Snowflake Security Addendum
Anexo de Segurança da Snowflake

Last Updated: April 5, 2024
Última Atualização: 5 de abril de 2024

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.

Este Anexo de Segurança[1] está incorporado e faz parte do contrato por escrito entre a Snowflake e o Cliente que faz referência a este documento (o "**Contrato**"), e quaisquer termos em letras maiúsculas utilizados, mas não definidos neste documento, terão o significado estabelecido no Contrato. No caso de qualquer conflito entre os termos do Contrato e este Anexo de Segurança, este Anexo de Segurança prevalecerá.

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**").
A Snowflake utiliza provedores de nuvem de infraestrutura-como-um-serviço, conforme descrito mais detalhadamente no Contrato e/ou na Documentação (cada um, um "**Provedor de Nuvem**"), e fornece o Serviço ao Cliente usando um VPC/VNET e armazenamento hospedado pelo Provedor de Nuvem aplicável (o "**Ambiente de Nuvem**").

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.
A Snowflake mantém um programa de segurança abrangente e documentado baseado na NIST 800-53 (ou estrutura sucessora reconhecida pela indústria), sob o qual a Snowflake implementa e mantém salvaguardas físicas, administrativas e técnicas projetadas para proteger a confidencialidade, integridade, disponibilidade e segurança do Serviço e dos Dados do Cliente (o "**Programa de Segurança**"), incluindo mas não se limitando ao estabelecido abaixo. A Snowflake testa e avalia regularmente seu Programa de Segurança, e pode revisar e atualizar seu Programa de Segurança, bem como este Anexo de Segurança, desde que, entretanto, tais atualizações sejam projetadas para melhorar e não diminuir materialmente o Programa de Segurança.

1. <u>Snowflake's Audits & Certifications</u>
1. <u>Auditorias e Certificações da Snowflake</u>

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:
- ISO 27001, 27017, 27018, 9001
- SOC 2 Type II
- SOC 1 Type II
- For Snowflake's Business Critical Edition and Virtual Private Snowflake Edition only:

[1] For clarity, where Customer's Agreement refers to the defined term "Security Policy", such reference shall be interpreted to refer to this exhibit.
Para maior clareza, quando o Contrato do Cliente se referir ao termo definido "Política de Segurança", tal referência deve ser interpretada como referindo-se a este anexo.

- PCI-DSS Service Provider Level 1 Certification
- FedRAMP Moderate and FedRAMP High authorizations in certain U.S. Regions (as described in the Documentation).
- U.S. state government authorizations (e.g., StateRAMP or TX-RAMP) ("**State Authorizing Programs**") in certain U.S. Regions (as described in the Documentation)
- HITRUST CSF Certification
- IRAP at the Protected Level in certain Australian Regions (as described in the Documentation)

1.1. O sistema de gerenciamento de segurança da informação usado para fornecer o Serviço será avaliado por auditores terceirizados independentes, conforme descrito nas seguintes auditorias e certificações ("**Auditorias de Terceiros**"), pelo menos anualmente
- ISO 27001, 27017, 27018, 9001
- SOC 2 Tipo II
- SOC 1 Tipo II
- Somente para a Edição Crítica de Negócios e a Edição Virtual Privada da Snowflake
  - Certificação PCI-DSS Nível 1 de Provedor de Serviço
  - Autorizações de FedRAMP Moderado e FedRAMP High em determinadas Regiões dos Estados Unidos. (conforme descrito na Documentação)
  - Autorizações do governo estadual dos EUA (por exemplo, StateRAMP ou TX-RAMP) ("**Programas de Autorização Estaduais**") em certas regiões dos EUA (conforme descrito na Documentação) Certificação HITRUST CSF
  - IRAP no Nível Protegido em determinadas Regiões australianas (conforme descrito na Documentação)

1.2. Third-Party Audits are made available to Customer as described in Section 9.2.1.
1.2. As Auditorias de Terceiros são disponibilizadas ao Cliente conforme descrito na Seção 9.2.1.
1.3. To the extent Snowflake decides to discontinue a Third-Party Audit, Snowflake will adopt or maintain an equivalent, industry-recognized framework.
1.3. Na medida em que a Snowflake decidir descontinuar uma Auditoria de Terceiros, a Snowflake adotará ou manterá uma estrutura equivalente e reconhecida pela indústria.
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.
1.4. As informações relacionadas aos controles identificados pela Snowflake pelos quais o Cliente é responsável em conexão com FedRAMP, Programas de Autorização Estaduais, IRAP e PCI-DSS estão disponíveis mediante solicitação por escrito do Cliente. O Cliente é responsável pela realização de uma avaliação independente das suas responsabilidades sob quaisquer dos itens anteriores.

