Snowflake Security Addendum
Adendum Keamanan Snowflake

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. The language of this Agreement is English and Bahasa. In the event of a conflict between the English and Bahasa text, the English shall govern.
*Adendum Keamanan ini[1] dibuat dan merupakan bagian dari perjanjian tertulis antara Snowflake dan Pelanggan yang merujuk pada dokumen ini ("**Perjanjian**") dan setiap istilah dengan huruf kapital yang digunakan namun tidak didefinisikan di Adendum Keamanan ini akan memiliki pengertian yang sama seperti yang ditetapkan dalam Perjanjian. Jika terjadi pertentangan antara ketentuan Perjanjian dan Adendum Keamanan ini, maka Adendum Keamanan ini yang akan berlaku. Bahasa pada Perjanjian ini adalah Bahasa Inggris dan Bahasa Indonesia. Dalam hal terjadi pertentangan antara teks Bahasa Inggris dan Bahasa Indonesia, maka Bahasa Inggris yang akan berlaku.*

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 menggunakan penyedia layanan cloud infrastruktur-sebagai-layanan sebagaimana dijelaskan lebih lanjut di dalam Perjanjian dan/atau Dokumentasi (masing-masing, disebut "**Penyedia Cloud**") dan menyediakan Layanan kepada Pelanggan dengan menggunakan VPC/VNET dan penyimpanan yang dihosting oleh Penyedia Cloud yang berlaku ("**Lingkungan Cloud**").*

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 memelihara program keamanan terdokumentasi yang komprehensif berdasarkan NIST 800-53 (atau kerangka kerja penggantinya yang diakui industri), yang berdasarkan mana Snowflake melaksanakan dan memelihara perlindungan secara fisik, administratif dan teknis yang dirancang untuk melindungi kerahasiaan, integritas, ketersediaan dan keamanan Layanan dan Data Pelanggan ("**Program Keamanan**"), termasuk, namun tidak terbatas pada, sebagaimana ditetapkan di bawah ini. Snowflake secara teratur menguji dan mengevaluasi Program Keamanannya, dan dapat meninjau dan memperbarui Program Keamanannya serta Adendum Keamanan ini, dengan ketentuan bahwa pembaruan tersebut harus dirancang untuk meningkatkan dan tidak mengurangi Program Keamanan secara material.*

1. Snowflake's Audits & Certifications
1. Audit dan Sertifikasi Snowflake

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:
*1.1. Sistem manajemen perlindungan informasi yang digunakan untuk menyediakan Layanan akan dinilai oleh auditor pihak ketiga independen sebagaimana dijelaskan dalam audit dan sertifikasi berikut ini ("**Audit Pihak Ketiga**"), setidaknya atas dasar tahunan:*

- ISO27001
- *ISO27001*

- SOC 2 Type II

[1] For clarity, where Customer's Agreement refers to the defined term "Security Policy", such reference shall be interpreted to refer to this exhibit.
[1] *Untuk kejelasan, ketika Perjanjian Pelanggan merujuk pada ketentuan yang didefinisikan "Kebijakan Keamanan", rujukan tersebut harus ditafsirkan untuk merujuk pada eksibit ini.*

- *o* *SOC 2 Tipe II*

- o SOC 1 Type II
- *o* *SOC 1 Tipe II*

- o For Snowflake's Business Critical Edition and Virtual Private Snowflake Edition only:
- *o* *Hanya untuk Edisi Kritis Usaha Snowflake dan Edisi Snowflake Pribadi Virtual:*

  - PCI-DSS Service Provider Level 1 Certification
  - *Sertifikasi Tingkat 1 Penyedia Layanan PCI-DSS*

  - FedRAMP Moderate Authorized in certain U.S. Regions (as described in the Documentation)
  - *FedRAMP Moderate Authorized di Wilayah A.S. tertentu (sebagaimana dijelaskan di dalam Dokumentasi)*

