Master Agreement #: AR2472

Contractor: **CARAHSOFT TECHNOLOGY CORPORATION**

Participating Entity: **STATE OF IDAHO**

The following products or services are included in this contract portfolio:

- *Snowflake Cloud Data Lake, in accordance with the Snowflake Terms of Service incorporated into this Agreement as **Appendix A**. The State reserves the right to add other products or services as it deems appropriate, upon mutual written amendment of this Agreement.*

Master Agreement Terms and Conditions:

1. Scope: This addendum covers ***Cloud Solutions*** lead by the State of *Utah* for use by state agencies and other entities located in the Participating State authorized by that State's statutes to utilize State contracts with the prior approval of the State's Chief Procurement Official.

2. Participation: This NASPO ValuePoint Master Agreement may be used by all state agencies, institutions of higher institution, political subdivisions and other entities authorized to use statewide contracts in the State of Idaho. Issues of interpretation and eligibility for participation are solely within the authority of the State Chief Procurement Official.

3. Access to Cloud Solutions Services Requires State CIO Approval: Unless otherwise stipulated in this Participating Addendum, specific services accessed through the NASPO ValuePoint cooperative Master Agreements for Cloud Solutions by state executive branch agencies are subject to the authority and prior approval of the State Chief Information Officer's Office. The State Chief Information Officer means the individual designated by the state Governor within the Executive Branch with enterprise-wide responsibilities for leadership and management of information technology resources of a state.

   Pursuant to Idaho Code Section 67-827A and policy established by the Idaho Office of the Governor's Information Technology Services (ITS), Idaho state agencies are required to receive approval from ITS prior to purchasing certain types of IT property, including the goods and services covered by this agreement. The Contractor shall not fulfill orders placed

by Idaho state agencies unless it receives confirmation from the agency that ITS has given approval. This requirement does not apply to other public agencies in the state.

4. Primary Contacts: The primary contact individuals for this Participating Addendum are as follows (or their named successors):

Contractor

Name:	Jenna Tabatabaian
Address:	11493 Sunset Hills Road, Suite 100, Reston, VA 20190
Telephone:	703-889-9726
Fax:	703-871-8505
Email:	JENNA.TABATABAIAN@CARAHSOFT.COM

Participating Entity

Name:	Justin Gross
Address:	650 W State Street, Rm 100
Telephone:	208-332-1612
Fax:	208-327-7320
Email:	justin.gross@adm.idaho.gov

5. Participating Entity Modifications Or Additions To The Master Agreement

These modifications or additions apply only to actions and relationships within the Participating Entity.
Participating Entity must check one of the boxes below.

[___] No changes to the terms and conditions of the Master Agreement are required.

[X] The following changes are modifying or supplementing the Master Agreement terms and conditions.

5.1 Reporting and Administrative Fee.

a. **Idaho Administrative Fee.** A one and one-quarter percent (1.25%) Administrative Fee will apply to all purchases made under this PADD by any Purchasing Entity. On a quarterly basis, the Contractor shall remit to the Division of Purchasing an amount

equal to 1.25% of the Contractor's net (sales minus credits) quarterly sales made under the PADD. Pricing has been adjusted to incorporate the Administrative Fee so that the price to Purchasing Entities will reflect the adjustment. Notwithstanding the adjustment, all pricing updates and other terms and conditions of pricing shall be as set forth in the state of Utah Master Agreement (Master Agreement # AR2472). Administrative Fee Payment checks must be made out and mailed to:

State of Idaho Division of Purchasing
P.O. Box 83720
Boise, ID 83720-0075

b. **Reporting Timeline.** Administrative Fee payments and reports to DOP are due no later than thirty (30) calendar days after the end of each calendar quarter as detailed below:

1st Quarter: July 1 – September 30
2nd Quarter: October 1 – December 31
3rd Quarter: January 1 – March 31
4th Quarter: April 1 – June 30

c. **Required Reports.** Two (2) quarterly reports must accompany each Administrative Fee payment and be furnished electronically in Microsoft Excel format. The required reports are: 1) PADD Summary Usage Report; and 2) Detailed Usage Report. The PADD Summary Usage Report can be found on the "Information for Vendors" page of DOP's website: https://purchasing.idaho.gov/information-for-vendors/. The Detailed Usage Report template is attached to this PADD as **Attachment 1**. The reports must be emailed to: purchasing@adm.idaho.gov.

d. **Future Submission.** If, during the term of this agreement, the state implements a method of collecting usage reports or Administrative Fees electronically through its statewide ERP system or other electronic system, Contractor agrees to submit its reports or Administrative Fee payments using that system.

5.2 Governing Law. This PADD and all orders placed thereunder by Purchasing Entities shall be construed in accordance with, and governed by the laws of the state of Idaho, and the

parties consent to the jurisdiction and exclusive venue of the state courts of Ada county in the state of Idaho in the event of any dispute with respect to the PADD.

5.3 Assignment, Merger, Consolidation or Change of Contractor.

a. **Application of Idaho Statutes.** Assignments, mergers, consolidations, and changes of the Contractor under this Agreement are subject to the provisions of Idaho Code section 67-1027 and 67-9230.

b. **Consent to Assign.** Contractor shall not assign this contract, or its rights, obligations, or any other interest arising from the Agreement, or delegate any of its performance obligations, without the express written consent of the DOP Administrator and the Idaho Board of Examiners.

c. **Consent to Change of Contractor.** Any entity into which Contractor may be merged or with which it may be consolidated, any entity resulting from any merger or consolidation to which Contractor is a party, or any entity succeeding to the business of Contractor without first obtaining the prior written approval of the Administrator of the DOP and the Idaho State Board of Examiners.

d. **Effect of Non-Compliance.** At the option of the DOP Administrator, transfer without approval required by this section shall cause the annulment of the Contract. All rights of action for any breach of this Contract are reserved to the State notwithstanding such annulment. As provided in Idaho Code section 67-1027, the State shall not be obligated to pay the assignee until the assignment is recognized by the Idaho Board of Examiners and no damages shall accrue to Contractor or the assignee arising from the State's assignment and payment processes pursuant to Idaho Code sections 67-1027 and 67-9230.