2. Hosting Location of Customer Data
2. Local de Hospedagem dos Dados do Cliente

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.
2.1. Local de Hospedagem. O local de hospedagem dos Dados do Cliente é o Ambiente de Nuvem de produção na Região oferecido pela Snowflake e selecionado pelo Cliente em um Formulário de Pedido, ou como o Cliente configurar de outra forma através dos serviços.

3. Encryption
3. Criptografia

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.

3.1. Criptografia dos Dados do Cliente. A Snowflake criptografa os Dados do Cliente em-descanso usando criptografia AES 256-bit (ou melhor). A Snowflake usa a Camada de Segurança de Transporte (TLS) 1.2 (ou melhor) para Dados de Clientes em trânsito de/para o Serviço por redes não confiáveis.

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.

3.2. Gerenciamento de Chaves de Criptografia. O gerenciamento de chaves de criptografia da Snowflake está em conformidade com a NIST 800-53 e envolve a rotação regular das chaves de criptografia. Os módulos de segurança de hardware são usados para salvaguardar chaves de criptografia de alto nível. A Snowflake separa logicamente as chaves de criptografia dos Dados do Cliente.

4. System & Network Security
4. Segurança de Sistemas e Redes

4.1. Access Controls.

4.1. Controles de Acesso.

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.

4.1.1. Todo o acesso da equipe da Snowflake ao Ambiente de Nuvem ocorre através de um ID de usuário único, consistente com o princípio do menor privilégio, requer um VPN, bem como autenticação multifatorial e senhas que atendam ou excedam os requisitos de comprimento e complexidade da PCI-DSS.

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.

4.1.2. A equipe da Snowflake não terá acesso aos Dados do Cliente exceto (i) conforme razoavelmente necessário para fornecer Ofertas da Snowflake[2] sob o Contrato ou (ii) para cumprir a lei ou uma ordem vinculante de um órgão governamental.

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).

4.2. Controles de Endpoint. Para o acesso ao Ambiente de Nuvem, a equipe da Snowflake utiliza laptops emitidos pela Snowflake que utilizam controles de segurança que incluem, mas não estão limitados a, (i) criptografia de disco; (ii) ferramentas de detecção e resposta de endpoint (EDR) para monitorar e alertar sobre atividades suspeitas e Código Malicioso (conforme definido abaixo); e (iii) gerenciamento de vulnerabilidade de acordo com a Seção 4.7.3 (Gerenciamento de Vulnerabilidade).

[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.
Se a(s) Oferta(s) da Snowflake não estiverem definidas no Contrato, "Oferta(s) da Snowflake" significa o Serviço, Serviços Técnicos (incluindo quaisquer Entregáveis) e qualquer serviço de suporte e outros serviços auxiliares (incluindo, sem limitação, serviços para prevenir ou abordar problemas de serviço ou problemas técnicos) fornecidos pela Snowflake.

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.

4.3. Separação de Ambientes. A Snowflake separa logicamente os ambientes de produção dos ambientes de desenvolvimento. O Ambiente de Nuvem é lógica e fisicamente separado dos escritórios e redes corporativas da Snowflake.

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.

4.4. Firewalls / Grupos de Segurança. A Snowflake protegerá o Ambiente de Nuvem utilizando o firewall padrão da indústria ou a tecnologia de grupos de segurança com políticas padrão de negação para evitar a entrada e saída de protocolos de tráfego de rede diferentes daqueles exigidos pelos negócios.

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.

4.5. Endurecimento. O Ambiente de Nuvem deve ser endurecido utilizando práticas padrão da indústria para protegê-lo de vulnerabilidades, inclusive mudando senhas padrão, removendo software desnecessário, desativando ou removendo serviços desnecessários, e aplicando patches regulares conforme descrito neste Anexo de Segurança.

4.6. Monitoring & Logging.

4.6. Monitoramento e Registro.

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.

4.6.1. Registros de Infraestrutura. Ferramentas ou serviços de monitoramento, tais como ferramentas de detecção de intrusão baseadas no host, são utilizadas para registrar certas atividades e mudanças dentro do Ambiente de Nuvem. Estes registros são ainda mais monitorados, analisados em busca de anomalias e armazenados com segurança para evitar adulterações por pelo menos um ano.