  - HITRUST CSF Certification (where AWS or Microsoft are the Cloud Provider)
  - *Sertifikasi HITRUST CSF (dimana AWS atau Microsoft merupakan Penyedia Cloud)*

  - IRAP at the Protected Level in certain Australian Regions (as described in the Documentation)
  - *IRAP pada Tingkat Yang Dilindungi di Wilayah Australia tertentu (seperti yang dijelaskan dalam Dokumentasi)*

  - HIPAA Compliance Report for Business Associates (where Google is the Cloud Provider)
  - *Laporan Kepatuhan HIPAA untuk Rekan Usaha (dimana Google merupakan Penyedia Cloud)*

1.2. Third-Party Audits are made available to Customer as described in Section 9.2.1.
1.2. Audit Pihak Ketiga disediakan untuk Pelanggan sebagaimana dijelaskan dalam Bagian 9.2.1.

1.3. To the extent Snowflake discontinues a Third-Party Audit, Snowflake will adopt or maintain an equivalent, industry-recognized framework.
1.3. Sepanjang Snowflake memutuskan untuk menghentikan Audit Pihak Ketiga, Snowflake akan memakai atau mempertahankan kerangka kerja yang setara dan diakui industri.
1.4 Information related to Snowflake-identified controls for which Customer is responsible in connection with FedRAMP, 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 Informasi terkait kontrol yang diidentifikasi Snowflake untuk mana Pelanggan bertanggung jawab sehubungan dengan FedRAMP, IRAP, dan PCI-DSS tersedia berdasarkan permintaan tertulis oleh Pelanggan. Pelanggan bertanggung jawab untuk melaksanakan suatu penilaian independen atas tanggung jawabnya berdasarkan hal-hal manapun tersebut.

2. Hosting Location of Customer Data
2. Lokasi Hosting Data Pelanggan

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. Lokasi Hosting. Lokasi hosting Data Pelanggan adalah pembuatan Lingkungan Cloud di dalam Wilayah yang ditawarkan oleh Snowflake dan dipilih oleh Pelanggan pada Formulir Pemesanan atau sebagaimana yang dikonfigurasi Pelanggan melalui layanan.

3. Encryption
3. Enkripsi

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

3.1. *Enkripsi Data Pelanggan. Snowflake mengenkripsi Data Pelanggan at-rest dengan menggunakan enkripsi AES 256-bit (atau lebih baik). Snowflake menggunakan Transport Layer Security (TLS) 1.2 (atau lebih baik) untuk Data Pelanggan dalam persinggahan melalui jaringan yang tidak tepercaya.*

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. *Manajemen Kunci Enkripsi. Manajemen kunci enkripsi Snowflake sesuai dengan NIST 800-53 dan melibatkan rotasi reguler dari kunci enkripsi. Modul keamanan piranti keras digunakan untuk melindungi kunci enkripsi tingkat atas. Snowflake secara logis memisahkan kunci enkripsi dari Data Pelanggan.*

4. System & Network Security
4. Keamanan Sistem & Jaringan

4.1. Access Controls.

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

4.1.1 *Pengendalian Akses. Seluruh akses personel Snowflake ke Lingkungan Cloud adalah melalui identitas pengguna yang unik dan konsisten dengan prinsip hak istimewa yang minim. Seluruh akses tersebut memerlukan VPN dengan otentikasi multi-faktor dan kata sandi yang memenuhi atau melebihi persyaratan panjang dan kompleksitas 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. *Personel Snowflake tidak akan mengakses Data Pelanggan kecuali (i) sebagaimana diperlukan secara wajar untuk menyediakan Penawaran Snowflake[2] berdasarkan Perjanjian atau (ii) untuk mematuhi hukum atau perintah yang mengikat dari badan pemerintah.*

