Snowflake Reseller Public Sector Access Terms
(Last Updated March 25, 2022)

THESE SNOWFLAKE RESELLER PUBLIC SECTOR ACCESS TERMS ("**ACCESS TERMS**") ARE HEREBY MADE A PART OF THE AGREEMENT (THE "**AGREEMENT**") BETWEEN THE ORDERING ACTIVITY UNDER GSA SCHEDULE CONTRACTS IDENTIFIED IN THE PURCHASE ORDER ("**YOU**" "**YOUR**" OR "**CUSTOMER**") AND THE APPLICABLE PERSON AUTHORIZED TO RESELL SNOWFLAKE OFFERINGS ("**RESELLER**"). IF YOU ARE ACCEPTING THESE ACCESS TERMS ON BEHALF OF A BUSINESS, GOVERNMENT ENTITY OR GOVERNMENT AGENCY, YOU REPRESENT AND WARRANT THAT YOU ARE AUTHORIZED TO BIND SUCH ENTITY(IES) TO THESE ACCESS TERMS. THE RIGHTS GRANTED UNDER THESE ACCESS TERMS ARE EXPRESSLY CONDITIONED UPON SUCH AUTHORITY AND ACCEPTANCE. THE SNOWFLAKE OFFERINGS ARE PROVIDED ON A SUBSCRIPTION AND/OR LICENSE BASIS ONLY AND ARE NOT SOLD TO YOU.

1. Scope. For clarity, these Access Terms are not an agreement with Snowflake Inc. nor with any of its Affiliates (collectively, "**Snowflake**"). These Access Terms set the terms, rules, conditions, and restrictions that apply to your use of the Snowflake Offerings and any ancillary services, such as Technical Services or Support, under your Agreement with the Reseller.

2. Use of the Snowflake Offerings.

2.1. In General. Reseller gives you and your Users access to the Snowflake Offerings for the Subscription Term solely for use by you and your Users in accordance with the Agreement, these Access Terms, the Documentation and the Order Form. You may permit your Contractors and Affiliates to serve as Users provided that any use of the Snowflake Offerings by each of such Contractor or Affiliate is solely for the benefit of Customer or such Affiliate. You will comply with these Access Terms in connection with your use of the Snowflake Offerings and shall be responsible for each User's compliance with these Access Terms. Contractual commitments by Snowflake to Reseller do not apply as between you and Snowflake. You must look solely to Reseller regarding any claims or damages relating to, or arising out of, the Snowflake Service, the Agreement, and/or these Access Terms. Reseller is not an agent of Snowflake and is not acting on behalf of Snowflake, and you are not a third party beneficiary of any agreement between Reseller and Snowflake.

2.2. Snowflake Offerings, Generally. The Snowflake Service will operate in substantial conformity with the applicable Documentation and Order Form. Technical Services and Deliverables (if any) will be provided in a professional and workmanlike manner and will substantially conform with the specifications in the applicable SOW. If Reseller, is not able to correct any reported non-conformity with the aforementioned ("Limited Warranty"), either Reseller or Customer may terminate the applicable Order Form or Statement of Work (as applicable), and Customer, as its sole remedy, will be entitled to receive a refund of any unused Fees that Customer has pre-paid for the applicable Service or Technical Services purchased thereunder. This Limited Warranty will not apply if the error or non-conformance was caused by misuse of the Service or Deliverables, modifications to the Service or Deliverables by Customer or any third-party, or third-party hardware, software, or services used in connection with the Service. For Technical Services and Deliverables, this warranty will not apply unless Customer provides written notice of a claim within thirty (30) days after expiration of the applicable Statement of Work.

2.3. Disclaimers; Limitations on Snowflake Liability. EXCEPT FOR THE LIMITED WARRANTY IN SECTION 2.2 ABOVE AND TO THE EXTENT PROHIBITED BY LAW, OR TO THE EXTENT ANY STATUTORY RIGHTS APPLY THAT CANNOT BE EXCLUDED, LIMITED OR WAIVED, NEITHER SNOWFLAKE, NOR RESELLER ON BEHALF OF SNOWFLAKE, MAKES ANY REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE. SNOWFLAKE DISCLAIMS ALL WARRANTIES, INCLUDING ANY IMPLIED OR EXPRESS WARRANTIES (a) OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, (b) ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE, OR (c) THAT THE SNOWFLAKE SERVICE, CLIENT SOFTWARE, SAMPLE DATA, TECHNICAL SERVICES, SUPPORT, OR THIRD-PARTY APPLICATIONS CONTENT WILL BE UNINTERRUPTED, ERROR FREE, OR FREE OF HARMFUL COMPONENTS. SNOWFLAKE WILL NOT BE LIABLE TO CUSTOMER FOR ANY DAMAGES OF ANY KIND (INCLUDING DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES, DAMAGES FOR LOST PROFITS, REVENUES, CUSTOMERS, OPPORTUNITIES, GOODWILL, USE, OR DATA, THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR ANY INVESTMENTS, EXPENDITURES, OR COMMITMENTS BY YOU IN CONNECTION WITH YOUR USE OF THE SNOWFLAKE SERVICE, CLIENT SOFTWARE, SAMPLE DATA, TECHNICAL SERVICES, SUPPORT, OR THIRD PARTY APPLICATIONS) ARISING IN CONNECTION WITH, OR RELATED TO, YOUR INABILITY TO USE THE SNOWFLAKE SERVICE, INCLUDING AS A RESULT OF ANY TERMINATION OR SUSPENSION OF RESELLER ORDER FORMS UNDER ANY AGREEMENT BETWEEN SNOWFLAKE AND RESELLER, DISCONTINUATION OR DOWNTIME OF THE SNOWFLAKE SERVICE, OR ANY UNAUTHORIZED ACCESS TO, DISCLOSURE OR ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ACCOUNT CUSTOMER DATA.

2.4. Third-Party Applications. Through the use of the Snowflake Service, you may have access to Third-Party Applications, which may be made available directly to you by other entities or individuals under separate terms and conditions or supplemental terms and conditions to these Access Terms, which may include separate fees and charges. Your use of any Third-Party Application is solely at your own risk.

2.5. Snowflake Service Policies. All access to and use of Snowflake Offerings is subject to the Snowflake Acceptable Use Policy and Documentation. Notwithstanding anything in the Acceptable Use Policy and Documentation, the Snowflake Acceptable Use Policy is not an agreement (separate or otherwise) between you and Snowflake.

2.6. Your Responsibilities. Except to the extent responsibility is accepted in writing or unless otherwise agreed by Reseller, you are solely responsible for use of the Snowflake Offerings. To the extent the Snowflake Service requires you to install Client Software, you are granted a limited, non-transferable, non-sublicensable, non-exclusive license during the term of your Agreement to use the object code form of the Client Software internally in connection with your use of the Snowflake Service as provided in the Documentation.

2.7. Sample Data; Third Party Applications. Sample Data may be made available to you as part of the Snowflake Service. You acknowledge that Sample Data is example data only, which may not be complete, current, or accurate. You will not (and will not permit any third party to) copy or export any Sample Data and you agree that the Sample Data may be deleted at any time or you may be required to cease using Sample Data at any time. URL links or interconnectivity may be provided with the Snowflake Service to facilitate your use of Third Party Applications, but such use shall be at your sole discretion. Notwithstanding the foregoing, any procurement or use of Third Party Applications is solely between you and the applicable third party and/or you and the Reseller.

2.8. Customer-Controlled Data Sharing Functionality.

a. Generally. The Snowflake Service includes the capability for you, at your option and in your sole discretion, to share Customer Data with other Customer-designated Snowflake customers designated by you and/or Read Only Users (defined below), and to access or use data from other Snowflake customers, as further described in the Documentation. The Snowflake customer sharing its data is a "**Provider**," and the Snowflake customer accessing or using shared data is a "**Consumer**."

b. When You are the Provider. Provider may, at its option and in its sole discretion, grant Consumer access to designated sets of Provider's Customer Data as further described in the Documentation. Provider acknowledges and agrees that: (1) Consumers will have the access designated by Provider (including to view, download, and query the Customer Data) and that it is Provider's sole responsibility to evaluate any risks related to its sharing of Customer Data with Consumers; and (2) Snowflake has no control over, and will have no liability for, any acts or omissions of any Consumer with respect to Provider's sharing of Customer Data. At all times, as Provider, you remain responsible for your Customer Data as set forth in these Access Terms.

c. When You are the Consumer. By accessing or using Provider's data, Consumer acknowledges that: (1) Snowflake has no liability for such data or Consumer's use of such data; (2) Snowflake may collect information about Consumer's use of and access to the Snowflake Service and to Provider's data (including identifying Consumer in connection with such information) and share it with Provider; and (3) you are obligated to use Provider's Customer Data in accordance with any terms imposed by Provider.

d. Reader Accounts. When you are a Provider, you may, at your option and in your sole discretion (using a mechanism provided by Snowflake), authorize third party entities that are not currently Snowflake customers ("**Read Only Consumers**") to access a read-only account on the Snowflake Service as further described in the Documentation ("**Reader Accounts**") solely to consume Customer Data shared by you, provided that:

(1) you shall be responsible for paying for any usage of the Reader Accounts;

(2) Users authorized to access the Reader Account ("**Read Only Users**") shall be prohibited from uploading any data into the Reader Accounts;

(3) such Read Only Users must submit support requests only as set forth in the Snowflake Support Policy;

(4) you represent that you have the right to share with Snowflake any personal information about Read Only Users that you provide to Snowflake; and

(5) you shall be responsible for any acts or omissions on the part of Read Only Users in their use of the Reader Accounts as if they were acts or omissions of you.

