Snowflake Security Policy

This Snowflake Security Policy ("Security Policy") outlines the technical and procedural measures that Snowflake undertakes to protect Customer Data from unauthorized access or disclosure. Snowflake maintains these security measures in a manner consistent with NIST 800-53. Snowflake has a written information security plan to implement the terms of this Security Policy that is reviewed and approved annually by its senior management team.

As used in this Security Policy: "Cloud Provider" means the third-party cloud provider, such as Amazon Web Services, Inc. ("AWS") or Microsoft Corporation ("Azure") that hosts the Service; "Cloud Private Network" means the VPC and/or VNET (as applicable to the Cloud Provider) from which the Service is provided; "ESD" and "VPS" means the Enterprise-for-Sensitive Data Edition and the Virtual Private Snowflake Edition of the Service, respectively; and "Snowflake Personnel" means Snowflake employees and individual subcontractors.

This Security Policy is referenced in and made a part of your customer agreement with Snowflake (the "Agreement") and any capitalized terms used but not defined herein shall have the meaning set forth in the Agreement or Documentation, as applicable. In the event of any conflict between the terms of the Agreement and this Security Policy, this Security Policy shall govern. This Security Policy may be updated from time to time upon reasonable notice to Customer (which may be provided through the Service) to reflect process improvements or changing practices, but any such modifications will not materially diminish either party's obligations as compared to those reflected below.

1. Customer Data Access and Management
1.1 Customer controls access to its Account in the Service via User IDs and passwords.
1.2 Snowflake Personnel do not have access to unencrypted Customer Data unless Customer provides access to its Snowflake account to such Snowflake Personnel. If such access is granted, Snowflake Personnel are prohibited from storing Customer Data on local desktops, laptops, mobile devices, shared drives, removable media such as USB drives, or on public facing systems that do not fall under the administrative control or compliance monitoring processes of Snowflake.
1.3 Snowflake uses Customer Data only as necessary to provide services to Customer, as provided in the Agreement.
1.4 Customer Data is stored only in the Service production environment in the Cloud Private Network.
1.5 Customer Data is stored in the available Service Region for the account requested by Customer.
1.6 Snowflake shall create and maintain flow diagram(s) indicating how Customer Data flows through the Service ("Flow Diagrams") and shall provide Flow Diagrams upon Customer's reasonable request. Flow Diagrams are Snowflake Confidential Information.

2. Encryption and Logical Separation of Customer Data
2.1 The Service in the production storage environment always encrypts Customer Data while at rest with AES 256-bit encryption.
2.2 The Service encrypts traffic with Transport Layer Security ("TLS") 1.2 when communicating across untrusted networks such as the public internet.
2.3 The Service assigns a unique Account Master Keys ("AMK"), Tables keys, and file keys to each Account on the Service. The Service rotates the AMK and Tables keys monthly.
2.4 The AMK, Tables keys, and file keys are logically separated from Customer Data. The Service employs hardware security modules to safeguard the top-level encryption keys, which are used to key wrap its hierarchical key deployment (e.g., AMK, Tables keys, and file keys).

3. Service Infrastructure Access Management
3.1 Access to the systems and infrastructure that support the Service is restricted to Snowflake Personnel who require such access as part of their job responsibilities.
3.2 Unique User IDs are assigned to Snowflake Personnel requiring access to the Snowflake servers that support the Service.
3.3 Server password policy for the Service in the production environment adheres to the PCI-DSS password requirements.
3.4 Access privileges of separated Snowflake Personnel are disabled promptly. Access privileges of persons transferring to jobs requiring reduced privileges are adjusted accordingly.
3.5 User access to the systems and infrastructure that support the Service is reviewed quarterly.
3.6 Access attempts to the systems and infrastructure that support the Service are logged, monitored, and alerted for suspicious activities.
3.7 Cloud Provider network security groups have deny-all default policies and only enable business required network protocols for egress and ingress network traffic. The Service only allows TLS 1.2 protocol from the public internet.