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.

4.6.2. Registros de Usuário. Conforme descrito mais detalhadamente na Documentação, a Snowflake também captura os registros de certas atividades e mudanças dentro da Conta, e torna esses registros disponíveis ao Cliente para preservação e análise pelo Cliente.

4.7. Vulnerability Detection & Management.

4.7. Detecção e Gerenciamento de Vulnerabilidade.

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.

4.7.1. Detecção de Antivírus e Vulnerabilidade. O Ambiente de Nuvem utiliza ferramentas avançadas de detecção de ameaças com atualizações diárias de assinaturas, que são usadas para monitorar e alertar sobre atividades suspeitas, malware, vírus e/ou códigos de computador maliciosos potenciais (conjuntamente, "**Código Malicioso**"). A Snowflake não monitora os Dados do Cliente quanto a Código Malicioso.

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.

4.7.2. Teste de Penetração e Detecção de Vulnerabilidade. A Snowflake realiza testes de penetração regularmente e contrata um ou mais terceiros independentes para realizar testes

de penetração do Serviço pelo menos anualmente. A Snowflake também executa varreduras semanais de vulnerabilidade para o Ambiente de Nuvem, utilizando bancos de dados de vulnerabilidade atualizados.

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.

4.7.3. Gestão de Vulnerabilidades. Vulnerabilidades que atendem a critérios de risco definidos disparam alertas e são priorizadas para correção com base em seu impacto potencial ao Serviço. Ao tomar conhecimento de tais vulnerabilidades, a Snowflake usará esforços comercialmente razoáveis para tratar de vulnerabilidades privadas, públicas (por exemplo, anunciadas pelo U.S.-Cert), críticas e graves no prazo de até 30 dias, e vulnerabilidades médias no prazo de até 90 dias. Para avaliar se uma vulnerabilidade é 'crítica', 'grave' ou 'média', a Snowflake utiliza o Sistema de Pontuação Comum de Vulnerabilidade (CVSS) da National Vulnerability Database (NVD) [Banco de Dados Nacional de Vulnerabilidade], ou, quando aplicável, a classificação U.S.-Cert.

5. Administrative Controls

5. Controles Administrativos

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.

5.1. Segurança da Equipe. A Snowflake exige triagem de antecedentes criminais em sua equipe como parte do seu processo de contratação, na medida permitida pela legislação aplicável.

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.

5.2. Treinamento da Equipe. A Snowflake mantém um programa documentado de conscientização e treinamento de segurança para sua equipe, incluindo, mas se não limitando a, treinamento de integração e contínuo.

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.

5.3. Contratos de Equipe. A equipe da Snowflake é obrigada a assinar termos de confidencialidade. A equipe da Snowflake também é obrigada a assinar a política de segurança de informação da Snowflake, que inclui o reconhecimento da responsabilidade de relatar incidentes de segurança envolvendo Dados do Cliente.

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.

5.4. Revisões e Separação de Acesso da Equipe. A Snowflake revisa os privilégios de acesso de sua equipe ao Ambiente de Nuvem pelo menos trimestralmente, e remove o acesso em tempo hábil para todos os funcionários separados.

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.

5.5. Gerenciamento de Risco e Avaliação de Ameaças da Snowflake. O processo de gerenciamento de risco da Snowflake é modelado na NIST 800-53 e na ISO 27001. O comitê de segurança da Snowflake se reúne regularmente para analisar relatórios e mudanças materiais no ambiente de ameaça, e para identificar possíveis deficiências de controle a fim de fazer recomendações para novos ou melhores controles e estratégias de mitigação de ameaças.

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).

5.6. Monitoramento de Inteligência de Ameaças Externas. A Snowflake analisa a inteligência de ameaças externas, incluindo anúncios de vulnerabilidade do US-Cert e outras fontes confiáveis de relatórios de vulnerabilidade. As vulnerabilidades anunciadas pelo U.S.-Cert, classificadas como críticas ou altas, são priorizadas para correção de acordo com a Seção 4.7.3 (Gerenciamento de Vulnerabilidades).

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

5.7. Gerenciamento de Mudanças. A Snowflake mantém um programa documentado de gerenciamento de mudanças para o Serviço.

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.

5.8. Gerenciamento de Risco do Fornecedor. A Snowflake mantém um programa de gerenciamento de risco de fornecedores para fornecedores que tratam Dados de Clientes, projetado para garantir que cada fornecedor mantenha medidas de segurança consistentes com as obrigações da Snowflake sob este Anexo de Segurança.