2.9. General Restrictions. You will not (and will not permit any third party to): (a) sell, rent, lease, license, distribute, provide access to, sublicense, or otherwise make available any Snowflake Service (or Deliverables, if applicable) to a third party (except as set forth in the Documentation for Snowflake Service features expressly intended to enable you to provide your third parties with access to Customer Data, or the SOW, as applicable) or in a service bureau or outsourcing offering; (b) use any Snowflake Service to provide, or incorporate any Snowflake Service into, any general purpose data warehousing service for the benefit of a third party; (c) reverse engineer, decompile, disassemble, or otherwise seek to obtain the source code or non-public APIs to any Snowflake Service, except to the extent expressly permitted by applicable law (and then only upon advance written notice to Snowflake); (d) remove or obscure any proprietary or other notices contained in any Snowflake Service; or (e) use any Snowflake Offerings in violation of the Acceptable Use Policy.

2.10. Preview Service Terms. Certain products, features, services, software, regions or cloud providers may be made available to you through the Snowflake Service that are not yet generally available, including such products, features, services, software, regions or cloud providers that are labeled as "private preview," "public preview," "pre-release" or "beta" (collectively, "**Previews**"). You may access and use Previews solely for your internal evaluation purposes. EXCEPT AS OTHERWISE AGREED BETWEEN THE PARTIES IN WRITING, PREVIEWS ARE PROVIDED AS-IS, WITH ALL FAULTS, AND AS AVAILABLE, AND PREVIEWS ARE EXCLUDED FROM ANY SUPPORT, SERVICE LEVEL, PRIVACY, SECURITY OR OTHER COMPLIANCE COMMITMENTS, AND FROM ANY WARRANTIES, INDEMNITIES OR LIABILITY TO THE MAXIMUM EXTENT PERMITTED BY LAW. You shall not use Previews to process personal data or other data that is subject to heightened compliance requirements. Previews may be changed or discontinued at any time without notice, and Previews may also not be chosen for release into general availability.

3. Customer Data.

3.1. Rights in Your Data. As between you and Snowflake, you or your licensors retain all right, title and interest (including any and all intellectual property rights) in and to the Customer Data and any modifications made thereto in the course of the operation of the Snowflake Service as provided to Snowflake. You grant to Snowflake and its Affiliates a non-exclusive, worldwide, royalty-free right to process the Customer Data solely to the extent necessary to provide the Snowflake Offerings to Customer, to prevent or address service or technical problems with the Snowflake Service, or as may be required by law or regulation.

3.2. Use Obligations.

a. In General. Your use of the Snowflake Service and all Customer Data shall comply with applicable laws and government regulations, including but not limited to any data localization or data sovereignty laws or regulations, and laws governing personal data. You are solely responsible for the accuracy, content and legality of all Customer Data. You warrant that you have and will have sufficient rights in Customer Data to grant the rights to Snowflake under these Access Terms and that the processing of Customer Data by Snowflake will not violate any laws or the rights of any third party.

b. HIPAA Data. You agree not to upload to any Snowflake Service any HIPAA Data unless you have entered into a BAA with Reseller, and in any case, never to provide HIPAA Data other than by uploading it to the editions of the Snowflake Service which are specifically designated for HIPAA Data in the Documentation.

3.3. Privacy. Customer Personal Data (as defined in the DPA) shall be processed in compliance with the DPA, including but not limited to (where applicable) the SCCs (as defined therein). You must also comply with the DPA and (where applicable) the SCCs, as "Customer" (as defined therein). Notwithstanding anything to the contrary in the DPA (including the SCCs), it is not an agreement between you and Snowflake nor with any of Snowflake's Affiliates. Any rights you have thereunder must be enforced through the Reseller in accordance with **Section 2.1 (In General)** above.

3.4 Security. The Snowflake Service and Customer Data are secured in compliance with the Security Addendum. You must also comply with the Security Addendum, as "Customer" (as defined therein). Notwithstanding anything to the contrary in the Security Addendum, it is not an agreement between you and Snowflake nor with any of Snowflake's Affiliates. Any rights you have thereunder must be enforced through the Reseller in accordance with **Section 2.1 (In General)** above.

4. Intellectual Property.

4.1. Snowflake Technology. You agree that Snowflake or its suppliers retain all right, title and interest (including all patent, copyright, trademark, trade secret and other intellectual property rights) in and to the Snowflake Offerings, all Documentation and Client Software, any Deliverables, and any and all related and underlying technology and documentation; and any derivative works, modifications, or improvements of any of the foregoing, including any Feedback that may be incorporated (collectively, "**Snowflake Technology**"). Except for the express limited rights set

forth in these Access Terms, no right, title or interest in any Snowflake Technology is granted to you. Further, you acknowledge that the Snowflake Service is offered as an online, hosted solution, and that you have no right to obtain a copy of the underlying computer code for any Snowflake Offering, except (if applicable) for the Client Software in object code format. Notwithstanding anything to the contrary herein, Snowflake may freely use and incorporate into Snowflake's products and services any suggestions, enhancement requests, recommendations, corrections, or other feedback provided by you or by any Users of the Snowflake Offerings relating to Snowflake's products or services ("**Feedback**").

4.2. Usage Data. Notwithstanding anything to the contrary in these Access Terms, Snowflake may collect and use Usage Data for the development, improvement, support, and operation of its products and services.

4.3. Marketing. Snowflake may use and display your name, and service marks on Snowflake's website and in Snowflake's marketing materials in connection with identifying you as a customer of Snowflake to the extent permitted by the General Services Acquisition Regulation (GSAR) 552.203-71.

5. Retrieval of Data and Suspension of Service.

5.1. Retrieval of Data. Upon written notice to Snowflake, Customer will have up to thirty (30) calendar days from termination or expiration of the Agreement to access the Snowflake Service solely to the extent necessary to retrieve Customer Data (**"Retrieval Right"**). If Customer exercises its Retrieval Right, the Agreement, inclusive of these Access Terms, and the applicable Order Form shall continue in full force and effect for the duration of the Retrieval Right. Snowflake shall have no further obligation to make Customer Data available after termination of the Agreement and shall thereafter promptly delete Customer Data. After the Retrieval Right period, Customer will have no further access to Customer Data and shall cease use of and access to the Snowflake Offerings (including any related Snowflake Technology) and delete all copies of Client Software, Documentation, any associated passwords or access codes, and any other Snowflake Confidential Information in its possession. Notwithstanding any termination or anything to the contrary in this Agreement or any Order Form, Customer shall pay for all of its use of the Snowflake Offerings.

5.2. Suspension of Service. Snowflake reserves the right to suspend the provision of any and all Snowflake Offerings if: (a) Snowflake reasonably determines suspension is necessary to avoid material harm to Snowflake or its other customers, including if the Snowflake Offerings are experiencing denial of service attacks, mail flooding, or other attacks or disruptions outside of Snowflake's control; or (b) as required by law or at the request of governmental entities.

6. Support and Availability. You will be provided the level of Support for the Snowflake Service specified in the applicable Order Form, in accordance with the Support Policy. All requests for support will be directed to Snowflake and Reseller should not have access to Customer's Account and/or Customer Data. Should you grant Reseller access to your Account or any Customer Data, you hereby consent to such access by Reseller.

7. Technical Services.

7.1. Provision of Technical Services. Snowflake will, through the Reseller, perform Technical Services (if any) will be provided as set forth in each applicable SOW, subject to the terms and conditions of these Access Terms.

7.2. Assistance. You acknowledge that timely access to applicable Your Materials (defined below), resources, personnel, equipment or facilities is necessary for the provision of Technical Services. You agree to provide such access and to reasonably cooperate with Snowflake in order for Snowflake to duly render the relevant Technical Services.

7.3. Your Materials. You hereby grant Snowflake a limited right to use any materials provided to Snowflake in connection with Technical Services projects ("**Your Materials**") solely for the purpose of providing Technical Services to you. You will retain any of the rights (including all intellectual property rights) in and to Your Materials. You warrant that you have and will have sufficient rights in Your Materials to grant the rights to Snowflake under these Access Terms and that Your Materials will not violate the rights of any third party.

7.4. Access to Customer Data under a SOW. With respect to any access by Snowflake or others to any Customer Data under an SOW, you are solely responsible for ensuring that both the duration and scope of access is strictly limited to the access required under the specific SOW. You agree that you will not grant Snowflake access to Customer Data unless specifically required and noted in an SOW, and only during the term of the applicable Technical Services project. Unless otherwise specified in an SOW, you must ensure that: (a) any access to Customer Data that you grant is limited to read-only access in your development environment for the Snowflake Service (and you will not grant access to any other environment, such as its test, prod or disaster recovery), and (b) you will not grant access to any Customer Data that is unencrypted or contains personal data. To the extent access to Customer Data is granted, you will provide the recipient of such access with: (i) secure workstations and networks for accessing Customer Data that are monitored, managed,

configured, supported and maintained by you, and (ii) unique user ID/passwords to each Snowflake resource that requires access to Customer Data, and these credentials will be solely managed by you.

7.5. License to Deliverables. The Technical Services Snowflake performs (e.g., providing guidance on configuring the Snowflake Service) and the resulting Deliverables are generally applicable to Snowflake's business and are part of Snowflake Technology. Snowflake grants you a limited, non-exclusive, royalty-free, non-transferable worldwide license to use the Deliverables internally solely in connection with your use of the Snowflake Service during the period in which you have authorized access to the Snowflake Service.

7.6. Change Orders; Other Terms. You may submit written requests to Reseller to change the scope of Technical Services under an existing SOW. Reseller will promptly notify you if it believes that the requested change may requires an adjustment to the fees, schedule, assumptions or scope for the performance of the Technical Services. You will be notified in such cases. Any change requests must be agreed to by Snowflake in writing before taking effect.

