Snowflake Security Addendum

This Security Addendum[1] is incorporated into and made a part of the written agreement between Snowflake 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.

Snowflake 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**").

Snowflake maintains a comprehensive documented security program based on NIST 800-53 (or industry recognized successor framework), under which Snowflake 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. Snowflake 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. Snowflake's Audits & Certifications

1.1. The information security management system used to provide the Service shall be assessed by independent third-party auditors as described in the following audits and certifications ("**Third-Party Audits**"), on at least an annual basis:

- ISO27001
- SOC 2 Type II
- SOC 1 Type II
- For Snowflake's Business Critical Edition and Virtual Private Snowflake Edition only:
  - PCI-DSS Service Provider Level 1 Certification
  - FedRAMP Moderate Authorized in certain U.S. Regions (as described in the Documentation)
  - HITRUST CSF Certification (where AWS or Microsoft are the Cloud Provider)
  - HIPAA Compliance Report for Business Associates (where Google is the Cloud Provider)

1.2. Third-Party Audits are made available to Customer as described in Section 9.2.1.

1.3. To the extent Snowflake discontinues a Third-Party Audit, Snowflake will adopt or maintain an equivalent, industry-recognized framework.

2. Hosting Location of Customer Data

2.1. Hosting Location. The hosting location of Customer Data is the production Cloud Environment in the Region offered by Snowflake and selected by Customer on an Order Form or as Customer otherwise configures via the services.

3. Encryption

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

3.2. Encryption Key Management. Snowflake's encryption key management conforms to NIST 800-53 and involves regular rotation of encryption keys. Hardware security modules are used to safeguard top-level encryption keys. Snowflake logically separates encryption keys from Customer Data.

[1] For clarity, where Customer's Agreement refers to the defined term "Security Policy", such reference shall be interpreted to refer to this exhibit.

4. System & Network Security

4.1. Access Controls. All Snowflake personnel access to the Cloud Environment is via a unique user ID and consistent with the principle of least privilege. All such access requires a VPN, with multi-factor authentication and passwords meeting or exceeding PCI-DSS length and complexity requirements.

4.2. Endpoint Controls. For access to the Cloud Environment, Snowflake personnel use Snowflake-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).

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

4.4. Firewalls / Security Groups. Snowflake shall protect the Cloud Environment using 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.

4.5. 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.

4.6. Monitoring & Logging.

4.6.1. Infrastructure Logs. 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.

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

4.7. Vulnerability Detection & Management.

4.7.1. Anti-Virus & Vulnerability Detection. 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**"). Snowflake does not monitor Customer Data for Malicious Code.

4.7.2. Penetration Testing & Vulnerability Detection. Snowflake 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. Snowflake also runs weekly vulnerability scans for the Cloud Environment using updated vulnerability databases.

4.7.3. 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, Snowflake 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', Snowflake leverages the National Vulnerability Database's (NVD) Common Vulnerability Scoring System (CVSS), or where applicable, the U.S.-Cert rating.

5. Administrative Controls

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

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

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

5.4. Personnel Access Reviews & Separation. Snowflake 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.

5.5. Snowflake Risk Management & Threat Assessment. Snowflake's risk management process is modeled on NIST 800-53 and ISO 27001. Snowflake'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.

5.6. External Threat Intelligence Monitoring. Snowflake 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 4.7.3 (Vulnerability Management).

5.7. Change Management. Snowflake maintains a documented change management program for the Service.

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

6. **Physical & Environmental Controls**

6.1. Cloud Environment Data Centers. To ensure the Cloud Provider has appropriate physical and environmental controls for its data centers hosting the Cloud Environment, Snowflake regularly reviews those controls as audited under the Cloud Provider's third-party audits and certifications. 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:

6.1.1. Physical access to the facilities are controlled at building ingress points;
6.1.2. Visitors are required to present ID and are signed in;
6.1.3. Physical access to servers is managed by access control devices;
6.1.4. Physical access privileges are reviewed regularly;
6.1.5. Facilities utilize monitor and alarm response procedures;
6.1.6. Use of CCTV;
6.1.7. Fire detection and protection systems;
6.1.8. Power back-up and redundancy systems; and
6.1.9. Climate control systems.

6.2. Snowflake Corporate Offices. While Customer Data is not hosted at Snowflake's corporate offices, Snowflake's technical, administrative, and physical controls for its corporate offices covered by its ISO 27001 certification, shall include, but are not limited to, the following:

6.2.1. Physical access to the corporate office is controlled at office ingress points;
6.2.2. Badge access is required for all personnel and badge privileges are reviewed regularly;
6.2.3. Visitors are required to sign in;
6.2.4. Use of CCTV at building ingress points;
6.2.5. Tagging and inventory of Snowflake-issued laptops and network assets;
6.2.6. Fire detection and sprinkler systems; and
6.2.7. Climate control systems.