5.4 Amendments. Amendments to the Master Agreement (including, but not limited to extensions, renewals, and modifications to the terms, conditions and pricing) will automatically be incorporated into this PADD unless the Participating Entity elects not to incorporate an amendment by providing written notification to Contractor within ten (10) business days of the date the Participating Entity receives notice of the amendment to the Master Agreement. Failure of the Participating Entity to provide notice in accordance with this section 5.4 will result in the Master Agreement amendment automatically being

incorporated in this PADD. In the event the Participating Entity does not elect to incorporate an amendment into this PADD, the Contractor may terminate this PADD upon thirty (30) calendar days' written notice to the Participating Entity.

5.5 Insurance.

a. Unless otherwise agreed in a Participating Addendum, Contractor shall, during the term of this Master Agreement, maintain in full force and effect, the insurance described in this section. Contractor shall acquire such insurance from an insurance carrier or carriers licensed to conduct business in each Participating Entity's state and having a rating of A-, Class VII or better, in the most recently published edition of Best's Reports. Failure to buy and maintain the required insurance may result in this Master Agreement's termination or, at a Participating Entity's option, result in termination of its Participating Addendum.

b. Coverage shall be written on an occurrence basis. The minimum acceptable limits shall be as indicated below, with no deductible for each of the following categories:

1) Commercial General Liability covering premises operations, independent contractors, products and completed operations, blanket contractual liability, personal injury (including death), advertising liability, and property damage, with a limit of not less than $1 million per occurrence/$2 million general aggregate;

2) CLOUD MINIMUM INSURANCE COVERAGE:

Level of Risk	**Data Breach and Privacy/Cyber Liability including Technology Errors and Omissions** Minimum Insurance Coverage	**Crime Insurance** Minimum Insurance Coverage
Low	$2,000,000	$2,000,000

Moderate	$5,000,000	$5,000,000
High	$10,000,000	$10,000,000

3) Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.

4) Professional Liability. As applicable, Professional Liability Insurance Policy in the minimum amount of $1,000,000 per occurrence and $1,000,000 in the aggregate, written on an occurrence form that provides coverage for its work undertaken pursuant to each Participating Addendum.

c. Contractor shall pay premiums on all insurance policies. Such policies shall also reference this Master Agreement and shall have a condition that they not be revoked by the insurer until thirty (30) calendar days after notice of intended revocation thereof shall have been given to Purchasing Entity and Participating Entity by the Contractor.

d. Prior to commencement of performance, Contractor shall provide to the Lead State a written endorsement to the Contractor's general liability insurance policy or other documentary evidence acceptable to the Lead State that (1) names the Participating States identified in the Request for Proposal as additional insureds, (2) provides that no material alteration, cancellation, non-renewal, or expiration of the coverage contained in such policy shall have effect unless the named Participating State has been given at least thirty (30) days prior written notice, and (3) provides that the Contractor's liability insurance policy shall be primary, with any liability insurance of any Participating State as secondary and noncontributory. Unless otherwise agreed in any Participating Addendum, the Participating Entity's rights and Contractor's obligations are the same as those specified in the first sentence of this subsection. Before performance of any Purchase Order issued after execution of a Participating Addendum authorizing it, the Contractor shall provide to a Purchasing Entity or Participating Entity who requests it the same information described in this subsection.

e. Contractor shall furnish to the Lead State, Participating Entity, and, on request, the Purchasing Entity copies of certificates of all required insurance within thirty (30) calendar days of the execution of this Master Agreement, the execution of a Participating Addendum, or the Purchase Order's effective date and prior to performing any work. The insurance certificate shall provide the following information: the name and address of the insured; name, address, telephone number and signature of the authorized agent; name of the insurance company (authorized to operate in all states); a description of coverage in detailed standard terminology (including policy period, policy number, limits of liability, exclusions and endorsements); and an acknowledgment of the requirement for notice of cancellation. Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after any renewal date. These certificates of insurance must expressly indicate compliance with each and every insurance requirement specified in this section. Failure to provide evidence of coverage may, at sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.

f. Coverage and limits shall not limit Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

5.6 Termination for Convenience. The Participating Entity may terminate this PADD for its convenience, in whole or in part, with or without cause, upon thirty (30) calendar days' written notice to the Contractor specifying the date of termination.

5.7 Termination for Default.

a. The Participating Entity may terminate the PADD when the Contractor has been provided written notice of default or non-compliance and has failed to cure the default or non-compliance within a reasonable time, not to exceed thirty (30) calendar days, unless such longer period of time is mutually agreed upon between the parties in writing. The Participating Entity, upon termination for default or non-compliance, reserves the tight to take any legal action it may deem necessary including, without limitation, offset of damages against payments due.

b. A Purchasing Entity may terminate an order when the Contractor has been provided written notice of default or non-compliance and fails to cure such breach or non-compliance within thirty (30) calendar days of receiving written notice of said breach or non-compliance.

5.8 Public Records, Trade Secrets, and Non-Public Information.

a. The Idaho Public Records Law, Idaho Code Title 74, Chapter 1 ("the Act"), allows the open inspection and copying of public records. Public records include any writing containing information relating to the conduct or administration of the public's business prepared, owned, used, or retained by a State Agency or a local agency (political subdivision of the state of Idaho) regardless of the physical form or character. All, or most, of the documents related to this Agreement will be public records subject to disclosure under the Act.

b. The Act contains certain exemptions to the open inspection and copying of public records, including an exemption for trade secrets. The Act defines trade secrets to "include a formula, pattern, compilation, program, computer program, device, method, technique or process that derives economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by other persons and is subject to the efforts that are reasonable under the circumstances to maintain its secrecy." The Act also defines other records that may be exempt from public disclosure.

c. If Contractor considers any material that it provides related to this Agreement to be a trade secret, or otherwise protected from disclosure, Contractor must so indicate by marking as "exempt" **each page** containing such information. Marking an entire document as exempt is not acceptable or in accordance with the Act and will not be honored. A legend or statement on one (1) page that all or substantially all of the document is exempt from disclosure is not acceptable or in accordance with the Act and will not be honored. Prices provided in relation to this Agreement are not trade secrets. The State, to the extent allowed by law, will honor a designation of nondisclosure. Any questions regarding the applicability of the Act should be addressed to Contractor's own legal counsel prior to submission of the potentially exempt document. The Division of Purchasing will not provide interpretations of the Act.