8. INDEMNIFICATION

8.1. Indemnification by Reseller. Subject to the Attorney Generals acceptance of the procedures set forth in Section 8.3, Snowflake will have the right to intervene to defend Customer against any claim by a third party alleging that any Service or Deliverable, when used in accordance with this Agreement, infringes any intellectual property right of such third party and will indemnify and hold harmless Customer from and against any damages and costs awarded against Customer or agreed in settlement by Reseller (including reasonable attorneys' fees) resulting from such claim. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516. If Customer's use of the Service or Deliverable results (or in Snowflake's or Reseller's opinion is likely to result) in an infringement claim, Reseller may either: (a) substitute functionally similar products or Snowflake Offerings; (b) procure for Customer the right to continue using the Service or Deliverable; or if (a) and (b) are not commercially reasonable, (c) terminate this Agreement, or the applicable Order Form or SOW and refund to Customer the unused Fees that Customer has pre-paid for the applicable Service or Deliverable. The foregoing indemnification obligation of Reseller will not apply to the extent the applicable claim is attributable to: (1) the modification of the Service or Deliverable by any party other than Snowflake or based on Customer's specifications or requirements; (2) the combination of the Service or Deliverable with products or processes not provided by Snowflake; (3) any use of the Service or Deliverables in non-conformity with this Agreement; or (4) any action arising as a result of Customer Data, or any deliverables or components not provided by Snowflake. This Section sets forth Customer's sole remedy with respect to any claim of intellectual property infringement.

8.2. Customer Representation and Warranties. Customer agrees that it is solely responsible for all risks arising from or relating to any Customer Data, Customer Materials or any Customer-offered product or service used in connection with the Service, and hereby represents and warrants that any Customer Data, Customer Materials or any Customer-offered product or service used in connection with the Service will not violate this Agreement or applicable law, infringe or misappropriate any third-party rights, or cause harm to any third party or Snowflake.

8.3. **Procedures.** In the event of a potential obligation under this Section 8, the party receiving the claim will: (i) promptly notify the responsible party in writing of the claim, (ii) allow the responsible party the right to control the investigation, defense and settlement (if applicable) of such claim at the indemnifying party's sole cost and expense, and (iii) upon request of the responsible party, provide all necessary cooperation at the responsible party's expense. Failure by the other party to notify the responsible party of a claim under this Section 8 shall not relieve the responsible party of its obligations under this Section 8, however the responsible party shall not be liable for any litigation expenses that the other party incurred prior to the time when notice is given or for any damages and/or costs resulting from any material prejudice caused by the delay or failure to provide notice to the responsible party in accordance with this Section. The responsible party may not settle any claim that would bind the other party to any obligation (other than payment covered by the indemnifying party or ceasing to use infringing materials) or require any admission of fault by the other party, without the other party's prior written consent, such consent not to be unreasonably withheld, conditioned, or delayed. Any obligation under this Section 8 will not apply if the other party settles or makes any admission with respect to a claim without the indemnifying party's prior written consent.

9. LIMITATION OF REMEDIES AND DAMAGES. EXCEPT AS TO "EXCLUDED CLAIMS," TO THE MAXIMUM EXTENT PERMITTED BY LAW, AND NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT:

(A) NEITHER PARTY NOR ITS AFFILIATES SHALL BE LIABLE TO THE OTHER PARTY OR ITS AFFILIATES FOR ANY LOSS OF USE, LOST OR INACCURATE DATA, INTERRUPTION OF BUSINESS, COSTS OF DELAY, LOST PROFITS, OR ANY INDIRECT, SPECIAL, INCIDENTAL, RELIANCE, PUNITIVE, EXEMPLARY OR CONSEQUENTIAL DAMAGES OF ANY KIND, EVEN IF INFORMED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE;

(B) SUBJECT TO SUBSECTION (C) BELOW, EACH PARTY'S AND ITS AFFILIATES' TOTAL LIABILITY TO THE OTHER PARTY AND ITS AFFILIATES FOR ALL CLAIMS IN THE AGGREGATE (FOR DAMAGES OR LIABILITY OF ANY TYPE), SHALL NOT

EXCEED THE AMOUNT ACTUALLY PAID OR PAYABLE TO SNOWFLAKE IN THE PRIOR 12 MONTHS UNDER THE APPLICABLE ORDER FORM(S) OR SOW TO WHICH SUCH LIABILITY RELATES ("**GENERAL LIABILITY CAP**");

(C) IN THE CASE OF "DATA PROTECTION CLAIMS," EACH PARTY'S AND ITS AFFILIATES' TOTAL LIABILITY TO THE OTHER PARTY AND ITS AFFILIATES FOR ALL CLAIMS IN THE AGGREGATE (FOR DAMAGES OR LIABILITY OF ANY TYPE) SHALL NOT EXCEED TWO TIMES (2X) THE "GENERAL LIABILITY CAP";

(D) IN NO EVENT SHALL EITHER PARTY (OR ITS RESPECTIVE AFFILIATES) BE LIABLE FOR THE SAME EVENT UNDER BOTH THE GENERAL LIABILITY CAP AND THE DATA PROTECTION CLAIMS CAP. SIMILARLY, THOSE CAPS SHALL NOT BE CUMULATIVE; IF A PARTY (AND/OR ITS AFFILIATES) HAS ONE OR MORE CLAIMS SUBJECT TO EACH OF THOSE CAPS, THE MAXIMUM TOTAL LIABILITY FOR ALL CLAIMS IN THE AGGREGATE SHALL NOT EXCEED THE DATA PROTECTION CLAIMS CAP;

(E) THE PARTIES AGREE THAT THIS SECTION 9 WILL APPLY REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE AND WILL APPLY EVEN IF ANY LIMITED REMEDY SPECIFIED IN THIS AGREEMENT IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE; AND

(F) THE APPLICABLE MONETARY CAPS SET FORTH IN THIS SECTION 9 SHALL APPLY ACROSS THIS AGREEMENT AND ANY AND ALL SEPARATE AGREEMENT(S) ON AN AGGREGATED BASIS.

10. **CONFIDENTIALITY**. Each party (as "**Receiving Party**") will use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but not less than reasonable care) to (i) not use any Confidential Information of the other party (the "**Disclosing Party**") for any purpose outside the scope of this Agreement, and (ii) except as otherwise authorized by the Disclosing Party in writing, limit access to Confidential Information of the Disclosing Party to those of its and its Affiliates' employees and contractors who need that access for purposes consistent with this Agreement and who have signed confidentiality agreements with the Receiving Party containing protections not materially less protective of the Confidential Information than those herein. If Receiving Party is required by law or court order to disclose Confidential Information, then Receiving Party shall, to the extent legally permitted, provide Disclosing Party with advance written notification and cooperation to the fullest extent permitted by law in any effort to obtain confidential treatment of the Confidential Information, including an opportunity for the Disclosing Party to seek redactions or protective orders to prevent against disclosure. Snowflake recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor. In such cases, Snowflake shall have the opportunity to seek appropriate relief through a Reverse FOIA action.

11. **Federal Government End Use Provisions**.

11.1. Commercial Item. The Snowflake Offerings, including all related software and, to the extent applicable the Snowflake Technology, for ultimate federal government end use is made available solely in accordance with the following: The U.S. Government hereby agrees that the Snowflake Offerings qualify as "commercial items" as defined by FAR Part 2.101 or the state law corollary. The terms and conditions of these Access Terms shall pertain to the U.S. Government's use and disclosure of the Snowflake Offerings and shall supersede any conflicting contractual terms or conditions. Government technical data and software rights related to the Snowflake Offerings include only those rights customarily provided to the public as defined in these Access Terms. This customary commercial license is provided in accordance with FAR 12.211 (Technical Data) and FAR 12.212 (Software) and, for Department of Defense transactions, DFAR 252.227-7015 (Technical Data Commercial Items).

11.2. U.S. Government Region Terms. Certain deployments are made available that are expressly designated for use by U.S. government customers or that support customer ITAR compliance, as set forth in the Documentation ("U.S. SnowGov Regions"). If you elect to use the Snowflake Service in any U.S. SnowGov Region, your use of and access to the Snowflake Service in such U.S. SnowGov Region is subject to the Snowflake U.S. SnowGov Region Terms of Service. You shall be deemed to have accepted said U.S. SnowGov Region Terms of Service upon your use of the Snowflake Service in any U.S. SnowGov Region. Notwithstanding anything in the Snowflake U.S. SnowGov Region Terms of Service, the Snowflake U.S. SnowGov Region Terms of Service are not an agreement (separate or otherwise) between you and Snowflake. Any rights you have thereunder must be enforced through the Reseller in accordance with **Section 2.1 (In General)** above.

12. **Miscellaneous.**

12.1. Severability; Interpretation. If a court of competent jurisdiction holds any provision of these Access Terms to be unenforceable or invalid, that provision will be limited to the minimum extent necessary so that these Access Terms

will otherwise remain in effect. Section headings are inserted for convenience only and shall not affect the construction of these Access Terms.

12.2. Export Control. You agree to comply with all export and import laws and regulations of the United States and other applicable jurisdictions. Without limiting the foregoing, (i) you represent and warrant that you are not listed on any U.S. government list of prohibited or restricted parties or located in (or a national of) a country that is subject to a U.S. government embargo or that has been designated by the U.S. government as a "terrorist supporting" country, (ii) you will not (and will not permit any third parties to) access or use any Snowflake Offerings in violation of any U.S. export embargo, prohibition or restriction, and (iii) you will not submit to any Snowflake Service any information that is controlled under the U.S. International Traffic in Arms Regulations.

12.3. Entire Agreement. The Agreement, inclusive of these Access Terms and the Exhibits attached hereto, is the complete and exclusive statement of the mutual understanding of the parties and supersedes and cancels all prior written and oral agreements and communications relating to the Snowflake Offerings. Where there are any inconsistencies between the terms and conditions of these Access Terms and the Agreement, these Access Terms shall prevail as they apply to the Snowflake Offerings. Snowflake may change and update the Snowflake Offerings (in which case Snowflake may update the applicable Documentation accordingly) provided that, Snowflake will not materially decrease the overall functionality of the Snowflake Offerings during the applicable Subscription Term.