6. **Physical & Environmental Controls**

6. **Controles Físicos e Ambientais**

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. Centros de Dados dos Ambiente de Nuvem. Para garantir que o Provedor de Nuvem tenha controles físicos e ambientais adequados para seus centros de dados que hospedam o Ambiente de Nuvem, a Snowflake revisa regularmente esses controles conforme auditados de acordo com as auditorias e certificações de terceiros do Provedor de Nuvem. Cada Provedor de Nuvem deve ter uma auditoria anual SOC 2 Tipo II e certificação ISO 27001, ou estruturas equivalentes reconhecidas pela indústria. Tais controles incluem mas não se limitam ao seguinte:

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

6.1.1. O acesso físico às instalações é controlado nos pontos de entrada do edifício;

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

6.1.2. Os visitantes são obrigados a apresentar documento de identificação e fornecem sua assinatura;

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

6.1.3. O acesso físico aos servidores é gerenciado por dispositivos de controle de acesso;

6.1.4. Physical access privileges are reviewed regularly;

6.1.4. Os privilégios de acesso físico são revisados regularmente;

6.1.5. Facilities utilize monitor and alarm response procedures;

6.1.5. As instalações utilizam procedimentos de monitoramento e resposta a alarmes;

6.1.6. Use of CCTV;

6.1.6. Uso de CCTV [Televisão de Circuito Fechado];

6.1.7. Fire detection and protection systems;

6.1.7. Sistemas de detecção e proteção contra incêndios;

6.1.8. Power back-up and redundancy systems; and

6.1.8. Sistemas de backup de energia e redundância; e

6.1.9. Climate control systems.

6.1.9. Sistemas de controle climático.

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. Escritórios Corporativos da Snowflake. Embora os Dados do Cliente não sejam hospedados nos escritórios corporativos da Snowflake, os controles técnicos, administrativos e físicos da Snowflake para seus escritórios corporativos cobertos por sua certificação ISO 27001 deverão incluir mas não estão limitados ao seguinte:

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

6.2.1. O acesso físico ao escritório corporativo é controlado nos pontos de entrada do escritório;

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

6.2.2. O acesso por crachá é necessário para toda a equipe e os privilégios do crachá são revisados regularmente;

6.2.3. Visitors are required to sign in;

6.2.3. Os visitantes são obrigados a fornecer assinatura;

6.2.4. Use of CCTV at building ingress points;

6.2.4. Uso de CCTV nos pontos de entrada dos edifícios;

6.2.5. Tagging and inventory of Snowflake-issued laptops and network assets;

6.2.5. Etiquetagem e inventário dos laptops e ativos de rede emitidos pela Snowflake;

6.2.6. Fire detection and sprinkler systems; and

6.2.6. Sistemas de detecção de incêndio e extintores; e

6.2.7. Climate control systems.

6.2.7. Sistemas de controle climático.

7. Incident Detection & Response

7. Detecção e Resposta a Incidentes

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.

7.1. Relato de Incidentes de Segurança. Se a Snowflake tomar conhecimento de uma violação de segurança que leve à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso aos Dados do Cliente (um "**Incidente de Segurança**"), a Snowflake notificará o Cliente sem atraso indevido e, em qualquer caso, quando possível, notificará o Cliente dentro de 72 horas após tomar conhecimento[3]. Para facilitar a notificação em tempo hábil, o Cliente deve se cadastrar e manter um e-mail atualizado dentro do Serviço para este tipo de notificação. Quando nenhum e-mail for registrado, o Cliente reconhece que o meio de notificação ficará a critério razoável da Snowflake (que pode incluir o uso do endereço de e-mail designado pelo Cliente associado às funções OrgAdmin ou AccountAdmin da(s) Conta(s) afetada(s)) e a capacidade da Snowflake de notificar em tempo hábil será prejudicada.

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.

7.2. Investigação. No caso de um Incidente de Segurança conforme descrito acima, a Snowflake deverá prontamente tomar medidas razoáveis para conter, investigar e mitigar qualquer Incidente

[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.
Para maior clareza, quando o Contrato do Cliente se referir ao termo definido "Violação de Segurança", tal referência deve ser interpretada para se referir ao Incidente de Segurança, conforme definido neste documento.

de Segurança. Quaisquer registros determinados como sendo relevantes a um Incidente de Segurança devem ser preservados por pelo menos um ano.

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.

