Snowflake Security Addendum
Snowflake 보안 부록

Last Updated: August 8, 2024
최종 수정일: 2024 년 8 월 8 일

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.
본 보안 부록[2]은 본 문서를 언급하는 Snowflake 와 고객 간의 서면 계약("**본건 계약**")에 통합되어 그 일부를 구성하며, 본 보안 부록에 사용되었으나 정의되지 않은 용어는 본건 계약에 따른 의미를 갖습니다. 본건 계약과 본 보안 부록의 조건이 상충하는 경우, 본 보안 부록이 우선합니다.

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 는 본건 계약 및/또는 관련 문서에 상세히 기재된 바와 같이 IaaS(infrastructure-as-a-service) 클라우드 제공자(각 "클라우드 제공자")를 활용하며, 해당 클라우드 제공자가 호스팅하는 VPC/VNET 및 스토리지("클라우드 환경")를 사용하여 고객에게 본건 서비스를 제공합니다.

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.
Snowflake 는 NIST 800-53(또는 업계에서 인정하는 후속 프레임워크) 기반의 문서화된 포괄적인 보안 프로그램("보안 프로그램")을 유지하며, Snowflake 는 보안 프로그램에 따라 아래 명시된 사항을 포함하되 이에 한정되지 않고 본건 서비스 및 고객 데이터의 기밀성, 무결성, 가용성 및 보안을 보호하기 위하여 설계된 물리적, 관리적 및 기술적 보호조치를 실행하고 유지합니다. Snowflake 는 보안 프로그램을 정기적으로 테스트 및 평가하고, 보안 프로그램과 본 보안 부록을 검토 및 업데이트할 수 있습니다. 단, 이러한 업데이트는 보안 프로그램을 현저하게 축소시키지 않고 강화하도록 설계되어야 합니다.

[1] For clarity, where Customer's Agreement refers to the defined term "Security Policy", such reference shall be interpreted to refer to this exhibit.
명확히 하자면, 고객 계약에서 정의된 용어인 "보안 정책"을 언급하는 경우 이는 본 부록을 언급하는 것으로 해석됩니다.

1. Snowflake's Audits & Certifications
Snowflake 의 감사 및 인증

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:
본건 서비스를 제공하기 위하여 사용되는 정보보호 관리체계는 연 1 회 이상 아래 감사 및 인증에 기재된 바와 같이 독립적인 제 3 자 감사인에 의해 평가됩니다 ("제 3 자 감사").

- ISO 27001, 27017, 27018, 9001
  ISO 27001, 27017, 27018, 9001
- SOC 2 Type II
  SOC 2 유형 II
- SOC 1 Type II
  SOC 1 유형 II
- For Snowflake's Business Critical Edition and Virtual Private Snowflake Edition only:
  Snowflake 의 비즈니스 크리티컬 에디션(Business Critical Edition) 및 버츄얼 프라이빗 Snowflake 에디션(Virtual Private Snowflake Edition)에 한하여 다음 사항이 적용됩니다:
  - PCI-DSS Service Provider Level 1 Certification
    PCI-DSS 서비스제공자 레벨 1 인증
  - FedRAMP Moderate and FedRAMP High authorizations in certain U.S. Regions (as described in the Documentation)
    특정 미국 지역에서 FedRAMP Moderate 및 FedRAMP High 인증 (관련 문서에 명시됨)
  - U.S. state government authorizations (e.g., StateRAMP or TX-RAMP) ("**State Authorizing Programs**") in certain U.S. Regions (as described in the Documentation)
    특정 미국 지역에서 미국 주 정부 인증(예: StateRAMP 또는 TX-RAMP)("**주 인증 프로그램**")(관련 문서에 명시됨)
  - HITRUST CSF Certification
    HITRUST CSF 인증
  - IRAP at the Protected Level in certain Australian Regions (as described in the Documentation)
    특정 호주 지역에서 IRAP Protected 등급(관련 문서에 명시됨)

1.2. Third-Party Audits are made available to Customer as described in Section 9.2.1.
제 9.2.1 조에 규정된 바에 따라 제 3 자 감사가 고객에게 제공됩니다.