7. Incident Detection & Response

7.1. Security Incident Reporting. If Snowflake 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**"), Snowflake shall notify Customer without undue delay, and in any case, where feasible, notify Customer within 72 hours after becoming aware.[2]

7.2. Investigation. In the event of a Security Incident as described above, Snowflake 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.

7.3. Communication and Cooperation. Snowflake shall provide Customer timely information about the Security Incident to the extent known to Snowflake, including, but not limited to, the nature and consequences of the Security Incident, the measures taken and/or proposed by Snowflake to mitigate or contain the

[2] For clarity, where Customer's Agreement refers to the defined term "Security Breach", such reference shall be interpreted to refer to Security Incident, as defined herein.

Security Incident, the status of Snowflake'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 Snowflake personnel do not have visibility to the content of Customer Data, it will be unlikely that Snowflake 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 Snowflake with Customer in connection with a Security Incident shall not be construed as an acknowledgment by Snowflake of any fault or liability with respect to the Security Incident.

8. Deletion of Customer Data.

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

8.2. By Snowflake. 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, Snowflake shall promptly delete any remaining Customer Data.

9. Customer Rights & Shared Security Responsibilities

9.1. Customer Penetration Testing. Customer may provide a written request for a penetration test of its Account ("**Pen Test**") by submitting such request via a support ticket. Following receipt by Snowflake of such request, Snowflake and Customer shall mutually agree in advance on details of such Pen Test, including the start date, scope and duration, as well as reasonable conditions designed to mitigate potential risks to confidentiality, security, or other potential disruption of the Service or Snowflake's business. Pen Tests and any information arising therefrom are deemed Snowflake's Confidential Information. If Customer discovers any actual or potential vulnerability in connection with a Pen Test, Customer must immediately disclose it to Snowflake and shall not disclose it to any third-party.

9.2. Customer Audit Rights.

9.2.1. Upon written request and at no additional cost to Customer, Snowflake shall provide Customer, or its appropriately qualified third-party representative (collectively, the "**Auditor**"), access to reasonably requested documentation evidencing Snowflake's compliance with its obligations under this Security Addendum in the form of (i) Snowflake's ISO 27001, HITRUST CSF, and PCI-DSS third-party certifications, (ii) Snowflake's SOC 1 Type II audit report, SOC 2 Type II audit report, and HIPAA Compliance Report for Business Associates, (iii) Snowflake's most recently completed industry standard security questionnaire, such as a SIG or CAIQ, and (iv) data flow diagrams for the Service (collectively with Third-Party Audits, "**Audit Reports**").

9.2.2. Customer may also send a written request for an audit (including inspection) of Snowflake's facilities. Following receipt by Snowflake of such request, Snowflake and Customer shall mutually agree in advance on the details of the audit, including reasonable start date, scope and duration of and security and confidentiality controls applicable to any such audit. Snowflake may charge a fee (rates shall be reasonable, taking into account the resources expended by Snowflake) for any such audit. Audit Reports, any audit, and any information arising therefrom are deemed Snowflake's Confidential Information.

9.2.3. Where the Auditor is a third-party (or Customer is using a third-party to conduct an approved Pen Test under Section 9.1), such third party may be required to execute a separate confidentiality agreement with Snowflake prior to any audit, Pen Test, or review of Audit Reports, and Snowflake may object in writing to such third party if in Snowflake's reasonable opinion the third party is not suitably qualified or is a direct competitor of Snowflake. Any such objection by Snowflake will require Customer to appoint another third party or conduct such audit, Pen Test, or review itself. Expenses incurred by Customer or the third party in connection with such audit, Pen Test, or review, shall be borne exclusively by Customer or the third party.

9.3. Sensitive Customer Data. Customer Data for which PCI-DSS, HIPAA, FedRAMP, or similar heightened requirements apply may only be uploaded to Editions and Regions of the Service specifically designated in the Documentation as appropriate for such data. 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.

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

9.4.1. Snowflake has no obligation to assess the content of Customer Data 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, such as the "tri-secret secure" feature (as described in the Documentation), pseudonymization of Customer Data, and configuration of the Service to back-up Customer Data;

9.4.2. to be responsible for managing and protecting its User roles and credentials, including but not limited to (i) requiring that all Users keep credentials confidential and not share such information with unauthorized parties, (ii) reporting to Snowflake any suspicious activities in the Account or if 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;

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

9.4.4. to promptly update its Client Software whenever Snowflake announces an update.