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. *Pengendalian Titik Akhir. Untuk mengakses Lingkungan Cloud, personel Snowflake menggunakan laptop yang dikeluarkan oleh Snowflake yang memiliki pengendalian keamanan yang mencakup, namun tidak terbatas pada, (i) enkripsi cakram, (ii) alat deteksi dan tanggapan titik akhir (EDR) untuk memantau dan memperingatkan aktivitas mencurigakan dan Kode Berbahaya (sebagaimana didefinisikan di bawah), dan (iii) manajemen kerentanan sesuai dengan Bagian 4.7.3 (Manajemen Kerentanan).*

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

4.3. *Pemisahan Lingkungan. Snowflake secara logis memisahkan lingkungan produksi dari lingkungan pengembangan. Lingkungan Cloud secara logis dan secara fisik terpisah dari kantor dan jaringan perusahaan Snowflake.*

---

[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.

[2] *Apabila Penawaran Snowflake tidak didefinisikan di dalam Perjanjian, "Penawaran Snowflake" berarti Layanan, Layanan Teknis (termasuk setiap Hasil Kerja), dan setiap layanan dukungan dan tambahan (termasuk, tanpa terbatas, layanan untuk mencegah atau mengatasi permasalahan layanan atau teknis) yang diberikan oleh 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. Firewall/Grup Keamanan. Snowflake harus melindungi Lingkungan Cloud dengan menggunakan firewall standar industri atau teknologi grup keamanan dengan kebijakan bawaan yaitu menolak semua untuk mencegah protokol lalu lintas jaringan keluar dan masuk selain yang diperlukan oleh usaha.

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. Pengetatan. Lingkungan Cloud akan diperketat dengan menggunakan praktik berstandar industri untuk melindunginya dari kerentanan, termasuk dengan mengubah kata sandi bawaan, menghapus piranti lunak yang tidak perlu, menonaktifkan atau menghapus layanan yang tidak perlu, dan patching reguler seperti yang dijelaskan dalam Adendum Keamanan ini.

4.6. Monitoring & Logging.

4.6. Pemantauan & Pencatatan

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. Catatan Infrastruktur. Alat atau layanan pemantauan, seperti alat deteksi intrusi berbasis host, digunakan untuk mencatat aktivitas dan perubahan tertentu dalam Lingkungan Cloud. Catatan ini dipantau lebih lanjut, dianalisis untuk menemukan anomali, dan disimpan dengan aman untuk mencegah gangguan setidaknya selama satu tahun.

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. Catatan Pengguna. Sebagaimana dijelaskan lebih lanjut dalam Dokumentasi, Snowflake juga menangkap catatan dari aktivitas dan perubahan tertentu dalam Akun dan menyediakan catatan tersebut kepada Pelanggan untuk disimpan dan dianalisis oleh Pelanggan.

4.7. Vulnerability Detection & Management.

4.7. Deteksi & Manajemen Kerentanan.

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. Anti-Virus & Deteksi Kerentanan. Lingkungan Cloud memanfaatkan alat pendeteksi ancaman tingkat lanjut dengan pembaruan tanda tangan sehari-hari, yang digunakan untuk memantau dan memperingatkan aktivitas mencurigakan, potensi malware, virus, dan/atau kode komputer berbahaya (secara bersama-sama, disebut "**Kode Berbahaya**"). Snowflake tidak memantau Data Pelanggan untuk Kode Berbahaya.*

4.7.2. Penetration Testing & Vulnerability Detection. Snowflake regularly conducts penetration tests throughout the year and engages one or more independent third parties to conduct penetration tests of the Service at least annually. Snowflake also runs weekly vulnerability scans for the Cloud Environment using updated vulnerability databases.

4.7.2. Pengujian Penyusupan & Deteksi Kerentanan. Snowflake secara teratur melakukan pengujian penyusupan sepanjang tahun dan melibatkan satu atau lebih pihak ketiga independen untuk melakukan pengujian penyusupan atas Layanan setidaknya setiap tahun. Snowflake juga menjalankan pemindaian kerentanan mingguan untuk Lingkungan Cloud dengan menggunakan database kerentanan yang diperbarui.