1.3. To the extent Snowflake decides to discontinue a Third-Party Audit, Snowflake will adopt or maintain an equivalent, industry-recognized framework.
Snowflake가 어떠한 제3자 감사를 중단하기로 결정하는 경우, Snowflake는 이에 준하는 업계에서 인정하는 프레임워크를 채택 또는 유지합니다.

1.4. Information related to Snowflake-identified controls for which Customer is responsible in connection with FedRAMP, State Authorizing Programs, IRAP, and PCI-DSS is available upon written request by Customer. Customer is responsible for performing an independent assessment of its responsibilities under any of the foregoing.
고객에게 책임이 있는 FedRAMP, 주 인증 프로그램, IRAP 및 PCI-DSS 관련 Snowflake 특정 통제에 관한 정보는 고객의 서면 요청에 따라 제공됩니다. 고객은 전술한 사항에 따른 자신의 책임에 대하여 독립적인 평가를 수행할 책임이 있습니다.

2. Hosting Location of Customer Data
고객 데이터의 호스팅 위치

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.
호스팅 위치. 고객 데이터의 호스팅 위치는 Snowflake가 제안하고 고객이 주문서에서 선택하거나 고객이 달리 서비스를 통하여 설정하는 지역 내 제품 클라우드 환경(production Cloud Environment)입니다.

3. Encryption
암호화

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 to/from the Service over untrusted networks.
고객 데이터의 암호화. Snowflake는 AES 256비트(또는 그 이상) 암호화를 사용하여 저장된(at-rest) 고객 데이터를 암호화합니다. Snowflake는 신뢰할 수 없는 네트워크를 통해 본건 서비스와 주고받는 전송 중인(in-transit) 고객 데이터를 위하여 전송 계층 보안(Transport Layer Security, "TLS") 1.2(또는 그 이상)를 사용합니다.

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.

암호화 키 관리. Snowflake 의 암호화 키 관리는 NIST 800-53 에 부합하며 암호화 키는 정기적으로 교체됩니다. 하드웨어 보안 모듈은 가장 높은 수준의 암호화 키를 보호하기 위하여 사용됩니다. Snowflake 는 암호화 키를 고객 데이터와 논리적으로 분리합니다.

4. System & Network Security
시스템 및 네트워크 보안

4.1. Access Controls.
접근 제어.

4.1.1. All Snowflake 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.
클라우드 환경에 대한 모든 Snowflake 인력의 접근은 고유 사용자 ID 를 통하여 이루어지며, 최소 권한의 원칙에 부합하고, VPN 과 PCI-DSS 길이 및 복잡성 요건을 충족하거나 그 이상의 요건을 갖춘 다중 인증 및 비밀번호가 요구됩니다.

4.1.2. Snowflake personnel will not access Customer Data except (i) as reasonably necessary to provide Snowflake Offerings[2] under the Agreement or (ii) to comply with the law or a binding order of a governmental body.
Snowflake 인력은 (i) 본건 계약에 따른 Snowflake 제공 서비스 [2] 를 제공하기 위하여 합리적으로 필요하거나 (ii) 법률 또는 정부기관의 구속력 있는 명령을 준수하기 위하여 필요한 경우를 제외하고 고객 데이터에 접근하지 않습니다.

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).
엔드포인트 제어(Endpoint Control). Snowflake 인력은 클라우드 환경에 접근하기 위하여 (i) 디스크 암호화, (ii) 의심스러운 활동 및 악성코드(아래 정의됨) 모니터링 및 경고를 위한 엔드포인트 탐지 및 대응(EDR) 도구, (iii) 제 4.7.3 조(취약점 관리)에 따른 취약점 관리를 포함하되 이에 한정되지 않는 보안 통제를 활용하는 Snowflake 가 제공하는 노트북을 사용합니다.