d. When submitting documents identified by Contractor as exempt, Contractor must:
   i. Identify with particularity the precise text, illustration, or other information contained within each page marked "exempt" (it is not sufficient to simply mark the entire page). The specific information you deem "exempt" within each noted page must be highlighted, italicized, identified by asterisks, contained within a text border, or otherwise be clearly distinguished from other text or other information and be specifically identified as "exempt."

   ii. Provide a separate document entitled "List of Redacted Exempt Information," which provides a succinct list of all exempt material noted in your submitted documents. The list must identify the page/section/paragraph number where the exempt information appears, the title of the section/paragraph where the exempt information appears, the specific portions of text or other information that is claimed to be exempt; or must identify the exempt information in a manner otherwise sufficient to allow the State to determine the precise material subject to the notation. Additionally, this list must identify with each notation the specific basis for your position that the material be treated as exempt from disclosure.

   iii. Submit a redacted copy of the document with all trade secret and exempt information removed or blacked out. The redacted copy must be submitted electronically, with the word "redacted" in the file name, whether the Proposal is submitted manually or electronically.

e. Contractor shall indemnify and defend the State against all liability, claims, damages, losses, expenses, actions, attorney fees and suits whatsoever for honoring a designation of exempt or for the Vendor's failure to designate individual documents as exempt. The Vendor's failure to designate as exempt any document or portion of a document that is released by the State shall constitute a complete waiver of any and all claims for damages caused by any such release. If the State receives a request for materials claimed exempt by the Vendor, the Vendor shall provide the legal defense for such claim.

5.9 Certification Concerning Boycott of Israel. Pursuant to Idaho Code section 67-2346, if payments under the Contract exceed one hundred thousand dollars ($100,000) and

Contractor employs ten (10) or more persons, Contractor certifies that it is not currently engaged in, and will not for the duration of the Agreement engage in, a boycott of goods or services from Israel or territories under its control. The terms in this section defined in Idaho Code section 67-2346 shall have the meaning defined therein.

6 Subcontractors: All contactors, dealers, and resellers authorized in the State of Idaho, as shown on the dedicated Contractor (cooperative contract) website, are approved to provide sales and service support to participants in the NASPO ValuePoint Master Agreement. The contractor's dealer participation will be in accordance with the terms and conditions set forth in the aforementioned Master Agreement.

7 Orders: Any order placed by a Participating Entity or Purchasing Entity for a product and/or service available from this Master Agreement shall be deemed to be a sale under (and governed by the prices and other terms and conditions) of the Master Agreement unless the parties to the order agree in writing that another contract or agreement applies to such order.

8 Price Schedule:

Price Schedule	
Item	**Prices**
1. Firm and fixed total cost for IMPLEMENTATION (Quick Start*) of the Cloud-Based Data Lake Solution.	$19,800.00
2. Firm and fixed total cost for access to online user training and administration training resources (If they are not publicly available).	$0.00
3. Price for three full years of cloud data storage (average expected data volume=2.20TB/mo) with compression & encryption on store for each of the following cloud platforms: AWS, Azure, Google.	$146,027.06 of Snowflake capacity; to be burned down at the following rates: AWS: $23.00 TB/mo Azure: $23.00 TB/mo Azure Government: $39.00 TB/mo Google: $20.00 TB/mo
4. Price for three full years of compute credits for system compute functions on each cloud platform mentioned in #3 above	$146,027.06 of Snowflake capacity; to be burned down at the following rates: AWS: $3.41/credit Azure: $3.41/credit Azure Government: $4.77/credit Google: $3.41/credit
5. Price for three full years for a redundant data lake implementation as a "hot backup/failover" on a separate cloud platform than the one where the production system is deployed	$ - Included in the price above.
Grand Total, Items 1 through 5:	**$165,827.06**

(* Setup, configure, testing, install/configure required connectors, configuration and administration documentation, and basic administrator training.)

IN WITNESS WHEREOF, the parties have executed this Addendum as of the date of execution by both parties below.

Participating Entity: State of Idaho	Contractor: Carahsoft Technology Corporation
Signature: Justin Gross Digitally signed by Justin Gross Date: 2021.06.23 13:55:53 -06'00'	Signature: Kristina Smith
Name: Justin Gross	Name: Kristina Smith
Title: Procurement Supervisor	Title: Director of Contracts
Date: 6/23/2021	Date: 6/23/2021

Please email fully executed PDF copy of this document to PA@naspovaluepoint.org to support documentation of participation and posting in appropriate data bases.

Appendix A

Snowflake Terms of Service

1. USE OF SERVICE

1.1. Service Provision and Access; Client Software. Snowflake will make the Service available to Customer for the Subscription Term solely for use by Customer and its Users in accordance with the terms and conditions of this Agreement, the Documentation, and the Order Form. Customer may permit its Contractors and Affiliates to serve as Users provided that any use of the Service by each such Contractor or Affiliate is solely for the benefit of Customer or such Affiliate. Customer shall be responsible for each User's compliance with this Agreement. To the extent use of a Service requires Customer to install Client Software, Snowflake grants to Customer a limited, non-transferable, non-sublicensable, non-exclusive license during the Subscription Term to use the object code form of the Client Software internally in connection with Customer's and its Affiliates' use of the Service, subject to the terms and conditions of this Agreement and the Documentation.

During the term of this Agreement, Customer accepts that Snowflake will grant to a reseller (or resellers) the non-exclusive right to resell the Service to Customer pursuant to the terms set forth in this Agreement and the definitive terms entered into by and between Snowflake and said reseller (or resellers). For the avoidance of doubt, the foregoing does not prohibit Snowflake from selling the Service directly to the Customer. Customer may procure use of any Service from an authorized reseller of Snowflake ("Reseller") pursuant to a separate Reseller Order Form that references this Agreement. Customer's use of any Service procured through a Reseller will be subject to the terms of this Agreement and all fees payable for such use shall be payable pursuant to the terms set forth in the Reseller Order Form.

1.2. Affiliates. Customer Affiliates may purchase services from Snowflake by executing an Order Form or Statement of Work ("**SOW**") which is governed by the terms of this Agreement. This will establish a new and separate agreement between the Customer Affiliate and the Snowflake entity signing such Order Form. If the Customer Affiliate resides in a different country than Customer, then the Order Form may include modifications to terms applicable to the transaction(s) (including but not limited to tax terms and governing law).

