recognized equivalent frameworks. Such controls, shall include, but are not limited to, the following:

5.1.1. Physical access to the facilities are controlled at building ingress points;

5.1.2. Visitors are required to present ID and are signed in;

5.1.3. Physical access to servers is managed by access control devices;

5.1.4. Physical access privileges are reviewed regularly;

5.1.5. Facilities utilize monitor and alarm response procedures;

5.1.6. Use of CCTV;

5.1.7. Fire detection and protection systems;

5.1.8. Power back-up and redundancy systems; and

5.1.9. Climate control systems.

5.2. StarTree Corporate Offices. While Customer Data is not hosted at StarTree's corporate offices, StarTree's technical, administrative, and physical controls for its corporate offices, shall include, but are not limited to, the following:

5.2.1. Physical access to the corporate office is controlled at office ingress points;

5.2.2. Badge access is required for all personnel and badge privileges are reviewed regularly;

5.2.3. Visitors are required to sign in;

5.2.4. Use of CCTV at building ingress points;

5.2.5. Tagging and inventory of StarTree-issued laptops and network assets;

5.2.6. Fire detection and sprinkler systems; and

5.2.7. Climate control systems.

6. Incident Detection & Response

6.1. Security Incident Reporting. If StarTree becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data (a "Security Incident"), StarTree shall notify Customer without undue delay, and in any case, where feasible, notify Customer within 72 hours after becoming aware. To facilitate timely notification, Customer must register and maintain an up-to-date email within the Service for this type of notification. Where no such email is registered, Customer acknowledges that the means of notification shall be at StarTree's reasonable discretion and StarTree's ability to timely notify shall be negatively impacted.

6.2. Investigation. In the event of a Security Incident as described above, StarTree shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident. Any logs determined to be relevant to a Security Incident, shall be preserved for at least one year.

6.3. Communication and Cooperation. StarTree shall provide Customer timely information about the Security Incident to the extent known to StarTree, including, but not limited to, the nature and consequences of the Security Incident, the measures taken and/or proposed by StarTree to mitigate or contain the Security Incident, the status of StarTree's investigation, a contact point from which additional information may be obtained, and the categories and approximate number of data records concerned. Notwithstanding the foregoing, Customer acknowledges that because StarTree personnel may not have visibility to the content of Customer Data, it may be unlikely that StarTree can provide information as to the particular nature of the Customer Data, or where applicable, the identities, number, or categories of affected data subjects. Communications by or on behalf of StarTree with Customer in connection with a Security Incident shall not be construed as an acknowledgment by StarTree of any fault or liability with respect to the Security Incident.

7. Deletion of Customer Data.

7.1. By Customer. The Service provides Customer controls for the deletion of Customer Data, as further described in the Documentation.

7.2. By StarTree. Subject to applicable provisions of the Agreement, upon the later of (i) expiration or termination of the Agreement and (ii) expiration of any post-termination "retrieval period" set forth in the Agreement, StarTree shall promptly delete any remaining Customer Data.

8. Customer Rights & Shared Security Responsibilities

8.1. Customer Penetration Testing. Customer may provide a written request for a copy of the latest penetration test ("Pen Test") by submitting such request via a support ticket. Pen Tests and any information arising therefrom are deemed StarTree's Confidential Information. If Customer discovers any actual or potential vulnerability in connection with a Pen Test, Customer must immediately disclose it to StarTree and shall not disclose it to any third-party.

8.3. Sensitive Customer Data. Use of the Service to meet requirements of PCI-DSS, HIPAA, FedRAMP, or similar heightened standards, require additional controls which shall be implemented by Customer, including that Customer Data subject to such requirements may only be uploaded to Editions and Regions of the Service specifically designated in the Documentation for such requirements. Additionally, Customer must implement all appropriate Customer-configurable security controls, including IP whitelisting and MFA for all User interactive logins (e.g., individuals authenticating to the Service) to protect such data.

8.4. Shared Security Responsibilities. Without diminishing StarTree's commitments in this Security Addendum, Customer agrees:

8.4.1. StarTree has no obligation to assess the content or accuracy of Customer Data, including to identify information subject to any specific legal, regulatory or other requirement and Customer is responsible for making appropriate use of the Service to ensure a level of security appropriate to the particular content of Customer Data, including, where appropriate, implementation of encryption functionality, pseudonymization of Customer Data, and configuration of the Service to back-up Customer Data;

8.4.2. Customer is responsible for managing and protecting its User roles and credentials, including but not limited to (i) ensuring that all Users keep credentials confidential and not share such information with unauthorized parties, (ii) promptly reporting to StarTree any suspicious activities related to Customer's Account (e.g., a user credential has been compromised), (iii) appropriately configuring User and role-based access controls, including scope and duration of User access, taking into account the nature of its Customer Data, and (iv) maintaining appropriate password uniqueness, length, complexity, and expiration;

8.4.3. To appropriately manage and protect any Customer-managed encryption keys and customer provided accounts to ensure the integrity, availability, and confidentiality of the key and Customer Data encrypted with such key; and

8.4.4. To promptly update its Client Software whenever StarTree announces an update;

8.4.5 If Customer experiences a security incident, Customer shall promptly inform StarTree.