[2] If Snowflake Offering(s) is not defined in the Agreement, "Snowflake Offering(s)" means the Service, Technical Services (including any Deliverables), and any support and other ancillary services (including, without limitation, services to prevent or address service or technical problems) provided by Snowflake.
Snowflake 제공 서비스가 본건 계약에 정의되어 있지 않은 경우, "Snowflake 제공 서비스"는 Snowflake 가 제공하는 본건 서비스, 기술 서비스(결과물 포함), 지원 및 기타 부수 서비스(서비스 또는 기술 문제를 예방하거나 해결하기 위한 서비스를 포함하되 이에 한정되지 아니합니다)를 의미합니다.

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

환경 분리. Snowflake 는 프로덕션 환경과 개발 환경을 논리적으로 분리합니다. 클라우드 환경은 Snowflake 사업장 및 네트워크와 논리적 및 물리적으로 분리되어 있습니다.

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.

방화벽/보안 그룹. Snowflake 는 업무상 필요한 경우가 아닌 네트워크 트래픽 프로토콜이 유출·유입되는 것을 방지하기 위하여 업계 표준 방화벽 또는 차단 우선 정책(deny-all default policies)의 보안 그룹 기술을 사용하여 클라우드 환경을 보호합니다.

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.

강화. 클라우드 환경은 취약점으로부터 보호될 수 있도록 기본 비밀번호 변경, 불필요한 소프트웨어 제거, 불필요한 서비스 비활성화 또는 제거, 본 보안 부록에 명시된 정기적인 패치 등을 포함한 산업 표준 관행에 따라 강화됩니다.

4.6. Monitoring & Logging.

모니터링 및 로깅.

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.

인프라 로그. 호스트 기반 침입 감지 도구 등 모니터링 도구 또는 서비스는 클라우드 환경 내 특정 활동 및 변경사항을 기록하는 데 사용됩니다. 해당 로그는 추가 모니터링과 이상 분석이 이루어지고, 최소 1 년간 위변조 방지를 위하여 안전하게 보관됩니다.

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.

사용자 로그. 관련 문서에 상세히 기재된 바와 같이, Snowflake 는 계정 내 특정 활동 및 변경 로그를 캡처하여 해당 로그를 고객의 보관 및 분석을 위하여 고객에게 제공합니다.

4.7. Vulnerability Detection & Management.
취약점 탐지 및 관리.

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.

안티 바이러스 및 취약점 탐지. 클라우드 환경은 의심스러운 활동, 잠재적인 악성코드, 바이러스 및/또는 악성 컴퓨터 코드(총칭하여 "**악성코드**")의 모니터링 및 경고에 사용되는 첨단 위협 탐지 도구(매일 시그니처 업데이트 됨)를 활용합니다. Snowflake 는 악성코드를 위해 고객 데이터를 모니터링하지 않습니다.

4.7.2. Penetration Testing & Vulnerability Detection. Snowflake regularly conducts penetration tests 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.

침투 테스트 및 취약점 탐지. Snowflake 는 침투 테스트를 실시하고 연 1 회 이상 독립적인 1 인 이상의 제 3 자를 고용하여 본건 서비스에 대한 침투 테스트를 실시합니다. 또한 Snowflake 는 업데이트된 취약점 데이터베이스를 사용하여 클라우드 환경에 대한 취약점 스캔을 매주 실시합니다.

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.