1.3. Compliance with Applicable Laws. Snowflake will provide the services in accordance with its obligations under laws and government regulations applicable to Snowflake's provision of the services to its customers generally, including, without limitation, those related to data privacy and data transfer, international communications, and the exportation of technical or personal data, without regard to Customer's particular use of the services and subject to Customer's use of the services in accordance with this Agreement.

1.4. Sample Data; Third Party Applications. Snowflake may make Sample Data available for Customer. Customer acknowledges that Sample Data is example data only, which may not be complete, current, or accurate. Customer will not (and will not permit any third party to) copy or export any Sample Data and agrees that Snowflake may delete or require Customer to cease using Sample Data at any time upon advance notice. Snowflake may also provide URL links or interconnectivity within the Service to facilitate Customer's use of Third Party Applications, at Customer's sole discretion. Notwithstanding the foregoing, any procurement or use of Third Party Applications are solely between Customer and the applicable third party and Snowflake will have no liability for such Third Party Applications.

1.5. Customer-Controlled Data Sharing Functionality.

(a) Generally. The Service includes the capability for Customer, at its option and in its sole discretion, to share Customer Data with other Customer-designated Snowflake customers and/or Read Only Users (as 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 Customer is 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 Provider remains responsible for its Customer Data as set forth in the Agreement.

(c) When Customer is 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 Service and to Provider's data (including identifying Consumer in connection with such information) and share it with Provider.

(d) Reader Accounts. When Customer is Provider, Customer may, at its option and in its 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 Customer; provided that: (1) Customer 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) Customer represents that it has the right to share with Snowflake any personal information about Read Only Users that Customer provides to Snowflake; (5) Customer shall be responsible for any acts or omissions on the part of Read Only Usersin their use of the Reader Accounts as if they were acts or omissions of Customer; and (6) Customer will be fully responsible for all costs, damages,losses, liabilities, and expenses (including reasonable attorneys' fees) brought by any Read Only Consumers or Read Only Users or arising from orrelating to any acts or omissions by Read Only Consumers or Read Only Users in their use of the Reader Accounts.

1.6. General Restrictions. Customer will not (and will not permit any third party to): (1) sell, rent, lease, license, distribute, provide access to, sublicense, or otherwise make available any Service (or Deliverables, if applicable) to a third party (except as set forth in the Documentation for Service features expressly intended to enable Customer to provide its third parties with access to Customer Data, or the SOW, as applicable) or in a service bureau or outsourcing offering; (2) use any Service to provide, or incorporate any Service into, any general purpose data warehousing service for the benefit of a third party; (3) reverse engineer, decompile, disassemble, or otherwise seek to obtain the source code or non-public APIs to any Service, except to the extent expressly permitted by applicable law (and then only upon advance written notice to Snowflake); (4) remove or obscure any proprietary or other notices contained in any Service; or (5) use any services in violation of the Acceptable Use Policy, which is incorporated herein by this reference and as attached hereto as Exhibit A and incorporated herein by this reference.

1.7. Preview Service Terms. Snowflake may make available to Customer certain products, features, services, software, regions or cloud providers 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**"). Customer may access and use Previews solely for its internal evaluation purposes and in accordance with the Preview Terms. In the event of any conflict between this Agreement and the Preview Terms, the Preview Terms shall govern and control solely with respect to the Previews.

2. CUSTOMER DATA

2.1. Rights in Customer Data. As between the parties, Customer or its 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 Service as provided to Snowflake. Subject to the terms of this Agreement, Customer hereby grants 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 services to Customer or as may be required by law. In accordance with Carahsoft NASPO Agreement Section 23, Data Access Controls, to the extent Purchasing Entity's express written consent is required for any of the foregoing, such consent is deemed provided by Customer's signing of a purchase order for the Services.

2.2. Use Obligations.

(a) In General. Customer's use of the services and all Customer Data will comply with applicable laws and government regulations. Customer is solely responsible for the accuracy, content and legality of all Customer Data. Customer warrants that Customer has and will have sufficient rights in the Customer Data to grant the rights to Snowflake under this Agreement and that the Customer Data will not violate the rights of any third party.

(b) HIPAA Data. Customer agrees not to upload to any Service any HIPAA Data unless Customer has entered into a BAA with Snowflake. Unless a BAA is in place, Snowflake will have no liability under this Agreement for HIPAA Data, notwithstanding anything to the contrary in this Agreement or in HIPAA or any similar federal or state laws, rules or regulations. If Customer is permitted to submit HIPAA Data to a Service, then Customer may submit HIPAA Data to Snowflake and/or the Service only by uploading it as Customer Data. Upon mutual execution of the BAA, the BAA is incorporated by reference into this Agreement and is subject to its terms.

2.3. Data Privacy. The parties shall comply with the DPA, which is attached hereto as Exhibit B and incorporated herein by this reference.

3. SECURITY. The parties shall comply with the Security Policy, which is attached hereto as Exhibit C and incorporated herein by this reference.

4. INTELLECTUAL PROPERTY

4.1. Snowflake Technology. Customer agrees 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 Service, all Documentation and Client Software, any Deliverables (as defined in the TSA), 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 this Agreement, no right, title or interest in any Snowflake Technology is granted to Customer. Further, Customer acknowledges that the Service is offered as an online, hosted solution, and that Customer has no right to obtain a copy of the underlying computer code for any Service, 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 Customer or by any users of the Services relating to Snowflake's products or services ("**Feedback**"). For clarity, neither the Service, Documentation, Client Software, Deliverables, Feedback or Snowflake Technology are data obtained by the Subcontractor in the performance of the Master Agreement under Section 2(b) of Exhibit 1 to the Master Agreement: Software-as-a-Service, and accordingly, none will become the property of the Purchasing Entity.

4.2. Usage Data. Notwithstanding anything to the contrary in this Agreement, or the Carahsoft NASPO Agreement Section 23, Data Access Controls, Section 26, Purchasing Entity Data, or Exhibit 1 to the Master Agreement: Software-as-a-Service, Snowflake may collect and use Usage Data to develop, improve, support, and operate its products and services. Snowflake may not share any Usage Data that includes Customer's Confidential Information with a third party except (i) in accordance with Section 5 (Confidential Information) of this Agreement, or

(ii) to the extent the Usage Data is aggregated and anonymized such that Customer and Customer's Users cannot be identified.