13. Definitions.

"**Affiliate**" means an entity that, directly or indirectly, owns or controls, is owned or is controlled by, or is under common ownership or control with a party. As used herein, "control" means the power to direct the management or affairs of an entity and "ownership" means the beneficial ownership of more than fifty percent (50%) of the voting equity securities or other equivalent voting interests of an entity.
"Acceptable Use Policy" means Snowflake's acceptable use policy attached hereto as Exhibit A.
"BAA" means a business associate agreement governing Snowflake's, your, and/or Reseller's respective obligations with respect to any HIPAA Data uploaded by you to the Snowflake Service in accordance with the terms of this Agreement.
"CCPA" means the California Consumer Privacy Act of 2018, as may be amended from time to time.
"Client Software" is any desktop client software included in the applicable Snowflake Service that is made available to you for installation on end user computers to be used in connection with the Snowflake Service for installation on your computer(s).
"Consumer" is defined in Section 2.8(a).
"**Confidential Information**" means all information that is identified as confidential at the time of disclosure by the disclosing party or should be reasonably known by the receiving party to be confidential or proprietary due to the nature of the information disclosed and the circumstances of the disclosure. All Customer Data will be deemed Confidential Information of Customer without any marking or further designation. All Snowflake Technology will be deemed Confidential Information of Snowflake without any marking or further designation. Confidential Information shall not include information that the receiving party can demonstrate: (i) was rightfully in its possession or known to it prior to receipt of the Confidential Information; (ii) is or has become public knowledge through no fault of the receiving party; (iii) is rightfully obtained by the receiving party from a third party without breach of any confidentiality obligation; or (iv) is independently developed by employees of the receiving party who had no access to such information.
"**Contractor**" means your independent contractors and consultants.
"Customer Data" means any data or data files of any type that are uploaded and/or stored in the Snowflake Service by or on behalf of you.
"**Data Protection Claims**" means any claims arising from a party's breach of Section 3.3 (Privacy), Section 3.4 (Security), or Section 10 (Confidentiality), where such breach results in the unauthorized disclosure of Customer Data, or breach of Section 3.2 (Use Obligations).

"**Data Protection Laws**" means all data protection and privacy laws applicable to the respective party in its role in the Processing of Personal Data under the Agreement, including, where applicable, EU & UK Data Protection Laws and the California Privacy Act of 2018, as amended from time to time.
"Deliverables" means the guides, code (including SQL queries) or other deliverables that Snowflake provides in connection with Technical Services. For clarity, Snowflake may use compilers, assemblers, interpreters and similar tools to develop Deliverables. The term "Deliverables" does not include such tools.
"DPA" means the Snowflake Customer Data Processing Addendum attached hereto as Exhibit B.
"Documentation" means Snowflake's technical documentation and usage guides for the applicable Snowflake Service made available at https://docs.snowflake.com (or such successor URL as may be designated by Snowflake) or through the Snowflake Service.
"**Excluded Claims**" means (a) a party's breach of its obligations in Section 10 (Confidentiality) (but excluding obligations and/or claims relating to Customer Data); (b) either party's express obligations under Section 8 (Indemnification); and (c) liability which, by law, cannot be limited, including personal injury, death, fraud, and gross negligence.

"Feedback" is defined in Section 4.1.
"**HIPAA**" means the Health Insurance Portability and Accountability Act, as amended and supplemented.
"**HIPAA Data**" means any patient, medical or other protected health information regulated by HIPAA or any similar federal or state laws, rules or regulations.
"Order Form" means the ordering document (and/or SOW, if any) between you and Reseller that specifies the Snowflake Offerings to be provided by Snowflake as well as applicable discounts, Subscription Term, and payment terms.
"Personal Data" means any information, including opinions, relating to an identified or identifiable natural person and includes similarly defined terms in Data Protection Laws, including the definition of "personal information" in the CCPA.
"Provider" is defined in Section 2.8(a).
"Reader Accounts" are defined in Section 2.8(d)
"Read Only Consumers" are defined in Section 2.8(d).
"Read Only Users" are defined in Section 2.6(d)(2).
"Sample Data" means any data (including from third-party sources) provided or made available to you by Snowflake solely for your internal testing, evaluation, and other non-production use of the Snowflake Service during the Subscription Term.
"SOW" means a statement of work describing the Technical Services to be performed, fees and any applicable milestones, dependencies and other technical specifications or related information for Technical Services related to the Snowflake Service.
"**Security Addendum**" means the Snowflake Security Addendum attached hereto as Exhibit C.
"**Snowflake Offerings**" means the Snowflake Service and any ancillary services provided in connection with the Snowflake Service, such as Support and Technical Services.
"**Snowflake Service**" or "**Service**" means a software-as-a-service offering made generally available by Snowflake, as described in the Documentation and set forth in an Order Form. Any APIs provided by Snowflake to access the Snowflake Service are deemed part of the Snowflake Service.
"**Snowflake Technology**" is defined in Section 4.1.
"Snowflake U.S. SnowGov Region Terms of Service" means the Snowflake U.S. SnowGov Region Terms of Service attached hereto as Exhibit E.
"Subscription Term" means the term designated on an Order Form.
"Support" means the technical support provided by Snowflake to prevent or address service or technical problems, as described in the Snowflake Support Policy.
"**Support Policy**" means the Snowflake Support Policy and Service Level Agreement attached hereto as Exhibit D.
"**Technical Services**" means consulting, education and training services related to the Snowflake Service provided by Snowflake through Reseller to Customer, as set forth in a SOW.
"**Third- Party Applications**" means separate or third-party data, services, offerings or applications (and other consulting services related thereto), made available to by you or to you that interoperate with the Snowflake Service and are subject to an independent agreement or supplemental terms to these Access Terms.
"**Usage Data**" means query logs, and any data (other than Customer Data) relating to the operation, support and/or about your use of the Snowflake Service.
"**User**" means the persons designated and granted access to the Service Offerings by you or on your behalf, including, as applicable, any of its and its Affiliates' Contractors.
"Your Materials" is defined in Section 7.3.

Exhibit A

Acceptable Use Policy
November 10, 2021*

Use of the Service and any Snowflake offerings are subject to this Acceptable Use Policy.

Capitalized terms have the meaning stated in the applicable agreement between Customer and Snowflake.

Customer agrees not to, and not to allow third parties to use the Service:

1. to store, transmit, or make available (a) content that is infringing, libelous, unlawful, tortious, or in violation of third-party rights, (b) content or technology that harms, interferes with, or limits the normal operation of the Service or Snowflake offerings, including monitoring traffic or data, or (c) viruses, malware, or other malicious code;
2. for illegal, threatening, or offensive uses, or for similarly objectionable purposes, such as propagating hate or violence or causing harm to others or to our reputation;
3. to transact in, or facilitate activities related to, misappropriating another individual's identity, including, but not limited to, improperly obtained credit card information and/or account credentials;
4. to attempt to gain unauthorized access to the Service or any Snowflake offerings or any related systems, including those of Snowflake's subcontractors and other customers or users;
5. to permit direct or indirect access to or use of the Service or any Snowflake offerings in a way that violates the Agreement or use of the Service or any Snowflake offerings to access or use any intellectual property in or related to the Service or any Snowflake offerings except as permitted under the Agreement;
6. to copy the Service or any Snowflake offerings, or any part, feature, function or user interface thereof except as expressly allowed for Client Software under the Agreement; or
7. to build similar or competitive products or services.

Customer may conduct benchmark tests of the Service (each a "**Test**"). Other than with respect to Tests involving Previews, which may not be disclosed externally, Customer may externally disclose a Test or otherwise cause the results of a Test to be externally disclosed if it includes as part of the disclosure all information necessary to replicate the Test.

Notwithstanding anything to the contrary in the Agreement, in the event of any conflict between the Agreement and this AUP, this AUP shall govern. This AUP may be non-materially updated by Snowflake from time to time upon reasonable notice (which may be provided through the Service or by posting an updated version of this AUP). Any violation of this AUP may result in the suspension or termination of your access to and use of the Service or any Snowflake offering in accordance with the terms and conditions of the Agreement.

* Please visit https://www.snowflake.com/legal for the latest version of the AUP.

Exhibit B

Data Processing Addendum

This Data Processing Addendum ("**DPA**") forms part of, and is subject to, the Master SaaS Agreement or other written or electronic terms of service or subscription agreement between the member of the Snowflake Group that is a party to such agreement ("**Snowflake**") and the legal entity defined as 'Customer' thereunder together with all Customer Affiliates who are signatories to an Order Form for their own Service Account pursuant to such agreement (collectively, for purposes of this DPA, "**Customer**", and together with Snowflake, the "**Parties**") (such agreement, the "**Agreement**"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

1. Definitions.

"**Account**" means Customer's account in the Service in which Customer stores and processes Customer Data.

"**Affiliate**" has the meaning set forth in the Agreement.

"**Authorized Affiliate**" shall mean a Customer Affiliate who has not signed an Order Form pursuant to the Agreement, but is either a Data Controller or Data Processor for the Customer Personal Data processed by Snowflake pursuant to the Agreement, for so long as such entity remains a Customer Affiliate.

"**California Consumer Privacy Act**" or "**CCPA**" means the California Consumer Privacy Act of 2018, as may be amended from time to time.

"**Customer Data**" has the meaning set forth in the Agreement.

"**Customer Personal Data**" means any Customer Data that is Personal Data.

"**Data Controller**" means an entity that determines the purposes and means of the Processing of Personal Data.

"**Data Processor**" means an entity that Processes Personal Data on behalf of a Data Controller.

"**Data Protection Laws**" means all data protection and privacy laws of the United States applicable to the respective party in its role in the Processing of Personal Data under the Agreement, including, where applicable, the CCPA.

"**Data Subject**" means the identified or identifiable natural person to whom Customer Personal Data relates."**Personal Data**" means any information, including opinions, relating to an identified or identifiable natural person and includes similarly defined terms in Data Protection Laws, including, but not limited to, the definition of "**personal information**" in the CCPA.

"**Processing**" shall mean any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination and "**Process**", "**Processes**" and "**Processed**" will be interpreted accordingly.

"**Purposes**" shall mean (i) Snowflake's provision of the Services as described in the Agreement, including Processing initiated by Users in their use of the Services; and (ii) further documented, reasonable instructions from Customer agreed upon by the Parties.

"**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data.

"**Services**" means the generally available Snowflake software-as-a-service offering described in the Documentation and procured by Customer, and any other services provided by Snowflake as described under the Agreement, including but not limited to support and technical services.

"**Snowflake Group**" means Snowflake Inc. and its Affiliates.