취약점 관리. 정의된 위험 기준을 충족하는 취약점에 대해서는 경고가 표시되고 본건 서비스에 미치는 잠재적 영향에 따라 우선적으로 시정됩니다. 이러한 취약점을 인지하게 되는 경우, Snowflake 는 위험 및 높음 수준의 취약점에 대해서는 30 일 이내에, 중간 수준의 취약점에 대해서는 90 일 이내에 민간 및 공공에 공지(예: U.S.-인증원(U.S.-CERT) 발표)하기 위하여 상업적으로 합리적인 노력을 기울일 것입니다. 취약점이 '위험', '높음' 또는 '중간' 수준인지 평가하기 위하여 Snowflake 는 미국 취약점 데이터베이스(National Vulnerability Database, "NVD")의 공통 취약점 등급 시스템(Common Vulnerability Scoring System, "CVSS") 또는 해당되는 경우 U.S.-인증원 등급을 활용합니다.

5. Administrative Controls
관리 통제

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.
인력 보안. Snowflake 는 관련 법률상 허용되는 범위 내에서 채용 절차의 일환으로 자사 인력에 대한 범죄경력조회를 요구합니다.

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.
인력 교육. Snowflake 는 자사 인력에 대한 입사(onboarding) 및 상시(on-going) 교육을 포함하되 이에 한정되지 않는 문서화된 보안 인식 및 교육 프로그램을 유지합니다.

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.
인력 계약. Snowflake 인력은 기밀유지계약에 서명하여야 합니다. 또한 Snowflake 인력은 고객 데이터와 관련된 보안사고 보고에 대한 책임을 확인하는 내용을 포함하는 Snowflake 의 정보보안 정책에 서명하여야 합니다.

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.
인력 접근 권한 검토 및 퇴직. Snowflake 는 최소 분기별로 인력의 클라우드 환경 접근 권한을 검토하고, 퇴직한 인력 전원의 접근 권한을 적시에 해제합니다.

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.
Snowflake 위험 관리 및 위협 평가. Snowflake 의 위험 관리 절차는 NIST 800--53 및 ISO 27001 을 기초로 한 것입니다. Snowflake 의 보안위원회는 정기적으로 회의를 개최하여 위협 환경의 중대한 변동사항과 보고 내용을 검토하고, 신규 또는 개선된 통제 및 위협 완화 전략을 권장하기 위하여 잠재적인 통제 미비점을 확인합니다.

5.6. External Threat Intelligence Monitoring. Snowflake reviews external threat intelligence, including U.S.-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).

외부 위협 정보 모니터링. Snowflake 는 U.S.-인증원의 취약점 발표내용 및 기타 신뢰할 수 있는 출처의 취약점 보고서를 포함한 외부 위협 정보를 검토합니다. U.S.-인증원에서 발표한 위험 또는 높음 등급의 취약점은 제 4.7.3 조(취약점 관리)에 따라 우선적으로 시정됩니다.

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

변경 관리. Snowflake 는 본건 서비스를 위한 문서화된 변경 관리 프로그램을 유지합니다.

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.

벤더 위험 관리. Snowflake 는 고객 데이터를 처리하는 벤더에 대하여 각 벤더가 본 보안 부록에 명시된 Snowflake 의 의무에 부합하는 보안 조치를 유지하도록 설계된 벤더 위험 관리 프로그램을 유지합니다.

6. Physical & Environmental Controls
물리적·환경적 통제

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:

클라우드 환경 데이터 센터. Snowflake 는 클라우드 제공자의 클라우드 환경을 호스팅하는 데이터 센터에 대한 적절한 물리적·환경적 통제를 보장할 수 있도록 클라우드 제공자의 제 3 자 감사 및 인증에 따라 정기적으로 해당 통제를 검토합니다. 각 클라우드 제공자는 SOC 2 유형 II 연간 감사 및 ISO 27001 인증 또는 업계에서 인정하는 이에 상응하는 프레임워크를 갖추어야 합니다. 이러한 통제는 다음을 포함하되 이에 한정되지 않습니다.