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. *Manajemen Kerentanan. Kerentanan yang memenuhi kriteria risiko yang ditentukan memicu peringatan dan diprioritaskan untuk perbaikan berdasarkan potensi dampaknya terhadap Layanan. Setelah menyadari kerentanan tersebut, Snowflake akan menggunakan upaya yang wajar secara komersial untuk mengatasi kerentanan kritis dan tinggi yang bersifat pribadi dan publik (misalnya, U.S.-Cert yang diumumkan) dalam waktu 30 hari, dan kerentanan sedang dalam waktu 90 hari. Untuk menilai apakah kerentanan tersebut bersifat 'kritis', 'tinggi', atau 'sedang', Snowflakes memanfaatkan Common Vulnerability Scoring System (CVSS) dari Database Kerentanan Nasional (NVD), atau jika berlaku, peringkat U.S.-Cert.*

5. Administrative Controls
5. Pengendalian Administratif

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. *Keamanan Personel. Snowflake mewajibkan pemeriksaan latar belakang kriminal pada personelnya sebagai bagian dari proses perekrutannya, sejauh diizinkan oleh hukum yang berlaku.*

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. *Pelatihan Personel. Snowflake mempertahankan kewaspadaannya terhadap keamanan dan program pelatihan bagi personelnya yang terdokumentasi, termasuk, namun tidak terbatas pada, pelatihan orientasi dan pelatihan yang sedang berlangsung.*

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. *Perjanjian Dengan Personel. Personel Snowflake diharuskan menandatangani perjanjian kerahasiaan. Personel Snowflake juga diwajibkan untuk menandatangani kebijakan perlindungan informasi Snowflake, yang mencakup tanggung jawab untuk melaporkan insiden keamanan yang melibatkan Data Pelanggan.*

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. *Peninjauan & Pemisahan Akses Personel. Snowflake meninjau hak istimewa atas akses personelnya ke Lingkungan Cloud setidaknya setiap triwulanan, dan menghapus akses secara tepat waktu untuk semua personel yang terpisah.*

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. *Manajemen Risiko & Penilaian Ancaman Snowflake. Proses manajemen risiko Snowflake mengikuti NIST 80053 dan ISO 27001. Komite keamanan Snowflake bertemu secara teratur untuk meninjau laporan dan perubahan material di dalam lingkungan ancaman, dan untuk mengidentifikasi potensi kekurangan pengendalian untuk membuat rekomendasi untuk pengendalian baru atau peningkatan pengendalian dan strategi untuk mengurangi ancaman.*

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. *Pemantauan Intelijen Ancaman Eksternal. Snowflake meninjau intelijen ancaman eksternal, termasuk pengumuman kerentanan US-Cert dan sumber laporan kerentanan tepercaya lainnya.*

Kerentanan yang dinilai sebagai kritis atau tinggi, yang diumumkan oleh U.S.Cert, diprioritaskan untuk perbaikan sesuai dengan Bagian 4.7.3 (Manajemen Kerentanan).

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

5.7. Manajemen Perubahan. Snowflake mengelola program manajemen perubahan yang terdokumentasi untuk Layanan.

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. Manajemen Resiko Vendor. Snowflake mengelola program manajemen risiko vendor untuk vendor yang mengolah Data Pelanggan yang dirancang untuk memastikan setiap vendor mempertahankan tindakan perlindungan yang konsisten dengan kewajiban Snowflake dalam Adendum Keamanan ini.