4. Risk Management
4.1 Snowflake's Risk Management process is modeled on NIST 800-53 Tier 3.

4.2 Snowflake conducts risk assessments of various kinds throughout the year, including self- and third-party assessments and tests, automated scans, and manual reviews.

4.3 Results of assessments, including formal reports as relevant, are reported to the VP of Security. A Security Committee meets weekly to review reports, identify control deficiencies and material changes in the threat environment, and make recommendations for new or improved controls and threat mitigation strategies to senior management.

4.4 Changes to controls and threat mitigation strategies are evaluated and prioritized for implementation on a risk-adjusted basis.

4.5 Threats are monitored through various means, including threat intelligence services, vendor notifications, and trusted public sources.

5. Vulnerability Scanning and Penetration Testing

5.1 Vulnerability scans are automatically performed weekly on systems required to operate and manage the Service. The vulnerability database is updated regularly.

5.2 Scans that detect vulnerabilities meeting Snowflake-defined risk criteria automatically trigger notifications to security personnel.

5.3 Potential impact of vulnerabilities that trigger alerts are evaluated by staff.

5.4 Vulnerabilities that trigger alerts and have published exploits are reported to the Security Committee, which determines and supervises appropriate remediation action.

5.5 Vulnerabilities are prioritized based on potential impact to the Service, with "critical" and "high" vulnerabilities typically being addressed within 30 days of discovery and "medium" vulnerabilities being addressed within 90 days of discovery.

5.6 Security management monitors or subscribes to trusted sources of vulnerability reports and threat intelligence.

5.7 Penetration tests by an independent third party expert are conducted at least annually.

5.8 Penetration tests performed by Snowflake Security are performed regularly throughout the year.

6. Remote Access & Wireless Network

6.1 All access by Snowflake Personnel to the Cloud Private Network requires successful authentication through a secure connection via approved methods such as VPNs and enforced with mutual certificate authentication and multi-factor authentication ("MFA").

6.2 VPN access is further enforced by mutual TLS authentication.

6.3 Snowflake corporate offices, including LAN and Wi-Fi networks in those offices, are considered to be untrusted networks.

7. System Event Logging, Monitoring & Alerting

7.1 Monitoring tools and services are used to monitor systems including network, server events, and Cloud Provider API security events, availability events, and resource utilization.

7.2 Snowflake infrastructure Security event Logs are collected in a central system and protected from tampering. Logs are stored for a minimum of 12 months.

7.3 All Snowflake provided user endpoints have Endpoint Detection & Response ("EDR") tools to monitor and alert for suspicious activities and potential malware.

7.4 All Cloud Private Networks leverage advanced threat detection tools to monitor and alert for suspicious activities and potential malware.

8. System Administration and Patch Management

8.1 Snowflake shall create, implement and maintain system administration procedures for systems that access Customer Data that meet or exceed industry standards, including without limitation, system hardening, system and device patching (operating system and applications) and proper installation of threat detection software as well as daily signature updates of same.

8.2 Snowflake Security reviews US-Cert new vulnerabilities announcements weekly and assess their impact to Snowflake based on a Snowflake-defined risk criteria, including applicability and severity.

8.3 Applicable US-Cert security updates rated as "high" or "critical" are addressed within 30 days of the patch release and those rated as "medium" are addressed within 90 days of the patch release.

9. Snowflake Security Training and Snowflake Personnel

9.1 Snowflake maintains a security awareness program for Snowflake Personnel, which provides initial education, ongoing awareness and individual Snowflake Personnel acknowledgment of intent to comply with Snowflake's corporate security policies. New hires complete initial training on security, HIPAA, and PCI, sign a proprietary information agreement, and digitally sign the information security policy that covers key aspects of the Snowflake Information Security Policy.

9.2 All Snowflake Personnel acknowledge they are responsible for reporting actual or suspected security incidents or concerns, thefts, breaches, losses, and unauthorized disclosures of or access to Customer Data.

9.3 All Snowflake Personnel are required to satisfactorily complete quarterly security training.
9.4 Snowflake performs criminal background screening as part of the Snowflake hiring process, to the extent legally permissible.
9.5 Snowflake will ensure that its subcontractors, vendors, and other third parties (if any) that have direct access to the Customer Data in connection with the services adhere to data security standards consistent with NIST 800-53.