6.1.1. Physical access to the facilities are controlled at building ingress points;
건물 입구에서 시설에 대한 물리적 접근을 통제합니다.

6.1.2. Visitors are required to present ID and are signed in;
방문자에게 신분증을 제시하고 서명하도록 요구합니다.

6.1.3. Physical access to servers is managed by access control devices;
서버에 대한 물리적 접근을 접근 제어 장치로 관리합니다.

6.1.4. Physical access privileges are reviewed regularly;
물리적 접근 권한을 정기적으로 검토합니다.

6.1.5. Facilities utilize monitor and alarm response procedures;

시설은 모니터링 및 경보 대응 절차를 활용합니다.

6.1.6. Use of CCTV;
CCTV 를 사용합니다.

6.1.7. Fire detection and protection systems;
화재 감지 및 소방 시스템을 갖춥니다.

6.1.8. Power back-up and redundancy systems; and
전력 백업 및 이중화 시스템을 갖춥니다.

6.1.9. Climate control systems.
기후 제어 시스템을 갖춥니다.

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:

Snowflake 사업장. 고객 데이터는 Snowflake 의 사업장에서 호스팅되지 않으나, ISO 27001 인증 대상인 Snowflake 의 사업장에 대한 기술적, 관리적 및 물리적 통제는 다음을 포함하되 이에 한정되지 않습니다.

6.2.1. Physical access to the corporate office is controlled at office ingress points;
사업장 입구에서 사업장에 대한 물리적 접근을 통제합니다.

6.2.2. Badge access is required for all personnel and badge privileges are reviewed regularly;
모든 인력에 대해서는 배지 출입증이 요구되고, 배지 권한은 정기적으로 검토됩니다.

6.2.3. Visitors are required to sign in;
방문자에게 서명하도록 요구합니다.

6.2.4. Use of CCTV at building ingress points;
건물 입구에 CCTV 를 사용합니다.

6.2.5. Tagging and inventory of Snowflake-issued laptops and network assets;
Snowflake 가 제공하는 노트북 및 네트워크 자산을 태깅하고 목록으로 관리합니다.

6.2.6. Fire detection and sprinkler systems; and
화재 감지 및 스프링클러 시스템을 갖춥니다.

6.2.7. Climate control systems.
기후 관리 시스템을 갖춥니다.

7. Incident Detection & Response
사고 감지 및 대응

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[3]. 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 Snowflake's reasonable discretion (which may include using the Customer-designated email address associated with the OrgAdmin or AccountAdmin roles of the affected Account(s)) and Snowflake's ability to timely notify shall be negatively impacted.

보안사고 보고. Snowflake 가 우발적이거나 불법적인 고객 데이터의 파기, 분실, 변경, 무단 공개 또는 접근을 야기하는 보안 위반("**보안사고**")을 알게 되는 경우, Snowflake 는 부당한 지체 없이, 가능한 한 어떤 경우든, 알게 된 후 72 시간 이내에 고객에게 통지합니다.[3] 적시 통지가 원활하게 이루어질 수 있도록 고객은 이러한 유형의 통지를 위하여 본건 서비스에 최신 이메일을 등록하고 유지하여야 합니다. 이메일이 등록되지 않은 경우, 고객은 Snowflake 의 합리적인 재량으로 통지 수단이 결정되고 (해당 계정(들)의 OrgAdmin 또는 AccountAdmin 역할과 연동된 고객이 명시한 이메일로 전달 될 수 있습니다) Snowflake 가 적시에 통지할 수 있는 능력에 부정적인 영향이 미칠 수 있음을 인정합니다.

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.

조사. 전술한 보안사고가 발생하는 경우, Snowflake 는 보안사고를 억제, 조사 및 경감하기 위하여 신속히 합리적인 조치를 취합니다. 보안사고와 관련이 있는 것으로 판단되는 로그는 1 년 이상 보관하여야 합니다.

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 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 may not have visibility to the content of Customer Data, it may 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.