"**Sub-Processor**" means any other Data Processors engaged by a member of the Snowflake Group to Process Customer Personal Data.

2. Scope and Applicability of this DPA. This DPA applies where and only to the extent that Snowflake Processes Customer Personal Data on behalf of Customer as Data Processor in the course of providing the Services. Customer shall not submit any Customer Personal Data to Snowflake that would require Snowflake to enter into additional terms, such as the European standard contractual clauses, without Snowflake's express written consent in the form of an amendment to this DPA.

3. Roles and Scope of Processing.

3.1. Role of the Parties. As between Snowflake and Customer, Snowflake shall Process Customer Personal Data only as a Data Processor (or sub-processor) acting on behalf of Customer and, with respect to CCPA, as a "service provider" as defined therein, in each case regardless of whether Customer acts as a Data Controller or as a Data Processor on behalf of a third-party Data Controller ("**Third-Party Controller**") with respect to Customer Personal Data. To the extent any Usage Data (as defined in the Agreement) is considered Personal Data under applicable Data Protection Laws, Snowflake is the Data Controller of such data and shall Process such data in accordance with the Agreement and applicable Data Protection Laws.

3.2. Customer Instructions. Snowflake will Process Customer Personal Data only for the Purposes. Customer shall ensure its Processing instructions are lawful and that the Processing of Customer Personal Data in accordance with such instructions will not violate applicable Data Protection Laws. The Parties agree that the Agreement (including this DPA) sets out the exclusive and final instructions to Snowflake for all Processing of Customer Personal Data, and (if applicable) include and are consistent with all instructions from Third-Party Controllers. Any additional requested instructions requires the prior written agreement of Snowflake. Where applicable, Customer shall be responsible for any communications, notifications, assistance and/or authorizations that may be required in connection with a Third-Party Controller

3.3. Customer Affiliates. Snowflake's obligations set forth in this DPA shall also extend to Authorized Affiliates, subject to the following conditions:

(a) Customer must exclusively communicate any additional Processing instructions requested pursuant to 3.2 directly to Snowflake, including instructions from its Authorized Affiliates;

(b) Customer shall be responsible for Authorized Affiliates' compliance with this DPA and all acts and/or omissions by an Authorized Affiliate with respect to Customer's obligations in this DPA shall be considered the acts and/or omissions of Customer; and

(c) Authorized Affiliates shall not bring a claim directly against Snowflake. If an Authorized Affiliate seeks to assert a legal demand, action, suit, claim, proceeding or otherwise against Snowflake ("**Authorized Affiliate Claim**"): (i) Customer must bring such Authorized Affiliate Claim directly against Snowflake on behalf of such Authorized Affiliate, unless Data Protection Laws require the Authorized Affiliate be a party to such claim; and (ii) all Authorized Affiliate Claims shall be considered claims made by Customer and shall be subject to any liability restrictions set forth in the Agreement, including any aggregate limitation of liability.

3.4. Customer Processing of Personal Data. Customer agrees that it: (i) will comply with its obligations under Data Protection Laws with respect to its Processing of Customer Personal Data; (ii) will make appropriate use of the Services to ensure a level of security appropriate to the particular content of the Customer Personal Data, such as pseudonymizing and backing-up Customer Personal Data; and (iii) has obtained all consents, permissions and rights necessary under Data Protection Laws for Snowflake to lawfully Process Customer Personal Data for the Purposes, including, without limitation, Customer's sharing and/or receiving of Customer Personal Data with third-parties via the Services.

3.5. Details of Data Processing.

(a) Subject Matter: The subject matter of the Processing under this DPA is the Customer Personal Data.

(b) Frequency and duration: Notwithstanding expiry or termination of the Agreement, Snowflake will Process the Customer Personal Data continuously and until deletion of all Customer Personal Data as described in this DPA.

(c) Purpose: Snowflake will Process the Customer Personal Data for the Purposes, as described in this DPA.

(d) Nature of the Processing: Snowflake will perform Processing as needed for the Purposes, and to comply with Customer's Processing instructions as provided in accordance with the Agreement and this DPA

(e) Retention Period. The period for which Customer Personal Data will be retained and the criteria used to determine that period shall be determined by Customer during the term of the Agreement via its use and configuration of the Service. Upon termination or expiration of the Agreement, Customer may retrieve or delete all Customer Personal Data as set forth in the Agreement. Any Customer Personal Data not deleted by Customer shall be deleted by Snowflake promptly 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.

(f) Categories of Data Subjects: The categories of Data Subjects to which Customer Personal Data relate are determined and controlled by Customer in its sole discretion, and may include, but are not limited to:

(i) Prospects, customers, business partners and vendors of Customer (who are natural persons);

(ii) Employees or contact persons of Customer's prospects, customers, business partners and vendors; and/or

(iii) Employees, agents, advisors, freelancers of Customer (who are natural persons).

(g) Categories of Personal Data: The types of Customer Personal Data are determined and controlled by Customer in its sole discretion, and may include, but are not limited to:

(i) Identification and contact data (name, address, title, contact details);

(ii) Financial information (credit card details, account details, payment information);

(iii) Employment details (employer, job title, geographic location, area of responsibility); and/or

(iv) IT information (IP addresses, cookies data, location data).

(h) Special Categories of Personal Data (if applicable): Subject to any applicable restrictions and/or conditions in the Agreement or Documentation, Customer may also include "special categories of personal data" or similarly sensitive Personal Data (as described or defined in Data Protection Laws) in Customer Personal Data, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Customer Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data Processed for the purposes of uniquely identifying a natural person, data concerning health and/or data concerning a natural person's sex life or sexual orientation.

4. Sub-Processing.

4.1. Authorized Sub-Processors. Customer provides Snowflake with a general authorization to engage Sub-processors, subject to Section 4.3 (Changes to Sub-processors), as well as Snowflake's current Sub-processors listed at www.snowflake.com/legal/snowflake-sub-processors ("**Sub-processor Site**") as of the effective date of this DPA and members of the Snowflake Group.

4.2. Sub-Processor Obligations. Snowflake shall: (i) enter into a written agreement with each Sub-processor imposing data protection obligations no less protective of Customer Personal Data as Snowflake's obligations under this DPA to the extent applicable to the nature of the services provided by such Sub-processor; and (ii) remain liable for each Sub-processor's compliance with the obligations under this DPA. Upon written request, and subject to any confidentiality restrictions, Snowflake shall provide Customer all relevant information it reasonably can in connection with its applicable Sub-processor agreements where required to satisfy Customer's obligations under Data Protection Laws.

4.3. Changes to Sub-Processors. Snowflake shall make available on its Sub-processor Site a mechanism to subscribe to notifications of new Sub-processors. Snowflake shall provide such notification to those emails that have subscribed at least fourteen (14) days in advance of allowing the new Sub-processor to Process Customer Personal Data (the "**Objection Period**"). During the Objection Period, objections (if any) to Snowflake's appointment of the new Sub-processor must be provided to Snowflake in writing and based on reasonable grounds relating to data protection. In such event, the Parties will discuss those objections in good faith with a view to achieving resolution. If it can be reasonably demonstrated to Snowflake that the new Sub-processor is unable to Process Customer Personal Data in compliance with the terms of this DPA and Snowflake cannot provide an alternative Sub-processor, or the Parties are not otherwise able to achieve resolution as provided in the preceding sentence, Customer, as its sole and exclusive remedy, may provide written notice to Snowflake terminating the Order Form(s) with respect only to those aspects of the Services which cannot be provided by Snowflake without the use of the new Sub-processor. Snowflake will refund Customer any prepaid unused fees of such Order Form(s) following the effective date of termination with respect to such terminated Services.

5. Security.

5.1. Security Measures. Snowflake shall implement and maintain appropriate technical and organizational security measures designed to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of the Customer Personal Data in accordance with Snowflake's Security Addendum attached to the Agreement as Exhibit C ("**Security Addendum**").

5.2. Confidentiality of Processing. Snowflake shall ensure that any person who is authorized by Snowflake to Process Customer Personal Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

5.3. No Assessment of Customer Personal Data by Snowflake. Snowflake shall have no obligation to assess the contents or accuracy of Customer Personal Data, including to identify information subject to any specific legal, regulatory, or other requirement. Customer is responsible for reviewing the information made available by Snowflake relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws.

6. Customer Audit Rights.

6.1. 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 DPA in the form of the relevant audits or certifications listed in the Security Addendum, such as (i) Snowflake's ISO 27001, HITRUST CSF, and PCI-DSS third-party certifications, (ii) Snowflake's SOC 2 Type II audit reports, SOC 1 Type II audit reports, HIPAA Compliance Report for Business Associates, and (iii) Snowflake's most recently completed industry standard security questionnaire, such as a SIG or CAIQ (collectively, "**Reports**").

6.2. 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. The Reports, audit, and any information arising therefrom shall be considered Snowflake's Confidential Information and may only be shared with a third party (including a Third-Party Controller) with Snowflake's prior written agreement.

6.3. Where the Auditor is a third-party, the Auditor may be required to execute a separate confidentiality agreement with Snowflake prior to any review of Reports or an audit of Snowflake, and Snowflake may object in writing to such Auditor, if in

Snowflake's reasonable opinion, the Auditor is not suitably qualified or is a direct competitor of Snowflake. Any such objection by Snowflake will require Customer to either appoint another Auditor or conduct the audit itself. Any expenses incurred by an Auditor in connection with any review of Reports or an audit shall be borne exclusively by the Auditor.

7. Data Transfers.

7.1. Hosting and Processing Locations. Snowflake will only host Customer Personal Data in the region(s) offered by Snowflake and selected by Customer on an Order Form or as Customer otherwise configures via the Services (the "**Hosting Region**"). Customer is solely responsible for the regions from which its Users access the Customer Personal Data, for any transfer or sharing of Customer Personal Data by Customer or its Users and for any subsequent designation of other Hosting Regions (either for the same Account, a different Account, or a separate Service). Once Customer has selected a Hosting Region, Snowflake will not Process Customer Personal Data from outside the Hosting Region except as reasonably necessary to provide the Services procured by Customer, or as necessary to comply with the law or binding order of a governmental body.

