SNOWFLAKE COMPUTING, INC.
ENHANCED DATA AND SECURITY POLICY

Effective: January 1, 2016

Introduction
At Snowflake we take the protection of client data extremely seriously. This Snowflake Data and Security Policy describes the organizational and technical measures Snowflake implements platform wide designed to prevent unauthorized access, use, alteration or disclosure of customer data. The Snowflake service operates on Amazon Web Services ("AWS"); this policy describes activities of Snowflake within its instance on AWS unless otherwise specified.

I. General Security Features of the Snowflake Service
   - Regular updates of OS, applications, and database security patches
   - Firewall (security groups) configurations.
   - Managing and monitoring server accounts and server access.
   - Managing and monitoring system and application resources.
   - Logical data separation across customers.
   - Encryption of data in transit across untrusted networks and for data at rest (see below).

II. Certifications
   - Snowflake has a SOC 2 Type 1 certification. Upon request, Snowflake will provide a copy of its independent auditor’s SOC 2 Type 1 report, subject to the confidentiality provisions of customer’s service agreement with Snowflake.
   - Snowflake is currently pursuing HIPAA certification and expects this to be completed by April 1, 2016. Customers who have HIPAA Data must sign a Business Associate Agreement with Snowflake prior to loading this data into the Snowflake Service.

III. Access to Customer Data
   - Snowflake uses customer data only to provide the Snowflake service in strict accordance with each customer’s service agreement with Snowflake. Snowflake does not share or resell any customer data or information derived from customer data. Snowflake does not produce any reports or summaries based on the content of customer data.
   - Customer data is stored in Snowflake’s production environment within AWS and protected by AWS security as described at http://aws.amazon.com/security/sharing-the-security-responsibility/. Access to the production environment is restricted to a small number of Snowflake personnel who require access as part of their job functions. No other personnel access is permitted.

IV. Encryption of Customer Data
   - Customer data stored in Snowflake’s production storage environment for all customer accounts are fully encrypted using strong AES 256-bit encryption.
   - Snowflake is in the process of converting all customers to use encryption for data that is temporarily stored in Snowflake’s staging environment before copying into or out of Snowflake’s production storage environment. Staging encryption is enabled for all customers who have updated to encryption-compatible drivers. The customer can choose either 128-bit or 256-bit encryption for the staging environment.
   - In the course of standard operations, Snowflake has no visibility into encrypted customer data.
   - Customer accounts are assigned unique encryption keys to encrypt database tables and data files.

V. Notification of Security Breach
   - Snowflake will notify customer promptly in writing upon verification of a security breach of the Snowflake service. Notification will describe the breach and the status of Snowflake’s investigation.
   - Snowflake will provide commercially reasonable assistance to customer to determine whether a verified security breach of the Snowflake service affected customer data.
VI. Physical Security and Environmental Controls
   - The Snowflake service is exclusively hosted on Amazon AWS in the Oregon region. Amazon does not disclose the location of its data centers. As such, Snowflake builds on the physical security and environmental controls provided by AWS. See http://aws.amazon.com/security/ for details of AWS security infrastructure.

VII. Customer Responsibilities
   - Managing its own user accounts and roles from within the Snowflake service.
   - Protecting its own account and user credentials by using multi-factor authentication for all end-users.
   - Compliance with the terms of customer’s service agreement with Snowflake, including with respect to compliance with laws.
   - Promptly notifying Snowflake if a user credential has been compromised or if customer suspects possible suspicious activities that could negatively impact security of the Snowflake service or customer’s account.
   - Customer may not perform any security penetration tests or security assessment activities without the express advance written consent of Snowflake.