6. Physical & Environmental Controls
6. Pengendalian Fisik & Lingkungan

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. Pusat Data Lingkungan Cloud. Untuk memastikan bahwa Penyedia Cloud memiliki pengendalian fisik dan lingkungan yang sesuai untuk pusat datanya yang menyediakan hosting Lingkungan Cloud, Snowflake secara teratur meninjau pengendalian tersebut seperti yang diaudit berdasarkan audit dan sertifikasi pihak ketiga Penyedia Cloud. Setiap Penyedia Cloud harus memiliki audit tahunan SOC 2 Tipe II dan sertifikasi ISO 27001, atau kerangka kerja setara yang diakui industri. Pengendalian tersebut, harus mencakup, namun tidak terbatas pada, hal-hal berikut:

6.1.1. Physical access to the facilities are controlled at building ingress points;
6.1.1. Akses secara fisik ke fasilitas yang dikendalikan di titik masuk gedung;

6.1.2. Visitors are required to present ID and are signed in;
6.1.2. Pengunjung harus menunjukkan identitas dan mendaftar masuk;

6.1.3. Physical access to servers is managed by access control devices;
6.1.3. Akses secara fisik ke server yang dikelola oleh perangkat pengendalian akses;

6.1.4. Physical access privileges are reviewed regularly;
6.1.4. Hak istimewa atas akses secara fisik yang ditinjau secara teratur;

6.1.5. Facilities utilize monitor and alarm response procedures;
6.1.5. Fasilitas yang menggunakan prosedur pemantauan dan respons alarm;

6.1.6. Use of CCTV;
6.1.6. Penggunaan CCTV;

6.1.7. Fire detection and protection systems;
6.1.7. Sistem pendeteksi api dan sistem perlindungan;

6.1.8. Power back-up and redundancy systems; and
6.1.8. Sistem cadangan dan kelebihan daya; dan

6.1.9. Climate control systems.
6.1.9. Sistem pengendalian iklim.

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. Kantor Perusahaan Snowflake. *Apabila Data Pelanggan tidak di-hosting di kantor perusahaan Snowflake, pengendalian secara teknis, administratif, dan fisik milik Snowflake untuk kantor perusahaannya yang tercakup dalam sertifikasi ISO 27001, harus mencakup, namun tidak terbatas pada, hal-hal berikut:*

6.2.1. Physical access to the corporate office is controlled at office ingress points;
6.2.1. Akses secara fisik ke kantor perusahaan yang dikendalikan di titik masuk gedung;

6.2.2. Badge access is required for all personnel and badge privileges are reviewed regularly;
6.2.2. Akses berupa tanda pengenal diperlukan untuk semua personel dan hak istimewa atas tanda pengenal ditinjau secara berkala;

6.2.3. Visitors are required to sign in;
6.2.3. Pengunjung diharuskan untuk mendaftar masuk;

6.2.4. Use of CCTV at building ingress points;
6.2.4. Penggunaan CCTV di titik masuk gedung;

6.2.5. Tagging and inventory of Snowflake-issued laptops and network assets;
6.2.5. Pemberian tanda dan inventaris laptop dan aset jaringan yang dikeluarkan Snowflake;

6.2.6. Fire detection and sprinkler systems; and
6.2.6. Sistem pendeteksi api dan alat pemadam; dan

6.2.7. Climate control systems.
6.2.7. Sistem pengendalian iklim.

7. Incident Detection & Response
7. Deteksi & Respons Insiden

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 and Snowflake's ability to timely notify shall be negatively impacted.

*7.1. Pelaporan Insiden Keamanan. Apabila Snowflake mengetahui adanya pelanggaran keamanan yang menyebabkan kerusakan, kehilangan, perubahan, pengungkapan yang tidak sah dari, atau akses ke Data Pelanggan ("**Insiden Keamanan**"), Snowflake akan memberitahukan Pelanggan tanpa penundaan yang tidak semestinya, dan dalam hal apa pun, jika memungkinkan, memberitahukan Pelanggan dalam waktu 72 jam setelah mengetahui hal tersebut.[3] Agar pemberitahuan dapat disampaikan tepat pada waktunya, Pelanggan diharuskan untuk mendaftarkan dan mempertahankan surel yang terkini dalam Layanan untuk cara pemberitahuan ini. Jika tidak ada surel semacam itu yang terdaftar, Pelanggan mengakui bahwa cara pemberitahuan harus sesuai dengan kebijaksanaan wajar Snowflake dan kemampuan Snowflake untuk memberitahukan secara tepat waktu akan terpengaruh secara negatif.*