8. Security Incident Response.

8.1. Security Incident Reporting. If Snowflake becomes aware of a Security Incident, Snowflake shall notify Customer without undue delay, and in any case, where feasible, notify Customer within seventy-two (72) hours after becoming aware. Snowflake's notification shall be sent to the email registered by Customer within the Service for such purposes, and 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. Snowflake shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident.

8.2. Security Incident Communications. Snowflake shall provide Customer timely information about the Security Incident, 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 Personal Data, it will be unlikely that Snowflake can provide information as to the particular nature of the Customer Personal 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.

9. Cooperation.

9.1. Data Subject Requests. Snowflake shall promptly notify Customer if Snowflake receives a request from a Data Subject that identifies Customer Personal Data or otherwise identifies Customer, including where the Data Subject seeks to exercise any of its rights under applicable Data Protection Laws (collectively, "**Data Subject Request**"). The Service provides Customer with a number of controls that Customer may use to assist it in responding to Data Subject Requests and Customer will be responsible for responding to any such Data Subject Requests. To the extent Customer is unable to access the relevant Customer Personal Data within the Services using such controls or otherwise, Snowflake shall (upon Customer's written request and taking into account the nature of the Processing) provide commercially reasonable cooperation to assist Customer in responding to Data Subject Requests.

9.2. Data Protection Impact Assessments. Snowflake shall provide reasonably requested information regarding the Services to enable Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by Data Protection Laws, so long as Customer does not otherwise have access to the relevant information.

9.3. Government, Law Enforcement, and/or Third Party Inquiries. If Snowflake receives a demand to retain, disclose, or otherwise Process Customer Personal Data for any third party, including, but not limited to law enforcement or a government authority ("**Third-Party Demand**"), then Snowflake shall attempt to redirect the Third-Party Demand to Customer. Customer agrees that Snowflake can provide information to such third-party as reasonably necessary to redirect the Third-Party Demand. If Snowflake cannot redirect the Third-Party Demand to Customer, then Snowflake shall, to the extent legally permitted to do so, provide Customer reasonable notice of the Third-Party Demand as promptly as feasible under the circumstances to allow Customer to seek a protective order or other appropriate remedy.

10. Relationship with the Agreement.

10.1. The Parties agree that this DPA shall replace and supersede any existing data processing addendum, attachment, exhibit or standard contractual clauses that Snowflake and Customer may have previously entered into in connection with the Services..

10.2. Except as provided by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict in connection with the Processing of Customer Personal Data. Notwithstanding the foregoing, and solely to the extent applicable to any Customer Personal Data comprised of patient, medical or other protected health information regulated by HIPAA or any similar U.S. federal or state health care laws, rules or regulations ("**HIPAA Data**"), if there is any conflict between this DPA and a business associate agreement between Customer and Snowflake ("**BAA**"), then the BAA shall prevail solely with respect to such HIPAA Data.

10.3. Notwithstanding anything to the contrary in the Agreement or this DPA, each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or relating to this DPAand any other data protection agreements in connection with the Agreement (if any), shall be subject to any aggregate limitations on liability set out in the Agreement. Without limiting the Parties' obligations under the Agreement, each party agrees that any regulatory penalties incurred by one party (the "**Incurring Party**") in relation to the Customer Personal Data that arise as a result of, or in connection with, the other party's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce the Incurring Party's liability under the Agreement as if it were liability to the other party under the Agreement.

10.4. In no event shall this DPA benefit or create any right or cause of action on behalf of a third party (including a Third-Party Controller), but without prejudice to the rights or remedies available to Data Subjects under Data Protection Laws or this DPA.

Exhibit C
Snowflake Security Addendum

This Security Addendum is incorporated into and made a part of the Snowflake Reseller Public Sector Access Terms (the "**Access Terms**") and any capitalized terms used but not defined herein shall have the meaning set forth in the Access Terms. In the event of any conflict between the terms of the Access Terms and this Security Addendum, this Security Addendum shall govern. This Security Addendum is made available at www.snowflake.com/legal-gov. Any references made to the "Agreement" in this Security Addendum shall refer to the "Access Terms".

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 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.

1. **Snowflake's Audits & Certifications**

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:

- ISO27001
- SOC 2 Type II
- SOC 1 Type II
- For Snowflake's Business Critical Edition and Virtual Private Snowflake Edition only:
  - PCI-DSS Service Provider Level 1 Certification
  - FedRAMP Moderate Authorized in certain U.S. Regions (as described in the Documentation).
  - HITRUST CSF Certification (where AWS or Microsoft are the Cloud Provider)
  - IRAP at the Protected Level in certain Australian Regions (as described in the Documentation)
  - HIPAA Compliance Report for Business Associates (where Google is the Cloud Provider)

1.2. Third-Party Audits are made available to Customer as described in Section 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.

1.4. 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.

2. **Hosting Location of Customer Data**

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.

3. **Encryption**

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.

3.2. 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.

4. System & Network Security

4.1. Access Controls.

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.

4.1.2. Snowflake personnel will not access Customer Data except (i) as reasonably necessary to provide services under the Agreement or (ii) to comply with the law or a binding order of a governmental body.

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).

4.3. 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.

4.4. 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.

4.5. 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.

4.6. Monitoring & Logging.

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.

4.6.2. 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.

4.7. Vulnerability Detection & Management.

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.

4.7.2. 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.

4.7.3. 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.

5. Administrative Controls

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.

5.2. Personnel Training. Snowflake maintains a documented security awareness and training program for its personnel, including, but not limited to, onboarding and on-going training.

5.3. 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.

5.4. 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.

5.5. 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.

5.6. 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).

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

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.

6. **Physical & Environmental Controls**

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:

- 6.1.1. Physical access to the facilities are controlled at building ingress points;
- 6.1.2. Visitors are required to present ID and are signed in;
- 6.1.3. Physical access to servers is managed by access control devices;
- 6.1.4. Physical access privileges are reviewed regularly;
- 6.1.5. Facilities utilize monitor and alarm response procedures;
- 6.1.6. Use of CCTV;
- 6.1.7. Fire detection and protection systems;
- 6.1.8. Power back-up and redundancy systems; and
- 6.1.9. Climate control systems.

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:

- 6.2.1. Physical access to the corporate office is controlled at office ingress points;
- 6.2.2. Badge access is required for all personnel and badge privileges are reviewed regularly;
- 6.2.3. Visitors are required to sign in;
- 6.2.4. Use of CCTV at building ingress points;
- 6.2.5. Tagging and inventory of Snowflake-issued laptops and network assets;
- 6.2.6. Fire detection and sprinkler systems; and
- 6.2.7. Climate control systems.

7. Incident Detection & Response

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. 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.

7.2. 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.

7.3. 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.

8. Deletion of Customer Data.

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

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.

9. Customer Rights & Shared Security Responsibilities

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.

9.2. Customer Audit Rights.

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**").

9.2.2. 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.

9.2.3. 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.

9.3. 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.

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

9.4.1. Snowflake has no obligation to assess the content or accuracy 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;

9.4.2. 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;

9.4.3. 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

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

Updated: March 7, 2022

Exhibit D
SNOWFLAKE
SUPPORT POLICY AND SERVICE LEVEL AGREEMENT

This Snowflake Support Policy and Service Level Agreement **("Policy")** describes Snowflake's support offering **("Snowflake Support")** in connection with Customer reported bugs, defects, or errors in the Service ("**Error(s)**"). Snowflake Support shall be provided in accordance with the Snowflake Reseller Public Sector Access Terms **("Access Terms").** Customer shall receive Premier Support or Priority Support as designated in the applicable Order Form **("Support Level").** This Policy may be updated by Snowflake from time to time. Capitalized terms not defined in this Policy shall have the meaning given to them in the Access Terms. This Policy is made available at www.snowflake.com/legal-gov. Any references made to the "Agreement" in this Policy shall refer to the "Access Terms".

I. Support

1. **Services.** As part of providing the services and as further described in the Documentation, Snowflake has processes designed to perform robust testing and validation before each release to minimize Errors.

2. **General Support Offering.** Customer shall designate one primary contact who will have administrator privileges and may designate additional contacts ("**Customer Contacts**"). Snowflake shall provide English-speaking remote assistance to Customer Contacts for questions or issues arising from any Error, as further described in this Policy, including troubleshooting, diagnosis, and recommendations for potential workarounds for the duration of Customer's subscription to the applicable Service. Snowflake shall also provide the specific entitlements for the corresponding Support Level procured by Customer as further described in this Policy and the tables below. Details for Priority Support are described in the Priority Support Services Description at https://www.snowflake.com/legal, which is incorporated herein by this reference.

3. **Contacting Snowflake Support.** Customer Contacts may contact Snowflake Support by: (a) submitting a support request to the Snowflake webpage hosting the community forums and support portal located at https://community.snowflake.com (or such successor URL as may be designated by Snowflake) (such website, the "**Snowflake Community**") and designating the appropriate severity level according to Table 1 below, (b) submitting a support request in the web interface as described in the Documentation, (c) submitting the support request to support@snowflake.com if Customer Contacts cannot access the Snowflake Community, or (d) in the event Customer Contacts cannot access Snowflake Community or email, they may contact Snowflake Support by phone at the intake phone number identified in the Snowflake Community solely for purposes of having the support request submitted on their behalf (each a "**Support Case**"). All Customer Contacts must be reasonably trained in the use and functionality of the Service and the Snowflake Documentation and shall use reasonable diligence to ensure a perceived Error is not an issue with Customer equipment, software, or internet connectivity.

4. **Submission of Support Cases.** Each Support Case shall; (a) designate the Severity Level of the Error in accordance with the definitions in Table 1, (b) identify the Customer Account that experienced the error, (c) include information sufficiently detailed to allow Snowflake Support to attempt to duplicate the Error (including any relevant error messages, but not export-controlled data, personal data (other than as required herein), sensitive data, other regulated data, or Customer Data), and (d) provide contact information for the Customer Contact most familiar with the issue. Information submitted in a Support Case is not Customer Data. Unless Customer expressly designates the Severity Level, the Support Case will default to Severity Level 4. If Customer believes the issue to be related to Client Software (as defined in the Agreement), then the Support Case shall also include the applicable Client Software log files. If Customer Contacts submit Support Cases related to enhancement or feature requests, Snowflake shall treat those tickets as closed once the request has been forwarded internally.