4.3. Marketing. [Reserved.]

5. 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 cooperate in any effort to obtain confidential treatment of the Confidential Information. The Receiving Party acknowledges that disclosure of Confidential Information would cause substantial harm for which damages alone would not be a sufficient remedy, and therefore that upon any such disclosure by the Receiving Party, the Disclosing Party will be entitled to seek appropriate equitable relief in addition to whatever other remedies it might have at law.

6. FEES AND PAYMENT; TAXES; PAYMENT DISPUTES

6.1. Fees and Payment. All Fees and payment terms are as set forth in the applicable Order Form. Except as expressly set forth in this Agreement, all payment obligations are non-cancelable and Fees are non-refundable. If Customer issues a purchase order upon entering into an Order Form, then: i) any such purchase order submitted by Customer is for its internal purposes only, and Snowflake rejects, and in the future is deemed to have rejected, any purchase order terms to the extent they add to or conflict in any way with this Agreement or the applicable Order Form and such additional or conflicting terms will have no effect, (ii) it shall be without limitation to Snowflake's right to collect Fees owing hereunder, iii) it shall be for the total Fees owing under the applicable Order Form, and iv) on request, Snowflake will reference the purchase order number on its invoices (solely for administrative convenience), so long as Customer provides the purchase order at least ten (10) business days prior to the invoice date.

6.2. Taxes. Fees do not include Taxes. Customer is responsible for paying all Taxes associated with its purchases hereunder including without limitation all use or access of the Service by its Users. If Snowflake has the legal obligation to pay or collect Taxes for which Customer is responsible under this Section, Snowflake will invoice Customer and Customer will pay that amount unless Customer provides Snowflake with a valid tax exemption certificate authorized by the appropriate taxing authority. Taxes will not be deducted from payments to Snowflake, except as required by applicable law, in which case Customer will increase the amount payable as necessary so that, after making all required deductions and withholdings, Snowflake receives and retains (free from any liability for Taxes) an amount equal to the amount it would have received had no such deductions or withholdings been made. Upon Snowflake's request, Customer will provide to Snowflake its proof of withholding tax remittance to the respective tax authority. Customer will provide its VAT/GST Registration Number(s) on the Order Form to confirm the business use of the ordered services.

6.3. Payment Disputes. Snowflake will not exercise its rights under Section 7.2 (Termination for Cause) or Section 7.5(a) (Suspension of Service) with respect to non-payment by Customer if Customer is disputing the applicable charges reasonably and in good faith and is cooperating diligently to resolve the dispute. If the parties are unable to resolve such a dispute within thirty (30) days, each party shall have the right to seek any remedies it may have under this Agreement, at law or in equity, irrespective of any terms that would limit remedies on account of a dispute. For clarity, any undisputed amounts must be paid in full.

6.4 Reseller Orders. If Customer has procured the Service or Technical Services through a Snowflake-authorized distributor or reseller ("**Reseller**"), then different terms regarding invoicing, payment and taxes may apply as specified between Customer and its Reseller. Customer acknowledges that: (a) Snowflake may share information with the Reseller related to Customer's use and consumption of the Service or Technical Services for account management and billing purposes; (b) the termination provisions below will also apply if Customer's Reseller fails to pay applicable fees; and (c) Reseller is not authorized to make any changes to this Agreement or otherwise authorized to make any warranties, representations, promises or commitments on behalf of Snowflake or in any way concerning the Service or Technical Services.

7. TERM AND TERMINATION

7.1. Term. This Agreement is effective as of the Effective Date and will remain in effect until terminated in accordance with its terms. If there is no SOW, Order Form or Retrieval Right currently in effect, either party may terminate this Agreement upon written notice to the other party. Each Order Form will terminate upon expiration of the applicable Subscription Term, unless expressly stated otherwise therein or in this Agreement.

7.2. Termination for Cause. Either party may terminate this Agreement (including all related Order Forms) if the other party (a) fails to cure any material breach of this Agreement (including a failure to pay Fees) within thirty (30) days after written notice; (b) ceases operation without a successor; or (c) seeks protection under any bankruptcy, receivership, trust deed, creditors' arrangement, composition, or comparable proceeding, or if any such proceeding is instituted against that party and is not dismissed within 60 days. Except where an exclusive remedy is specified, the exercise of either party of any remedy under this Agreement, including termination, will be without prejudice to any other remedies it may have under this Agreement, by law or otherwise. For any termination of this Agreement by Customer for cause in accordance

with Section 7.2(a), Customer shall be entitled to a refund of any unused Fees Customer has pre-paid for the Service purchased hereunder.

7.3. Effect of Termination; Customer Data Retrieval. In accordance with Carahsoft NASPO Agreement Section 33(a), Transition Assistance, Exhibit 1 to the Master Agreement: Software-as-a-Service, Section 7 Termination and Suspension of Service, and Section 15, Import and Export of Data, the following shall fulfill Snowflake's obligations under those sections: upon written notice to Snowflake, Customer will have up to thirty (30) calendar days from termination or expiration of this Agreement to access the Service solely to the extent necessary to retrieve Customer Data ("**Retrieval Right**"). If Customer exercises its Retrieval Right, this Agreement 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 this 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 Service (including any related Snowflake Technology) and delete all copies of Client Software, Documentation, any Service passwords or access codes, and any other Snowflake Confidential Information in its possession. Snowflake's obligations under this section are only with respect to Customer Data and not Data. Further, in accordance with Section 7(e), to ensure permanent deletion, Customer must implement Tri-Secret Secure.

7.4. Survival. The following Sections will survive any expiration or termination of this Agreement: 1.5 (General Restrictions), 4 (Intellectual Property), 5 (Confidentiality), 6.1 (Fees and Payment), 6.2 (Taxes), 7 (Term and Termination), 8.2 (Warranty Disclaimer), 11 (Indemnification), 12 (Limitation of Remedies and Damages), 13 (General Terms), and 14 (Definitions).