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. Investigasi. Dalam hal terjadi Insiden Keamanan seperti yang dijelaskan di atas, Snowflake harus segera mengambil langkah-langkah yang wajar untuk menahan, menyelidiki, dan mengurangi Insiden Keamanan apa pun. Setiap catatan yang dianggap relevan dengan Insiden Keamanan, harus disimpan setidaknya selama satu tahun.

[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.
[3] Untuk memperjelas, pada saat Perjanjian Pelanggan merujuk pada istilah "Pelanggaran Keamanan" yang didefinisikan, referensi tersebut harus ditafsirkan untuk merujuk pada Insiden Keamanan, sebagaimana didefinisikan dalam Adendum Keamanan ini

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 do not have visibility to the content of Customer Data, it will be unlikely that Snowflake can provide information as to the particular nature of the Customer Data, or where applicable, the identities, number, or categories of affected data subjects. Communications by or on behalf of Snowflake with Customer in connection with a Security Incident shall not be construed as an acknowledgment by Snowflake of any fault or liability with respect to the Security Incident.

7.3. Komunikasi dan Kerjasama. Snowflake akan memberikan informasi tepat pada waktunya kepada Pelanggan tentang Insiden Keamanan sejauh yang diketahui Snowflake, termasuk, namun tidak terbatas pada, sifat dan akibat Insiden Keamanan, tindakan yang diambil dan/atau yang diusulkan oleh Snowflake untuk mengurangi atau menahan Insiden Keamanan, status investigasi Snowflake, narahubung dari mana informasi tambahan dapat diperoleh, dan kategori serta perkiraan jumlah catatan data terkait. Tanpa mengesampingkan ketentuan sebelumnya, Pelanggan mengakui bahwa karena personel Snowflake tidak dapat melihat isi Data Pelanggan, kemungkinan besar Snowflake tidak dapat memberikan informasi mengenai sifat tertentu dari Data Pelanggan, atau jika berlaku, identitas, jumlah, atau kategori dari subyek data yang terpengaruh. Komunikasi yang dilakukan oleh atau atas nama Snowflake dengan Pelanggan sehubungan dengan Insiden Keamanan tidak akan ditafsirkan sebagai pengakuan oleh Snowflake atas kesalahan atau kewajiban apa pun sehubungan dengan Insiden Keamanan

8. Deletion of Customer Data.

8. Penghapusan Data Pelanggan.

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

8.1. Oleh Pelanggan. Layanan memberikan kendali kepada Pelanggan untuk menghapus Data Pelanggan, sebagaimana dijelaskan lebih lanjut dalam Dokumentasi.

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. Oleh Snowflake. Tunduk pada ketentuan Perjanjian yang berlaku, setelah (i) kadaluwarsa atau pengakhiran Perjanjian dan (ii) kadaluwarsanya setiap "periode perolehan kembali" pasca-pengakhiran yang ditetapkan dalam Perjanjian, Snowflake harus segera menghapus Data Pelanggan yang tersisa.

9. Customer Rights & Shared Security Responsibilities

9. Hak Pelanggan & Tanggung Jawab Keamanan Bersama

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. Pengujian Penyusupan oleh Pelanggan. Pelanggan dapat memberikan permintaan tertulis untuk melakukan pengujian penyusupan atas Akunnya ("**Pengujian Penyusupan**") dengan mengirimkan permintaan tersebut melalui tiket dukungan. Setelah diterimanya tanda terima tersebut oleh Snowflake, Snowflake dan Pelanggan harus menyetujui bersama sebelumnya mengenai perincian Pengujian Penyusupan tersebut, termasuk tanggal mulai, ruang lingkup, dan durasi, serta kondisi wajar yang dirancang untuk mengurangi potensi risiko terhadap kerahasiaan, keamanan, atau potensi gangguan lainnya terhadap Layanan atau usaha Snowflake. Pengujian Penyusupan dan informasi apa pun yang timbul darinya dianggap sebagai Informasi Rahasia Snowflake. Jika Pelanggan menemukan kerentanan yang nyata atau yang berpotensial sehubungan dengan Pengujian Penyusupan, Pelanggan harus segera*

mengungkapkannya kepada Snowflake dan tidak akan mengungkapkannya kepada pihak ketiga mana pun.