5. **Premier Support.** If Customer is receiving Premier Support, the following shall apply in addition to the support description in Section 1 (General Support Offering):

a. Follow-the-Sun Case Management. Snowflake Support shall implement follow-the-sun case management for handling Severity Level 1 Support Cases, to better facilitate uninterrupted support by utilizing Snowflake Support across multiple time zones.

b. Case Escalation. If Customer reasonably believes Snowflake Support is not performing in a professional manner or is failing to provide timely responses in accordance with this Policy, Customer may escalate the Support

Case using the support escalation process described at the Snowflake Community ("**Case Escalation**"). Any Support Case escalated by Customer will be directed to Snowflake's management team for consideration.

6. **Priority Support.** If Customer is receiving Priority Support, the following shall apply in addition to the support description in Section 1 (General Support Offering) and Section 4 (Premier Support):

a. Follow-the-Sun Case Management. Snowflake Support shall implement follow-the-sun case management for handling Severity Level 1 and Severity Level 2 Support Cases, to better facilitate uninterrupted support by utilizing Snowflake Support across multiple time zones.

7. **Read-Only Users Support.** When Customer is a Provider (using Snowflake's data-sharing functionality to share its Customer Data) to Read-only Users, such Read-only Users shall not be designated as Customer Contacts and any Support Cases related to the Provider or its Read-only Users shall be submitted solely by Provider's other Customer Contacts.

8. **Other Support and Training.** Snowflake also offers various support and training resources such as documentation, community forums, FAQs and user guides available on the Snowflake Community. Additionally, Snowflake offers for-fee consultation and training services via Statements of Work.

Table 1: Error Severity Level Definitions

Severity Level 1 (Critical Severity)	An Error that (a) renders the Snowflake Service completely inoperative or (b) makes Customer's use of material features of the Service impossible, with no alternative available.
Severity Level 2 (High Severity)	An Error that (a) has a high impact to key portions of the Service or (b) seriously impairs Customer's use of material function(s) of the Service and Customer cannot reasonably circumvent or avoid the Error on a temporary basis without the expenditure of significant time or effort.
Severity Level 3 (Medium Severity)	An Error that has a medium-to-low impact on the Service, but Customer can still access and use some functionality of the Service.
Severity Level 4 (Low Severity)	An Error that has low-to-no impact on Customer's access to and use of the Service.

Table 2: Severity Level Response Times

Error Severity Level	Premier Support	Priority Support
	Initial Response Time Target	
Severity Level 1 (Critical Severity)	One (1) hour	Fifteen (15) Minutes
Severity Level 2 (High Severity)	Two (2) Business Hours	Two (2) Hours
Severity Level 3 (Medium Severity)	One (1) Business Day	Four (4) Business Hours
Severity Level 4 (Low Severity)	Two (2) Business Days	One (1) Business Day

9. **Error Response.** Upon receipt of a Support Case, Snowflake Support will attempt to determine the Error and assign the applicable Severity Level based on descriptions in Table 1. If Snowflake's Severity Level designation is different from that assigned by Customer, Snowflake will promptly notify Customer in advance of such designation. If Customer notifies Snowflake of a reasonable basis for disagreeing with Snowflake's designated Severity Level, the parties each will make a good faith effort to discuss, escalate internally, and mutually agree on the appropriate Severity Level. Snowflake shall use commercially reasonable efforts to meet the Initial Response Time Target for the applicable Severity Level, as measured during in-region Snowflake Support hours set forth in Table 3 below (such hour(s), "**Business Hour(s)**" with the total Business Hours in an in-region support day being "**Business Day(s)**").

Table 3: Global Snowflake Support Hours

Snowflake Service Region	Premier & Priority Support Business Hours			
	Sev 1 (Premier)	**Sev 1 & 2 (Priority)**	**Sev 2-4 (Premier)** **Sev 3-4 (Priority)**	**Excluded Holidays** **Sev 2-4 (Premier)** **Sev 3-4 (Priority)**
North America	24x7x365	24x7x365	6AM-6PM PT Mon-Fri	Recognized U.S. Federal Holidays

EMEA	24x7x365	24x7x365	6AM-6PM CE Mon-Fri	Recognized EMEA Bank Holidays
Asia Pacific	24x7x365	24x7x365	6AM-6PM AEDT Mon-Fri	Recognized APAC Holidays

II. Service Level Agreement

Definitions:

"**Average Daily Snowflake Credits**" is defined as Customer's actual Snowflake Credit consumption in the calendar month of the Cloud Provider Region in which the Service Level Failure occurred divided by the number of days in such month.

"**Calendar Minutes**" is defined as the total number of minutes in a given calendar month.

"**Cloud Provider Region**" is defined as the Region and Cloud Provider selected by Customer on an Order Form or as configured by Customer via the Service.

"Error Rate" is defined as the number of Failed Operations divided by the total number of Valid Operations. Repeated identical Failed Operations do not count towards the Error Rate.

"Failed Operations" is defined as Valid Operations where the Snowflake Service returns an internal error to Customer.

"Monthly Availability Percentage" is defined as the difference between Calendar Minutes and the Unavailable Minutes, divided by Calendar Minutes, and multiplied by one hundred (100).

"Unavailable" is defined as an Error Rate greater than one percent (1%) over a one-minute interval calculated across all Customer's Accounts within each applicable Cloud Provider Region. The Error Rate is 0 when a Customer Account is inactive, i.e., when there are no Valid Operations in the one-minute interval.

"Unavailable Minutes" is defined as the total accumulated minutes when the Service is Unavailable.

"Valid Operation" is defined as an operation that conforms to (a) the Snowflake Documentation; or (b) Service-use recommendations provided by Snowflake Support personnel.

The Monthly Availability Percentage for the Snowflake Service is ninety-nine and nine-tenths percent (99.9%) ("**Service Level**"). If the Snowflake Service fails to meet the Service Level in a given month ("**Service Level Failure**"), then as Customer's sole and exclusive remedy, Customer shall receive the applicable number of Snowflake Credits set forth in Table 4 below ("**Service Level Credits**"), credited against Customer's usage in the Cloud Provider Region in the calendar month following the Service Level Failure provided that Customer requests Service Level Credits within twenty-one (21) days of the calendar month in which the Service Level Failure occurred. Service Level Credits may not be exchanged for, or converted to, monetary amounts.

Table 4: Service Level Credit Calculation	
Monthly Availability Percentage	**Service Level Credit**
Under 99.9% but greater than or equal to 99.0%	1 x Average Daily Snowflake Credits

Under 99.0% but greater than or equal to 95.0%	3 x Average Daily Snowflake Credits
Under 95.0%	7 x Average Daily Snowflake Credits

Example Calculation - Customer has two Accounts (SFE1, SFE2) in the AWS US East Region. Each Account submits Valid Operations at a steady rate of 50 Valid Operations per minute. In the month of April, in each minute of a 250-minute period, all 50 Valid Operations submitted by SFE1 succeeded, whereas SFE2 experienced 2 Failed Operations out of a total of 50 Valid Operations. For the month of April, the Customer experienced an Error Rate of 2% across SFE1 and SFE2 Accounts in the AWS US East Region ((2 Failed Operations / 100 Valid Operations) * 100) during the 250-minute period. In this example, the Service was Unavailable for the period of 250 minutes because the Error Rate exceeded 1% across both Customer Accounts. There are 43,200 Calendar Minutes in the month of April (30 days x 24 hours x 60 minutes). This results in a Monthly Availability Percentage of 99.4% calculated as ((43,200 - 250)/43,200 * 100). If Customer used a total of three hundred (300) Snowflake Credits across both Customer Accounts in April, then Customer's Average Daily Snowflake Credits for April would be ten (10) Snowflake Credits (300 / 30 days in April). Since the Monthly Availability Percentage is 99.4%, Customer's Service Level Credit would be ten (10) Snowflake Credits (1 x 10 Average Daily Snowflake Credits), which would be credited against Customer's usage of the Snowflake Service in May.

III. Policy Exclusions

Snowflake will have no liability for any failure to meet the Service Level to the extent arising from:

(a) Customer's failure to process Customer Data in the Service in accordance with Snowflake's recommendations for use of the Service -- though, upon being notified of such a case, Snowflake will endeavor to help Customer address the failure (e.g., with additional recommendations);
(b) Customer or User equipment;
(c) third party acts, or services and/or systems not provided by or on behalf of Snowflake. (For the avoidance of doubt, this exclusion (c) does not apply to the acts, services or systems of any "Cloud Providers," as defined in the Snowflake Security Policy attached to the MSA as Exhibit C.);
(d) Force Majeure Events -- i.e., any cause beyond such party's reasonable control, including but not limited to acts of God, labor disputes or other industrial disturbances, systemic electrical, telecommunications, or other utility failures, earthquake, storms or other elements of nature, blockages, embargoes, riots, public health emergencies (including pandemics and epidemics), acts or orders of government, acts of terrorism, or war;
(e) evaluation or proof-of-concept use of the Snowflake Service; or
(f) Snowflake's preview features (e.g., beta functionality not intended for production use).

Updated: December 10, 2021

Exhibit E
SNOWFLAKE U.S. SNOWGOV REGION TERMS OF SERVICE

Last Updated: March 25, 2022

These U.S. SnowGov Region Terms of Service ("**Terms**") take effect as of the date the Order Form or other agreement that references these Terms becomes binding ("**Effective Date**"). These Terms supplement and amend the Access Terms. All capitalized terms not otherwise defined in these Terms shall have the meanings ascribed to such terms in the Access Terms or Order Form, as applicable. These Terms are made available at www.snowflake.com/legal-gov. Any references made to the "Agreement" in this Policy shall refer to the "Access Terms".