7.5. Suspension of Service. In addition to any of its other rights or remedies (including, without limitation, any termination rights) set forth in this Agreement, Snowflake reserves the right to suspend provision of services; (a) if Customer (or Customer's Reseller, if applicable) is thirty (30) days or more overdue on a payment, (b) if Snowflake deems such suspension necessary as a result of Customer's breach of Sections 1.5 (General Restrictions) or 2.2 (Use Obligations), (c) if Snowflake reasonably determines suspension is necessary to avoid material harm to Snowflake or its other customers, including if the Service is experiencing denial of service attacks, mail flooding, or other attacks or disruptions outside of Snowflake's control, or (d) as required by law or at the request of governmental entities.

8. WARRANTY.

8.1. Service Warranty. Snowflake warrants that (a) each Service operates in substantial conformity with the applicable Documentation, and (b) Technical Services and Deliverables will be provided in a professional and workmanlike manner and substantially in accordance with the specifications in the applicable SOW. If Snowflake is not able to correct any reported non-conformity with the warranties provided in the Carahsoft NASPO Agreement, Section 32, Warranty, or the warranties described in (a) or (b) of this section, either party may terminate the applicable Order Form (or SOW, 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 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 SOW.

8.2. Mutual Warranty. Each party warrants that it has validly entered into this Agreement and has the legal power to do so.

9. SUPPORT AND AVAILABILITY. During a Subscription Term, Snowflake will provide Customer the level of support for the Service specified in the applicable Order Form, in accordance with the Support Policy, which is attached hereto as Exhibit D and incorporated herein by this reference.

10. TECHNICAL SERVICES.

10.1. Provision of Technical Services. Snowflake will perform the Technical Services for Customer as set forth in each applicable Statement of Work, subject to the terms and conditions of the Agreement. The Snowflake personnel that Snowflake assign to perform the Technical Services will be professional and qualified in the performance of the applicable Technical Services. If Customer, in its reasonable judgement, believes that Snowflake personnel assigned to a project do not meet the requirements in this Section, Snowflake will in good faith discuss alternatives and will replace Snowflake personnel as reasonably necessary. Where expressly stated in an SOW, Snowflake will not remove Personnel expressly named in the SOW without the prior written permission of Customer.

10.2 Assistance. Customer acknowledges that timely access to applicable Customer Materials (defined below), resources, personnel, equipment or facilities is necessary for the provision of Technical Services. Customer agrees to provide such access and to reasonably cooperate with Snowflake during a Technical Services project. Snowflake will have no liability for any delay or deficiency to the extent resulting from Customer's breach of its obligations under this Section 10.

10.3 Customer Materials. Customer hereby grants Snowflake a limited right to use any materials provided to Snowflake in connection with Technical Services projects (the "Customer Materials") solely for the purpose of providing Technical Services to Customer. Customer will retain any of its rights (including all intellectual property rights) in and to the Customer Materials. Snowflake will treat Customer Materials subject to the confidentiality obligations under Section 5 (Confidentiality). Customer warrants that Customer has and will have sufficient rights in the Customer Materials to grant the rights to Snowflake under this Agreement and that the Customer Materials will not violate the rights of any third party rights.

10.4 Access to Customer Data. With respect to access to any Customer Data, Customer is solely responsible for ensuring that both the duration and scope of access is strictly limited to the access required under the specific SOW. Customer agrees that it 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 a SOW, Customer must ensure that (a) any access to Customer Data that it grants is limited to read-only access in Customer's development environment for the Snowflake Service (and Customer will not grant access to any other environment, such as the its test, prod or disaster recovery) and (b) Customer will not grant access to any Customer Data that is unencrypted or contains personal data . To the extent access to Customer Data is granted, Customer will provide Snowflake with: (i) secure Customer workstations and networks for accessing Customer Data that are monitored, managed, configured, supported and maintained by Customerand (ii) unique user ID/passwords to each Snowflake resource that requires access to Customer Data, and these credential will be solely managed by Customer.

10.5 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. Subject to the terms and conditions of the Agreement (including the restriction in Section 1.6 (General Restrictions)), Snowflake hereby grants Customer a limited, non-exclusive, royalty-free, non-transferable worldwide license to use the Deliverables internally solely in connection with such Customer's use of the Snowflake Service during the period in which such Customer has valid access to the Snowflake Service. The parties may mutually agree to SOWs with additional terms and restrictions related to the use of Deliverables provided as part of that project, in which case those terms and restrictions will also apply for purposes of those Deliverables only.

10.6 Change Orders; Other Terms. Customer may submit written requests to Snowflake to change the scope of Technical Services under an existing Statement of Work. Snowflake will promptly notify Customer if it believes that the requested change requires an adjustment to the fees, schedule, assumptions or scope for the performance of the Technical Services. Neither party is bound by a change request unless agreed in writing by both parties pursuant to a mutually executed amendment or change order (each, a "Change Order"). Snowflake will continue to perform Technical Services pursuant to the existing Statement of Work unless the parties mutually agree to such amendment or change order. Snowflake may use subcontractors to deliver Technical Services but will remain responsible for their performance of those Technical Services under the applicable terms and conditions of this Agreement. For clarity, Customer will be responsible for any consumption and other fees for the Service that are generated as part of the Technical Services. If applicable, Snowflake will provide the Technical Services pursuant to the TSA, which is attached hereto as Exhibit E and incorporated herein by this reference.

11. INDEMNIFICATION

11.1. Indemnification by Snowflake. Snowflake will 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 Snowflake (including reasonable attorneys' fees) resulting from such claim. If Customer's use of the Service or Deliverable results (or in Snowflake's opinion is likely to result) in an infringement claim, Snowflake may either: (a) substitute functionally similar products or services; (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 Snowflake 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

11.2. Indemnification by Customer. [Reserved.]

11.3. Indemnification Procedures. In the event of a potential indemnity obligation under this Section 11, the indemnified party will: (i) promptly notify the indemnifying party in writing of the claim, (ii) allow the indemnifying 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 indemnifying party, provide all necessary cooperation at the indemnifying party's expense. Failure by the indemnified party to notify the indemnifying party of a claim under this Section 11 shall not relieve the indemnifying party of its obligations under this Section 11, however the indemnifying party shall not be liable for any litigation expenses that the indemnified 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 indemnifying party in accordance with this Section. The indemnifying party may not settle any claim that would bind the indemnified 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 indemnified party, without the indemnified party's prior written consent, such consent not to be unreasonably withheld, conditioned or delayed. Any indemnification obligation under this Section 11 will not apply if the indemnified party settles or makes any admission with respect to a claim without the indemnifying party's prior written consent.