9.2. Customer Audit Rights.
9.2. Hak Audit Pelanggan.

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, HITRUST CSF, and PCI-DSS third-party certifications, (ii) Snowflake's SOC 2 Type II audit report, SOC 1 Type II audit report, and HIPAA Compliance Report for Business Associates, (iii) Snowflake's most recently completed industry standard security questionnaire, such as a SIG or CAIQ, and (iv) data flow diagrams for the Service (collectively with Third-Party Audits, "**Audit Reports**").

*9.2.1. Atas permintaan tertulis dan tanpa biaya tambahan kepada Pelanggan, Snowflake harus menyediakan Pelanggan, dan/atau perwakilan pihak ketiga yang memenuhi syarat (secara bersama-sama, disebut "**Auditor**"), akses terhadap dokumentasi yang diminta secara wajar yang membuktikan pemenuhan Snowflake terhadap kewajibannya berdasarkan Adendum Keamanan ini dalam bentuk, sebagaimana berlaku, (i) ISO 27001, HITRUST CSF, dan sertifikasi pihak ketiga PCI-DSS milik Snowflake, (ii) Laporan audit SOC 2 Tipe II, laporan audit SOC 1 Tipe II, Laporan Kepatuhan HIPAA untuk Rekan Bisnis milik Snowflake, (iii) Kuesioner keamanan berstandar industri terbaru dari Snowflake, seperti SIG atau CAIQ, dan (iv) diagram alir data (data flow diagram) untuk Layanan (secara bersama-sama dengan Audit Pihak Ketiga, disebut "**Laporan Audit**").*

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. Pelanggan juga dapat mengirimkan permintaan tertulis untuk melakukan audit atas pengendalian Snowflake yang berlaku, termasuk melakukan inspeksi ke fasilitasnya. Setelah diterimanya permintaan tersebut oleh Snowflake, Snowflake dan Pelanggan sebelumnya harus menyetujui bersama mengenai perincian audit, termasuk tanggal mulai yang wajar, ruang lingkup dan durasi, serta pengendalian perlindungan dan kerahasiaan yang berlaku untuk audit tersebut. Snowflake dapat mengenakan biaya (dengan tarif yang wajar, dengan mempertimbangkan sumber daya yang dikeluarkan oleh Snowflake) untuk audit tersebut. Laporan Audit, audit, dan informasi apa pun yang timbul daripadanya akan dianggap sebagai Informasi Rahasia 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. Apabila Auditor merupakan pihak ketiga (atau Pelanggan menunjuk pihak ketiga untuk melakukan Pengujian Penyusupan yang disetujui berdasarkan Bagian 9.1), pihak ketiga tersebut dapat diminta untuk menandatangani perjanjian kerahasiaan terpisah dengan Snowflake sebelum dilakukannya setiap audit, Pengujian Penyusupan, atau peninjauan Laporan Audit, dan Snowflake dapat mengajukan keberatan secara tertulis atas pihak ketiga tersebut, jika menurut pendapat wajar Snowflake, pihak ketiga tersebut tidak memiliki kualifikasi yang sesuai atau merupakan pesaing langsung dari Snowflake. Atas keberatan Snowflake, Pelanggan akan diharuskan untuk menunjuk pihak ketiga lain atau melakukan audit, Pengujian Penyusupan, atau peninjauan itu

sendiri. Setiap biaya yang dikeluarkan oleh Auditor sehubungan dengan setiap peninjauan Laporan Audit, atau audit atau Pengujian Penyusupan, akan ditanggung secara eksklusif oleh Auditor.