10. Physical Security
10.1 The Service is hosted with Cloud Providers and all physical security controls are managed by the Cloud Provider. Snowflake reviews the Cloud Provider's SOC 2 Type 2 report annually to ensure appropriate physical security controls, including:
    10.1.1 Visitor management including tracking and monitoring physical access.
    10.1.2 Physical access point to server locations are managed by electronic access control devices.
    10.1.3 Monitor and alarm response procedures.
    10.1.4 Use of CCTV cameras at facilities.
    10.1.5 Video capturing devices in data centers with 90 days of image retention.

11. Notification of Security Breach
11.1 A "Security Breach" is (a) the unauthorized access to or disclosure of Customer Data, or (b) the unauthorized access to the systems within the Service that transmit or analyze Customer Data.
11.2 Snowflake will notify Customer in writing within seventy-two (72) hours of a confirmed Security Breach.
11.3 Such notification will describe the Security Breach and the status of Snowflake's investigation.
11.4 Snowflake will take appropriate actions to contain, investigate, and mitigate the Security Breach.

12. Disaster Recovery & Business Continuity
12.1 Snowflake maintains a Disaster Recovery Plan ("DRP") for the Service. The DRP is tested annually.
12.2 Where AWS is the Cloud Provider, the Service is managed in different AWS Regions as standalone deployments, which can be employed as part of Customer's DRP strategy. To effectively use the AWS cross-regional availability of the Service for disaster recovery purposes, Customer is responsible for the following:
    12.2.1 Requesting additional Service accounts in different regions to support its DRP program.
    12.2.2 Managing its data replication across applicable regions.
    12.2.3 Configuring and managing its Snowflake accounts.
    12.2.4 Managing backup and restoration strategies.
12.3   Snowflake maintains a Business Continuity Plan ("BCP"). The BCP is assessed annually.

13. Snowflake Security Compliance, Certifications, and Third-party Attestations
13.1 Snowflake hires accredited third parties to perform audits and to attest to various compliance and certifications annually including:
    13.1.1 SOC 2 Type 2 Attestation Report.
    13.1.2 PCI-DSS Service Provider Level 1 Certification for ESD and VPS Editions of the Service.
    13.1.3 HIPAA Compliance Report for Business Associates for ESD and VPS Editions of the Service.
13.2 Snowflake ESD and VPS on AWS are FedRAMP Ready, for up to moderate risk impact levels.

14. Snowflake ESD and VPS Editions
14.1 Snowflake provides the ESD and VPS Editions for customers who have PCI-DSS, HIPAA, and certain other security compliance requirements. ESD and VPS features include the following:
    14.1.1 Tri-Secret Secure (where AWS is the Cloud Provider): This integration of the Service key management functions with customer-managed AWS KMS. This feature allows customers to provide part of the cipher that generates the AMK. Customer is responsible for maintaining and administering its AWS KMS.
    14.1.2 Encryption of Network Traffic: Customer Data is encrypted when transmitted inside the Cloud Private Network.

15. Customer Responsibilities
15.1 Customer acknowledges that Snowflake does not assess the contents of Customer Data and that Customer is responsible for making appropriate use of the Service to ensure a level of security appropriate to the particular nature of Customer Data, managing and protecting its accounts, roles and credentials, as well as taking appropriate steps to pseudonymize Customer Data where appropriate, and to update its Client Software whenever Snowflake announces an update.
15.2 Customer will promptly notify Snowflake if a user credential has been compromised or if Customer suspects possible suspicious activities that could negatively impact security of the Service or Customer's account.
15.3 Customer may not perform any security penetration tests or security assessment activities without the express advance written consent of Snowflake.

15.4 Customers whose Customer Data includes PCI, PHI, PII or other sensitive data must implement Snowflake-provided IP whitelisting and MFA in the Service and, to the extent Customer Data is subject to PCI-DSS, HIPAA, or FEDRAMP, Customer may only upload such data to the ESD or VPS Editions of the Service.

Updated July 2018