커뮤니케이션 및 협력. Snowflake 는 보안사고의 성격 및 결과, 보안사고를 경감하거나 억제하기 위하여 Snowflake 가 취하거나 제안하는 조치, Snowflake 의 조사 현황, 추가 정보를 입수할 수 있는 연락처, 관련 데이터 기록의 범주 및 대략적인 수를 포함하되 이에 한정되지 않는 Snowflake 가 알고

[3] 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.
명확히 하자면, 고객 계약에서 정의된 용어인 "보안 위반" 을 언급하는 경우 이는 본 보안부록에 정의된 보안사고를 언급하는 것으로 해석됩니다.

있는 보안사고에 대한 정보를 고객에게 적시에 제공합니다. 전술한 사항에도 불구하고, 고객은 Snowflake 인력이 고객 데이터의 내용에 대한 확인 권한이 없을 수 있으므로 Snowflake 가 고객 데이터의 특정한 성격 또는 (해당되는 경우)영향을 받은 정보주체의 신원, 수 또는 범주에 관한 정보를 제공하지 못할 수 있음을 인정합니다. 보안사고와 관련하여 Snowflake 가 직접 또는 대리인을 통해 고객과 커뮤니케이션을 하는 경우, 이는 Snowflake 가 보안사고에 관한 과실이나 책임을 인정하는 것으로 해석되지 않습니다.

8. Deletion of Customer Data.
고객 데이터 삭제.

8.1. By Customer. The Service provides Customer controls for the deletion of Customer Data, as further described in the Documentation.
고객에 의한 삭제. 본건 서비스는 관련 문서에 상세히 기재된 바와 같이 고객 데이터를 삭제할 수 있는 통제 권한을 고객에게 제공합니다.

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.
Snowflake 에 의한 삭제. 본건 계약의 관련 조항에 따라 Snowflake 는 (i) 본건 계약이 만료 또는 해지되는 시점과 (ii) 본건 계약에 명시된 해지 후 "회수 기간"이 만료되는 시점 중 나중에 도래하는 시점에 잔여 고객 데이터를 즉시 삭제합니다.

9. Customer Rights & Shared Security Responsibilities
고객 권리 및 보안 책임 공유

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.
고객 침투 테스트. 고객은 지원 티켓(support ticket)을 통하여 요청을 제출함으로써 자신의 계정에 대한 침투 테스트("침투 테스트")를 서면으로 요청할 수 있습니다. Snowflake 가 이러한 요청을 받은 후, Snowflake 와 고객은 시작일, 범위 및 기간, 그리고 과 기밀유지 및 보안에 대한 잠재적 위험 또는 본건 서비스 또는 Snowflake 의 사업에 대한 기타 잠재적 지장을 완화하기 위하여 설계된 합리적인 조건 등 침투 테스트의 세부사항에 대하여 사전에 상호 합의하여야 합니다. 침투 테스트

및 그로부터 발생하는 정보는 Snowflake 의 기밀정보로 간주됩니다. 고객이 침투 테스트와 관련하여 실제 또는 잠재적인 취약점을 발견하는 경우 이를 즉시 Snowflake 에 공개하여야 하고 제 3 자에게는 공개하지 않습니다.

9.2. Customer Audit Rights.
고객 감사권.

9.2.1. Upon written request and at no additional cost to Customer, Snowflake shall provide Customer, and/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, as applicable, (i) Snowflake's ISO 27001, 27017, and 27018, HITRUST CSF, and PCI-DSS third-party certifications; (ii) Snowflake's SOC 2 Type II audit report and SOC 1 Type II audit report; (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**").
Snowflake 는 서면 요청이 있는 경우 고객의 추가 비용 없이 고객 및/또는 적절한 자격을 갖춘 제 3 자 대리인(총칭하여 "**감사인**")에게 Snowflake 가 본 보안 부록에 따른 의무를 준수하였음을 증빙하는 합리적으로 요청된 문서에 대하여 경우에 따라 (i) Snowflake 의 ISO 27001, 27017 및 27018, HITRUST CSF 및 PCI-DSS 제 3 자 인증; (ii) Snowflake 의 SOC 2 유형 II 감사보고서 및 SOC 1 유형 II 감사보고서; (iii) SIG 또는 CAIQ 등 Snowflake 가 가장 최근에 작성한 업계 표준 보안설문지; 및 (iv) 본건 서비스에 대한 데이터 흐름도(제 3 자 감사와 함께 총칭하여 "**감사보고서**")의 형식으로 접근할 수 있는 권한을 제공합니다.