12. GENERAL TERMS

12.1. Assignment. This Agreement will bind and inure to the benefit of each party's permitted successors and assigns. Neither party may assign this Agreement without the advance written consent of the other party, except that either party may assign this Agreement in its entirety in connection with a merger, reorganization, acquisition, or other transfer of all or substantially all of such party's assets or voting securities to such party's successor; and Snowflake may assign this Agreement in its entirety to any Affiliate. Each party shall promptly provide notice of any such assignment. Any attempt to transfer or assign this Agreement except as expressly authorized under this Section will be null and void.

12.2. Severability; Interpretation. If a court of competent jurisdiction holds any provision of this Agreement to be unenforceable or invalid, that provision will be limited to the minimum extent necessary so that this Agreement will otherwise remain in effect. Section headings are inserted for convenience only and shall not affect the construction of the agreement.

12.3. Dispute Resolution. Each party agrees that before it seeks any form of legal relief (except for a provisional remedy as explicitly set forth below) it shall provide written notice to the other party of the specific issue(s) in dispute (and reference the relevant provisions of the contract between the parties which are allegedly being breached). Within thirty (30) days after such notice, knowledgeable executives of the parties shall hold at least one meeting (in person or by video- or tele-conference) for the purpose of attempting in good faith, to resolve the dispute. The parties agree to maintain the confidential nature of all disputes and disagreements between them, including, but not limited to, informal negotiations, mediation or arbitration, except as may be necessary to prepare for or conduct these dispute resolution procedures or unless otherwise required by law or judicial decision. The dispute resolution procedures in this Section shall not apply to claims subject to indemnification under Section 11 (Indemnification) or prior to a party seeking a provisional remedy related to claims of misappropriation or ownership of intellectual property, trade secrets or Confidential Information.

12.4. Governing Law; Jurisdiction and Venue; Snowflake Affiliate. Unless otherwise specified in the Order Form: (i) this Agreement will be governed by the laws of the United States without regard to conflicts of laws provisions thereof, and without regard to the United Nations Convention on the International Sale of Goods.

12.5. Notice. Any notice or communication required or permitted under this Agreement will be in writing to the parties at the addresses set forth in this Agreement or at such other address as may be given in writing by either party to the other in accordance with this Section and will be deemed to have been received by the addressee: (i) if given by hand, immediately upon receipt; (ii) if given by overnight courier service, the first business day following dispatch; (iii) if given by registered or certified mail, postage prepaid and return receipt requested, the second business day after such notice is deposited in the mail; or (iv) if given by email, immediately upon receipt. Notwithstanding the foregoing, except for notices pertaining to non-payment and except as otherwise expressly permitted in this Agreement or in an Order Form, notices related to termination of this Agreement or any claims (including without limitation breach, warranty or indemnity) may not be given via email. Email notifications to Snowflake shall be to legalnotices@snowflake.com.

12.6. Amendments; Waivers. No supplement, modification, or amendment of this Agreement will be binding, unless executed in writing by a duly authorized representative of each party to this Agreement, except as expressly set forth herein. No waiver will be implied from conduct or failure to enforce or exercise rights under this Agreement, nor will any waiver be effective unless in a writing signed by a duly authorized representative on behalf of the party claimed to have waived. No terms or conditions stated in a Customer purchase order, vendor onboarding process or web portal, or any other Customer order documentation (excluding Order Forms) shall be incorporated into or form any part of this Agreement, and all such terms or conditions shall be null and void, notwithstanding any language to the contrary therein, whether signed before or after this Agreement.

12.7. Entire Agreement. This Agreement is the complete and exclusive statement of the mutual understanding of the parties and supersedes and cancels all previous written and oral agreements and communications relating to the subject matter of this Agreement. Snowflake may change and update any Service (in which case Snowflake may update the applicable Documentation accordingly), subject to the warranty in Section 8.1 (Service Warranty).

12.8. Third Party Beneficiaries. There are no third-party beneficiaries under this Agreement.

12.9. Force Majeure. Neither party will be liable to the other for any delay or failure to perform any obligation under this Agreement (except for a failure to pay Fees) if the delay or failure results from 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.

12.10. Independent Contractors. The parties to this Agreement are independent contractors. There is no relationship of partnership, joint venture, employment, franchise or agency created hereby between the parties. Neither party will have the power to bind the other or incur obligations on the other party's behalf without the other party's prior written consent and neither party's employees are eligible for any form or type of benefits, including, but not limited to, health, life or disability insurance, offered by the other party to its employees.

12.11. Export Control. Customer agrees to comply with all export and import laws and regulations of the United States and other applicable jurisdictions. Without limiting the foregoing, (i) Customer represents and warrants that it is 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) Customer will not (and will not permit any third parties to) access or use any Service in violation of any U.S. export embargo, prohibition or restriction, and (iii) Customer will not submit to any Service any information that is controlled under the U.S. International Traffic in Arms Regulations.

12.12. Federal Government End Use Provisions. Snowflake provides the Service, including all related software and, to the extent applicable the Snowflake Technology, for ultimate federal government end use solely in accordance with the following: Government technical data and software rights related to the Service include only those rights customarily provided to the public as defined in this Agreement. 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) and DFAR 227.7202-3 (Rights in Commercial Computer Software or Computer Software Documentation). If a government agency has a need for rights not granted under these terms, it must negotiate with Snowflake to determine if there are acceptable terms for granting those rights, and a mutually acceptable written addendum specifically granting those rights must be included in any applicable agreement.

12.13. Counterparts. This Agreement may be executed in counterparts, each of which will be deemed an original and all of which together will be considered one and the same agreement.

13. Reseller Orders. Customer may procure the Service directly from Reseller pursuant to a separate agreement that includes the Reseller Order Form and other commercial terms (a "Reseller Arrangement"). Snowflake will be under no obligation to provide the Service to Customer under a Reseller Arrangement if it has not received a Reseller Order Form for Customer. Reseller is not authorized to make any changes to this Agreement or otherwise authorized to make any warranties, representations, promises or commitments on behalf of Snowflake or in any way concerning the Service.