7.3. Comunicação e Cooperação. A Snowflake deverá fornecer ao Cliente informações tempestivas sobre o Incidente de Segurança na medida do conhecimento da Snowflake, incluindo mas não se limitando à natureza e às consequências do Incidente de Segurança, as medidas tomadas e/ou propostas pela Snowflake para mitigar ou conter o Incidente de Segurança, a situação da investigação da Snowflake, um ponto de contato do qual informações adicionais podem ser obtidas, e as categorias e o número aproximado de registros de dados em questão. Não obstante o exposto, o Cliente reconhece que, como a equipe da Snowflake pode não ter visibilidade do conteúdo dos Dados do Cliente, pode ser improvável que a Snowflake possa fornecer informações sobre a natureza particular dos Dados do Cliente, ou, quando aplicável, as identidades, número ou categorias dos titulares dos dados afetados. As comunicações por ou em nome da Snowflake com o Cliente em relação a um Incidente de Segurança não serão interpretadas como um reconhecimento pela Snowflake de qualquer falha ou responsabilidade com relação ao Incidente de Segurança.

8. Deletion of Customer Data.

8. Eliminação dos Dados do Cliente.

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

8.1. Pelo Cliente. O Serviço fornece controles do Cliente para a eliminação dos Dados do Cliente, conforme descrito mais detalhadamente na Documentação.

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.

8.2. Pela Snowflake. Sujeito às disposições aplicáveis do Contrato, após (i) a expiração ou rescisão do Contrato e (ii) a expiração de qualquer “período de recuperação” pós-rescisão estabelecido no Contrato, a Snowflake deverá eliminar imediatamente quaisquer Dados do Cliente restantes.

9. Customer Rights & Shared Security Responsibilities

9. Direitos do Cliente e Responsabilidades de Segurança Compartilhadas

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.

9.1. Teste de Penetração do Cliente. O Cliente pode fornecer uma solicitação por escrito para um teste de penetração da sua Conta (“**Teste de Penetração**”), submetendo tal solicitação através de um requerimento de suporte. Após o recebimento de tal solicitação pela Snowflake, a Snowflake e o Cliente acordarão previamente os detalhes de tal Teste de Penetração, incluindo

a data de início, o escopo e a duração, bem como condições razoáveis projetadas para mitigar riscos potenciais à confidencialidade, segurança ou outras possíveis perturbações do Serviço ou dos negócios da Snowflake. Os Testes de Penetração e quaisquer informações que deles surjam são considerados Informações Confidenciais da Snowflake. Se o Cliente descobrir qualquer vulnerabilidade real ou potencial em conexão com um Teste de Penetração, o Cliente deverá revelá-la imediatamente à Snowflake e não deverá revelá-la a nenhum terceiro.

9.2. Customer Audit Rights.

9.2. Direitos de Auditoria do Cliente.

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**").

9.2.1. Mediante solicitação por escrito e sem custos adicionais para o Cliente, a Snowflake deverá fornecer ao Cliente e/ou ao seu representante terceirizado devidamente qualificado (conjuntamente, o "**Auditor**"), acesso à documentação razoavelmente solicitada que comprove o cumprimento das obrigações da Snowflake sob este Anexo de Segurança na forma de, conforme aplicável, (i) certificações de terceiros ISO 27001, 27017 e 27018, HITRUST CSF e PCI-DSS da Snowflake, (ii) relatórios de auditoria SOC 2 Tipo II e SOC 1 Tipo II, (iii) o questionário de segurança padrão da indústria mais recentemente preenchido pela Snowflake, como um SIG ou CAIQ, e (iv) diagramas de fluxo de dados para o Serviço (conjuntamente com Auditorias de Terceiros, "**Relatórios de Auditoria**").

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.

9.2.2. O Cliente também pode enviar uma solicitação por escrito para uma auditoria dos controles aplicáveis da Snowflake, incluindo a inspeção das suas instalações. Após o recebimento de tal solicitação pela Snowflake, a Snowflake e o Cliente acordarão previamente os detalhes da auditoria, incluindo a data de início, o escopo e a duração razoáveis e os controles de segurança e confidencialidade aplicáveis a tal auditoria. A Snowflake poderá cobrar uma taxa (as taxas devem ser razoáveis, levando em conta os recursos gastos pela Snowflake) por tal auditoria. Relatórios de Auditoria, qualquer auditoria e qualquer informação que dela resulte serão considerados Informações Confidenciais da Snowflake.

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.