9.2.2. Customer may also send a written request for an audit of Snowflake's applicable controls, including inspection of its facilities. Following receipt by Snowflake of such request, Snowflake and Customer shall mutually agree in advance on the details of the audit, including the 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 shall be considered Snowflake's Confidential Information.
또한 고객은 Snowflake 시설 점검 등 Snowflake 의 관련 통제에 대한 감사를 서면으로 요청할 수 있습니다. Snowflake 가 이러한 요청을 받은 후, 고객과 Snowflake 는 해당 감사의 합리적인 개시일, 범위, 기간 및 해당 감사에 적용되는 보안 및 기밀 통제 등 감사의 세부사항에 대해 사전에 상호 합의합니다. Snowflake 는 그러한 감사에 대하여 수수료(Snowflake 가 사용한 자원을 고려하여 합리적인 요율이어야 함)를 부과할 수 있습니다. 감사보고서, 감사 및 그로부터 발생하는 정보는 Snowflake 의 기밀정보로 간주됩니다.

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. Any expenses incurred by an Auditor in connection with any review of Audit Reports, or an audit or Pen Test, shall be borne exclusively by the Auditor.

감사인이 제 3 자인 경우(또는 고객이 제 9.1 조에 따라 승인된 침투 테스트를 실시하기 위하여 제 3 자를 이용하는 경우), 해당 제 3 자는 감사, 침투 테스트 또는 감사보고서 검토 전에 Snowflake 와 별도의 기밀유지계약을 체결하여야 할 수 있으며, Snowflake 는 Snowflake 의 합리적인 의견에 따라 해당 제 3 자가 적절한 자격을 갖추지 못하였거나 Snowflake 의 직접적인 경쟁자인 경우 해당 제 3 자에 대하여 서면으로 이의를 제기할 수 있습니다. Snowflake 가 그와 같이 이의를 제기하는 경우, 고객은 다른 제 3 자를 선임하거나 자체적으로 해당 감사, 침투 테스트 또는 검토를 실시하여야 합니다. 감사보고서 검토, 감사 또는 침투 테스트와 관련하여 감사인에게 발생한 비용은 감사인이 전적으로 부담합니다.

9.3 Sensitive Customer Data. Use of the Service to meet requirements of PCI-DSS, HIPAA, FedRAMP, State Authorizing Programs, the International Traffic in Arms Regulations (ITAR), the Defense Federal Acquisition Regulation Supplement (DFARS), the Criminal Justice Information Services (CJIS) Security Policy, Internal Revenue Service Publication 1075 (IRS 1075) or other similar heightened standards ("**Heightened Standards**"), may require additional controls which shall be implemented by Customer. 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 Customer Data subject to such Heightened Standards. Additionally, to the extent the Documentation or the Agreement (as amended) sets forth specific requirements related to Heightened Standards (e.g., additional agreements required by Snowflake and/or requirements to use designated Editions and/or Regions of the Service), Customer must satisfy such requirements before providing Snowflake any Customer Data subject to such Heightened Standards.