9.3. Sensitive Customer Data. Use of the Service to meet requirements of PCI-DSS, HIPAA, FedRAMP, or similar heightened standards, require additional controls which shall be implemented by Customer, including that Customer Data subject to such requirements may only be uploaded to Editions and Regions of the Service specifically designated in the Documentation for such requirements. Additionally, Customer must implement all appropriate Customer-configurable security controls, including IP whitelisting and MFA for all User interactive logins (e.g., individuals authenticating to the Service) to protect such data.

9.3. Data Pelanggan Yang Sensitif. Penggunaan Layanan untuk memenuhi persyaratan PCI-DSS, HIPAA, FedRAMP, atau standar tinggi serupa, memerlukan kontrol tambahan yang akan dilaksanakan oleh Pelanggan, termasuk Data Pelanggan tunduk terhadap persyaratan tersebut hanya dapat diunggah ke Edisi dan Wilayah Layanan yang secara khusus ditetapkan dalam Dokumentasi untuk persyaratan tersebut. Selain itu, Pelanggan harus menerapkan seluruh pengendalian perlindungan yang dapat dikonfigurasi Pelanggan yang sesuai, termasuk daftar putih IP dan MFA untuk seluruh login interaktif Pengguna (misalnya, individu yang memberikan verifikasi ke Layanan) untuk melindungi data tersebut.

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

9.4. Tanggung Jawab Keamanan Bersama. Tanpa mengurangi komitmen Snowflake dalam Adendum Keamanan ini, Pelanggan setuju:

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 (including not uploading data that requires a certification and/or authorization which is not identified in Section 1.1) 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. Snowflake tidak memiliki kewajiban untuk menilai isi, keakuratan atau legalitas Data Pelanggan, termasuk untuk mengidentifikasi informasi yang tunduk pada persyaratan hukum, peraturan, atau persyaratan lain apa pun dan Pelanggan bertanggung jawab untuk menggunakan Layanan secara tepat (termasuk tidak mengunggah data yang memerlukan suatu sertifikasi dan/atau otorisasi yang tidak diidentifikasi dalam Bagian 1.1) untuk memastikan tingkat perlindungan yang sesuai dengan isi tertentu dari Data Pelanggan, termasuk, apabila sesuai, penerapan fungsi enkripsi, seperti fitur "tri-secret secure" (sebagaimana dijelaskan dalam Dokumentasi), nama samara dari Data Pelanggan, dan konfigurasi Layanan untuk membuat cadangan atas Data Pelanggan;

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), (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. Pelanggan bertanggung jawab untuk mengelola dan melindungi peran dan kredensial Penggunanya, termasuk namun tidak terbatas pada (i) memastikan bahwa semua Pengguna menjaga kerahasiaan kredensial dan tidak membagikan informasi tersebut dengan pihak yang tidak berwenang, (ii) segera melaporkan ke Snowflake setiap aktivitas mencurigakan yang terkait dengan Akun Pelanggan (misalnya kredensial pengguna telah disusupi), (iii) melakukan konfigurasi Pengguna dan pengendalian akses berbasis peran dengan tepat, termasuk cakupan dan durasi akses Pengguna, dengan mempertimbangkan sifat Data Pelanggannya, dan (iv) menjaga keunikan, panjang, kerumitan, dan kadaluwarsa kata sandi yang sesuai;

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. untuk mengelola dan melindungi setiap kunci enkripsi yang dikelola oleh Pelanggan dengan tepat untuk memastikan integritas, ketersediaan, dan kerahasiaan kunci dan Data Pelanggan yang dienkripsi dengan kunci tersebut; dan

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

9.4.4. untuk segera memperbarui Piranti Lunak Kliennya setiap kali Snowflake mengumumkan pembaruan.