9.2.3. Quando o Auditor for um terceiro (ou o Cliente estiver usando um terceiro para conduzir um Teste de Penetração aprovado de acordo com a Seção 9.1), tal terceiro poderá ser obrigado a celebrar um termo de confidencialidade separado com a Snowflake antes de qualquer auditoria, Teste de Penetração, ou revisão de Relatórios de Auditoria, e a Snowflake poderá se opor por escrito a tal terceiro se, na opinião razoável da Snowflake, o terceiro não for

devidamente qualificado ou for um concorrente direto da Snowflake. Qualquer oposição nesse sentido por parte da Snowflake exigirá que o Cliente nomeie outro terceiro ou realize tal auditoria, Teste de Penetração, ou a própria revisão. Quaisquer despesas incorridas por um Auditor em conexão com qualquer revisão de Relatórios de Auditoria, ou uma auditoria ou Teste de Penetração, serão arcadas exclusivamente pelo Auditor.

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.

9.3. Dados Sensíveis de Clientes. O uso do Serviço para atender aos requisitos de PCI-DSS, HIPAA, FedRAMP, dos Programas de Autorização Estaduais, dos Regulamentos sobre o Tráfico Internacional de Armas (International Traffic in Arms Regulations ITAR), do Suplemento de Regulamentação de Aquisição Federal de Defesa (Defense Federal Acquisition Regulation Supplement - DFARS), da Política de Segurança dos Serviços de Informação de Justiça Criminal (Criminal Justice Information Services - CJIS), da Publicação da Receita Federal 1075 (Internal Revenue Service Publication 1075 - IRS 1075) ou de outros padrões elevados similares ("**Padrões Elevados**") pode exigir controles adicionais que devem ser implementados pelo Cliente. O Cliente deve implementar todos os controles de segurança configuráveis pelo Cliente, incluindo uma lista branca de IP e MFA para todos os logins interativos do Usuário (por exemplo, indivíduos que se autenticam no Serviço) para proteger os Dados do Cliente sujeitos a tais Padrões Elevados. Além disso, na medida em que a Documentação ou o Contrato (conforme alterado) estabeleça requisitos específicos relacionados a Padrões Elevados (por exemplo, contratos adicionais exigidos pelo Snowflake e/ou requisitos para usar Edições e/ou Regiões designadas do Serviço), o Cliente deve satisfazer tais requisitos antes de fornecer à Snowflake quaisquer Dados do Cliente sujeitos a tais Padrões Elevados.

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

9.4. Responsabilidades Compartilhadas de Segurança. Sem diminuir os compromissos da Snowflake neste Anexo de Segurança, o Cliente concorda que:

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;

9.4.1. A Snowflake não tem obrigação de avaliar o conteúdo, a precisão ou a licitude dos Dados do Cliente, incluindo a identificação de informações sujeitas a qualquer requisito legal, regulatório ou outro, e o Cliente é responsável por fazer uso apropriado do Serviço para garantir um nível de segurança apropriado ao conteúdo específico dos Dados do Cliente, incluindo, quando apropriado, a implementação da funcionalidade de criptografia, como o recurso "tri-secret cecure" (conforme descrito na Documentação), pseudonimização dos Dados do Cliente e configuração do Serviço para fazer backup dos Dados do Cliente;

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, and (iv) maintaining appropriate password uniqueness, length, complexity, and expiration;

9.4.2. O Cliente é responsável por gerenciar e proteger suas funções e credenciais de Usuário, incluindo mas não se limitando a (i) assegurar que todos os Usuários mantenham as credenciais confidenciais e não compartilhem tais informações com partes não autorizadas, (ii) informar prontamente à Snowflake quaisquer atividades suspeitas relacionadas à Conta do Cliente (por exemplo, caso uma credencial de usuário tenha sido comprometida) por meio do envio de um requerimento de suporte, designando-a como Nível de Gravidade 1 de acordo com a Política de Suporte, (iii) configurar adequadamente os controles de acesso baseados em Usuários e funções, incluindo o escopo e a duração do acesso do Usuário, levando em conta a natureza dos seus Dados de Cliente, e (iv) manter a singularidade, comprimento, complexidade e expiração apropriados da senha;

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

9.4.3. gerenciar e proteger adequadamente qualquer chave de criptografia gerenciada pelo Cliente para garantir a integridade, disponibilidade e confidencialidade da chave e dos Dados do Cliente criptografados com tal chave; e

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

9.4.4. atualizar prontamente seu Software de Cliente sempre que a Snowflake anunciar uma atualização.