1. **NEW DEFINED TERMS**. The following new defined terms are added to the Agreement:

1.1. "**Classified Data**" means data that has been classified by the U.S. government as "Confidential," "Secret," or "Top Secret" as defined in Executive Order 13526, Section 1.2a, or as otherwise deemed by the U.S. government to require special clearance for use, access, or maintenance.

1.2. **"Covered Defense Information"** or **"CDI"** has the meaning as defined in DFARS 252.204-7012 which, for the avoidance of doubt, includes Department of Defense Controlled Unclassified Information as that term is used in DoD Instruction 5200.48, *Controlled Unclassified Information* ("**DoD CUI**"), when handled by or on behalf of a contractor in support of performance of a contract with the Department of Defense.

1.3. **"Controlled Unclassified Information"** or **"CUI"** has the meaning as defined in 32 C.F.R. § 2002.4(h).

1.4. "**DFARS**" means the Defense Federal Acquisition Regulation Supplement as defined in 48 C.F.R. Chapter 2.

1.5. "**FedRAMP**" means the Federal Risk and Authorization Management Program.

1.6. "**ITAR**" means the International Traffic in Arms Regulations, as defined in 22 C.F.R. Subpart M.

1.7. **"U.S. Person"** means a U.S. Person as defined in 22 C.F.R. § 120.15.

1.8. "**U.S. Government Customer**" means a Snowflake Customer that is: (a) a U.S. Federal, state, or local government entity; (b) a tribal government entity; or (c) a commercial entity that is required to process data provided by an entity under Subsection (a) and/or (b) to perform a contract with such entity.

1.9. **"U.S. SnowGov Account**" means Customer's Account when hosted in any U.S. SnowGov Region.

1.10. "**U.S. SnowGov Region**" means Snowflake's Microsoft Azure Government (US Gov Virginia or successor designation) deployment (**"SnowGov Azure Deployment**"), Snowflake's Amazon Web Services GovCloud (US Gov West 1 or successor designation) deployment, and other Snowflake non-commercial deployments that are expressly designated by Snowflake for use by U.S. Government Customers, as set forth in the Documentation.

2. **SCOPE.** These Terms apply to Customer's use of and access to the Service when hosted in any U.S. SnowGov Region.

3. **AUTHORIZED CUSTOMERS.**

3.1. **U.S. Government Customer Use.** Use of and access to the Service when hosted in any U.S. SnowGov Region is limited to U.S. Government Customers.

3.2. **Exception.** Snowflake may, in its sole discretion, expressly permit a Customer that is not a U.S. Government Customer to use and access the Service when hosted in a U.S. SnowGov Region. In such case, Customer understands and agrees that Customer's use of and access to the Service when hosted in any U.S. SnowGov Region may, upon notice, be modified or terminated by Snowflake: (i) in order for Snowflake to comply with FedRAMP (or its successor); (ii) in order for Snowflake to maintain its existing authorizations (or successor or equivalent authorizations) or to obtain a higher authorization, certification or compliance level; (iii) as directed or required by the underlying cloud service provider; and/or (iv) as required by applicable laws and regulations.

3.3. **Prohibited Use.** Use of and access to the Service when hosted in any U.S. SnowGov Region other than in accordance with Sections 3.1 and 3.2 is strictly prohibited. Any such use shall be deemed a breach of these Terms and the Agreement and Snowflake reserves the right to immediately terminate all such unauthorized use.

4. Workloads.

4.1. Notwithstanding any provision to the contrary in the Agreement, but expressly subject to these Terms, Customer may upload Customer Data that is subject to ITAR in its U.S. SnowGov Account(s) and Customer Data that qualifies as CUI, provided the Customer Data does not qualify as Classified Data, CDI or DoD CUI.

4.2. Customer may not upload Customer Data that qualifies as CDI or DoD CUI in its U.S. SnowGov Account(s) unless and until Customer agrees to any additional terms and conditions required by Snowflake.

4.3. Customer may not place any Classified Data in its U.S. SnowGov Account(s). Customer will be solely responsible for sanitization costs incurred by Snowflake and its subcontractors, regardless of any limitation of liability or damages caps in the Agreement or these Terms if Customer introduces Classified Data, CDI or DoD CUI (unless and until Customer agrees to any additional terms and conditions required by Snowflake) into its U.S. SnowGov Account(s) or uses the Service in connection with Classified Data, CDI or DoD CUI (unless and until Customer agrees to any additional terms and conditions required by Snowflake).

5. Snowflake Obligations. Snowflake maintains a documented security program for the U.S. SnowGov Regions under which Snowflake has implemented and maintains administrative, physical, and technical safeguards designed to protect the confidentiality, integrity, and availability of the Service and Customer Data in accordance with the Security Addendum (the "**U.S. SnowGov Security Program**").

5.1. Snowflake has obtained FedRAMP authorizations for the Service when hosted in certain U.S. SnowGov Regions, as further detailed in the Security Addendum and/or Documentation. For so long as Customer is using the Service pursuant to these Terms in such FedRAMP-authorized U.S. SnowGov Regions, Snowflake will use commercially reasonable efforts to maintain its FedRAMP authorizations in effect as of the Effective Date (or successor or equivalent authorizations, as reasonably determined by Snowflake) at the current or a higher authorization level.

5.2. As part of the U.S. SnowGov Security Program, Snowflake will: (i) limit its access to the U.S. SnowGov Regions to Snowflake personnel (including employees and subcontractors) that are lawfully permitted to access ITAR data; and (ii) use commercially reasonable efforts to provide at least the same level of protection as required by its FedRAMP authorizations in effect as of the Effective Date (or successor or equivalent authorizations, as reasonably determined by Snowflake).

6. Customer Obligations - Snowflake Service Hosted in the SnowGov Azure Deployment.

6.1. For Customer to use a U.S. SnowGov Account hosted in the SnowGov Azure Deployment, Customer must comply with Microsoft requirements by seeking approval from Microsoft through the Microsoft Government validation process (currently available at: https://azure.microsoft.com/en-us/global-infrastructure/government/request/?ReqType=General). Customer must obtain Microsoft's written approval of eligibility before Customer's creation of a U.S. SnowGov Account hosted in the SnowGov Azure Deployment and is required to provide evidence to Snowflake's reasonable satisfaction to support Customer's compliance with this Section.

6.2. Notwithstanding anything to the contrary in the Agreement or DPA, while Customer's U.S. SnowGov Account in the SnowGov Azure Deployment may be configured by Customer to support compliance with certain non-U.S. laws, such as the EU's General Data Protection Regulation, any terms in the Agreement or DPA regarding compliance with non-U.S. laws will not apply to Customer's use of its U.S. SnowGov Account in the SnowGov Azure Deployment.

7. Customer Obligations Generally - Snowflake Service Hosted in the U.S. SnowGov Regions.

7.1. Customer represents, warrants, and agrees that it: (i) is a U.S. Person; (ii) is opening the U.S. SnowGov Account on behalf of an entity that is a U.S. Person; and (iii) will only assign an employee of Customer or Customer Contractor who is a U.S. Person as its U.S. SnowGov Account administrator.

7.2. Subject to Section 4 (Workloads) above, Customer represents and warrants that the U.S. SnowGov Account satisfies the requirements imposed on Customer with respect to Customer Data that is subject to ITAR and Customer Data that qualifies as CUI.

7.3. Customer represents and warrants that it is not subject to U.S. export restrictions or sanctions and is not suspended or debarred from contracting with any U.S. governmental entities. Customer will ensure that its use of the Service in the U.S. SnowGov Region complies with applicable U.S. export control laws, including properly managing: (i) access to the U.S. SnowGov Account, (ii) application of appropriate encryption safeguards, and (iii) the movement of Customer Data outside of a U.S. SnowGov Region (including through the use of replication or data sharing features). Customer will, if required by ITAR, have and maintain a valid Directorate of Defense Trade Controls registration and effective compliance program to ensure compliance with ITAR. If requested by Snowflake, Customer agrees to provide Snowflake with documentation and cooperation to verify the accuracy of the representations and warranties set forth in Sections 6.1 and 6.2.

7.4. The Documentation explains how the Service operates in the U.S. SnowGov Regions, including the availability and operation of certain Service features. For example, certain Usage Data may leave the U.S. SnowGov Regions. Customer is responsible for reading, understanding, and complying with the Documentation.

7.5. As described in the Documentation, Customer may have the ability to turn off features when using the Service in the U.S. SnowGov Regions. Disabling or turning off such features may impact the functionality and/or performance of the Service.

8. Support. Customer understands and agrees that, upon execution of these Terms, Snowflake support will be provided during Business Hours for the North America Region for all Customer Accounts, except in connection with Severity Level 1 Errors and unless otherwise agreed in writing by the parties. Snowflake support for U.S. SnowGov Accounts will be provided by persons who are lawfully permitted to access ITAR and CUI data in accordance with the Support Policy, provided that Customer submits support requests through a support ticket and indicates in such support ticket that it has a U.S. SnowGov Account. Notwithstanding anything in the Support Policy to the contrary, Customer may not submit support requests, including security-related questions or concerns, via email or phone if Customer requires support to be provided by persons who are lawfully permitted to access ITAR and CUI data.

9. Miscellaneous.

9.1. Term. These Terms are effective as of the Effective Date and will remain in effect for so long as Customer is using the Service in the U.S. SnowGov Region, unless terminated earlier in accordance with the Agreement. These Terms and/or any access to the U.S. SnowGov Regions may be immediately terminated by Snowflake if Customer ceases to meet applicable eligibility requirements for any deployment in the U.S. SnowGov Region.

9.2. Confidentiality. These Terms constitute Snowflake Confidential Information. Notwithstanding any provision to the contrary, Snowflake may disclose Customer Confidential Information as required by regulation, and to comply with and maintain its authorizations and certifications, including FedRAMP authorizations. If Snowflake is so required to disclose Customer Confidential Information, then Snowflake shall, to the extent permitted, provide Customer with advance written notification and cooperate in any effort to obtain confidential treatment of the Confidential Information.