민감 고객 데이터. PCI-DSS, HIPAA, FedRAMP, 주 인증 프로그램, 미국의 국제무기거래규정 (International Traffic in Arms Regulations, "ITAR"), 국방 연방 취득 규정 보완 (Defense Federal Acquisition Regulation Supplement, "DFARS"), 형사사법정보국(Criminal Justice Information Services, "CJIS")의 보안 정책, 미국 국제청 Publication 1075 (Internal Revenue Service Publication 1075, "IRS 1075") 또는 이와 유사한 수준의 강화된 기준("**강화된 기준**")의 요건을 충족하기 위한 본건 서비스의 사용은 고객이 이행하여야 하는 추가 통제를 요구할 수 있습니다. 고객은 강화된 기준의 적용을 받는 고객 데이터를 보호하기 위해 모든 사용자 인터랙티브 로그인(예: 본건 서비스에 인증한 개인)에 대하여 IP 화이트리스트 및 MFA 를 포함하여 고객이 설정할 수 있는 모든 적절한 보안 통제를 시행하여야 합니다. 또한 관련 문서 또는 본건 계약(수정본)이 강화된 기준과

관련된 특정 요구 사항(예: Snowflake 에서 요구하는 추가 계약 및/또는 지정된 버전 및/또는 본건 서비스 지역의 사용에 대한 요구 사항)을 명시하면 고객은 이러한 강화된 기준의 적용을 받는 고객 데이터를 Snowflake 에 제공하기 전에 명시된 요구 사항을 충족해야 합니다.

9.4 Shared Security Responsibilities. Without diminishing Snowflake's commitments in this Security Addendum, Customer agrees:
공동 보안 책임. 본 보안 부록에 포함된 Snowflake 의 책무를 축소하지 않고 고객은 다음 사항에 동의합니다:

9.4.1. Snowflake has no obligation to assess the content, accuracy or legality 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, 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;
Snowflake 는 특정 법률, 규제 또는 기타 요건이 적용되는 정보를 식별하는 것을 포함하여 고객 데이터의 내용, 정확성 또는 적법성을 평가할 의무가 없으며, 고객은 적절한 경우 " 3 중 비밀 보안(tri-secret secure)" 기능(관련 문서에 설명됨)과 같은 암호화 기능의 구현, 고객 데이터의 가명화 및 고객 데이터 백업을 위한 본건 서비스의 설정을 포함하여 고객 데이터의 특정 내용에 적합한 보안 수준을 보장하기 위하여 본건 서비스를 적절히 사용할 책임이 있습니다.

9.4.2. 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 Snowflake any suspicious activities related to Customer's Account (e.g., a user credential has been compromised) by submitting a support ticket and designating it as a Severity Level 1 in accordance with the Support Policy, (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, (iv) implementing all customer configurable User access controls for all User interactive logins (e.g. individuals authenticating to the Service) including IP whitelisting and MFA, and, and (v) maintaining appropriate password uniqueness, length, complexity, and expiration;
고객은 (i) 모든 사용자가 자격증명을 기밀로 유지하고 승인되지 않은 당사자와 해당 정보를 공유하지 않도록 하며, (ii) 지원 정책에 따라 지원 티켓을 제출하고 심각도 1 로 지정하여 고객 계정과 관련된 의심스러운 활동 (예: 사용자 자격증명이 손상된 경우)을 Snowflake 에 신속히 보고하고, (iii) 고객 데이터의 성격을 고려하여 사용자 접근 범위 및 기간을 포함한 사용자 및 역할 기반 접근 제어를 적절히 설정하고, (iv) 사용자 상호 작용 로그인(예: 서비스에 인증하는 개) 전체에 대해 IP 화이트리스팅 및 다중 인증(MFA)을 포함한, 고객이 설정 가능한 사용자 접근 제어를 구현하고, (v) 적절한 비밀번호 고유성, 길이, 복잡성 및 만료를 유지하는 것을 포함하되 이에 한정되지 않고 사용자 역할 및 자격증명을 관리하고 보호할 책임이 있습니다.

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
고객이 관리하는 암호화 키와 해당 키로 암호화된 고객 데이터의 무결성, 가용성 및 기밀성을 보장하기 위하여 해당 키를 적절하게 관리하고 보호합니다.

9.4.4. To promptly update its Client Software whenever Snowflake announces an update.
Snowflake 가 업데이트를 발표할 때마다 클라이언트 소프트웨어를 신속하게 업데이트합니다.