14.1 Sharing of Service Data with Reseller. If Customer procured the Service through a Reseller Arrangement, then Customer agrees that Snowflake may share certain Service Data with Reseller related to Customer consumption of the Service. This section shall not be read to conflict with Carahsoft NASPO Agreement Sections 23, Data Access Controls Section 26, Purchasing Entity Data, or Exhibit 1 to the

Master Agreement: Software-as-a-Service. Sharing Service Data with a Reseller under this section shall be considered required to "fulfill Subcontractor's obligations under this Agreement" in accordance with Section 23, Data Access Controls, and "strictly necessary to provide Service to the Purchasing Entity" in accordance with Section 26, Purchasing Entity Data.

14.2 Payment Provisions and Refunds with Reseller. If Customer procured the Service through a Reseller Arrangement, then Customer agrees that Reseller will determine the prices at which Service(s) are sold to the Customer. Further, all payment provisions will be as set forth in Customer's arrangement with the Reseller. Similarly, all refunds that may accrue under the terms of this agreement will need to be obtained through such Reseller.

14. DEFINITIONS

"**Acceptable Use Policy**" means Snowflake's acceptable use policy, attached as Exhibit 1.

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

"**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.

"BAA" means a business associate agreement governing the parties' respective obligations with respect to any HIPAA Data uploaded by Customer to the Service in accordance with the terms of this Agreement.

"**Client Software**" is any desktop client software included in the applicable Service that is made available to Customer by Snowflake for installation on end user computers.

"**Confidential Information**" shall have the meaning set forth in the Carahsoft NASPO Agreement. Confidential Information shall also mean all Snowflake Technology and the terms and conditions of this Agreement.

"Contractor" means the independent contractors and consultants permitted by Customer to serve as Users of the Service.

"**Customer Data**" means any data or data files of any type that are uploaded by or on behalf of Customer to the Service for storage in a data repository. For clarity, where a Party has a right or obligation under the Carahsoft NASPO Agreement with respect to "Customer Data" and not "Data" such right or obligation shall be limited to Customer Data.

"**Data Protection Claims**" means any claims arising from a party's breach of Section 2.3 (Data Privacy), 3 (Security), or 5 (Confidentiality), where such breach results in the unauthorized disclosure of Customer Data (as defined under the Security Policy), or breach of Section 2.2 (Use Obligations).

"**Deliverables**" means the guides, code (including SQL queries) or other deliverables that Snowflake provides to Customer 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.

"**Disclosing Party**" is defined in Section 5 (Confidential Information).

"**Documentation**" means Snowflake's technical documentation and usage guides for the applicable Service made available at https://docs.snowflake.net or through the Service.

"DPA" means the Customer Data Processing Addendum attached here to as Exhibit B and incorporated herein by this reference.

"**Excluded Claims**" means (a) Customer's breach of any of Section 2.2 (Use Obligations); (b) a party's breach of its obligations in Section 5 (Confidential Information) (but excluding obligations and/or claims relating to Customer Data); (c) either party's express obligations under Section 11 (Indemnification); and (d) liability which, by law, cannot be limited.

"**Feedback**" is defined in Section 4.1 (Snowflake Technology).

"**Fees**" means the fees payable by Customer for the applicable Service or Technical Services, as set forth in an Order Form or Statement of Work. For Technical Services, the terms Fees also includes travel, lodging, meal and other expenses incurred in the course of providing Technical Services, unless otherwise specified in the applicable SOW.

"**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 a Snowflake ordering document (and/or SOW, if applicable) executed by both Customer and Snowflake which specifies the services being provided by Snowflake and that is governed by this Agreement.

"Preview Terms" means the Preview Terms located at https://www.snowflake.com/legal-gov/.

"Reader Accounts", "Read Only Consumers", and "**Read Only Users"** are respectively as defined in Section 1.4(d) (Reader Accounts).

"**Receiving Party**" is defined in Section 5 (Confidentiality).

"Reseller Order Form" means a duly signed ordering document between Reseller and Customer that references this Agreement and the Service being provided by Snowflake pursuant to this Agreement and pricing and payment terms determined by Reseller. For clarity, Snowflake is not a party to the Reseller Order Form.

"Retrieval Right" is defined in Section 7.3 (Effect of Termination; Customer Data Retrieval).

"**Sample Data"** means any data (including from third-party sources) provided or made available to Customer by Snowflake solely for Customer's internal testing, evaluation, and other non-productive use of the Service during the Subscription Term.

"Security Policy" means the Snowflake Security Policy attached hereto as exhibit C and incorporated herein by this reference.

"**Service**" means a Snowflake software-as-a-service offering made generally available and ordered by Customer as set forth in an Order Form.

"**Snowflake**" means Snowflake, Inc.

"**Snowflake Technology"** is defined in Section 4.1 (Snowflake Technology).

"**SOW**" or "**Statement of Work**" means an Order Form (as defined above) or statement of work mutually agreed by the parties for the purchase of Technical Services that is governed by this Agreement.

"**Subscription Term**" means the set term designated on an Order Form.

"**Support Policy**" means the Snowflake Support Policy attached hereto as Exhibit D and incorporated herein by this reference.

"**Taxes**" means taxes, levies, duties or similar governmental assessments of any nature, including, for example, any sales, use, GST, value-added, withholding, or similar taxes, whether domestic or foreign, or assessed by any jurisdiction, but excluding any taxes based on net income, property, or employees of Snowflake.

"**Technical Services**" shall have the meaning set forth in the TSA.

"TSA" means the Technical Services Addendum attached hereto as Exhibit E and incorporated herein by this reference, describing Snowflake's current terms for the provision of Technical Services.

"Third Party Applications" means separate services or applications (and other consulting services related thereto), procured by Customer from a party other than Snowflake that can be used in connection with the Service.
"**Usage Data**" means query logs, and any data (other than Customer Data) relating to the operation, support and/or about Customer's use of the Service.

"User" means the persons designated and granted access to the Service by or on behalf of Customer, including its and its Affiliates' Contractors.

"VAT/GST Registration Number" means the value added tax/GST registration number of the business location(s) where Customer is legally registered and the ordered services are used for business use.

Exhibit A

Snowflake Acceptable Use Policy

This Snowflake acceptable use policy ("**AUP**") sets forth certain restrictions on accessing and using Snowflake Inc.'s and its affiliates (collectively, "**Snowflake**", "**We**", "**Our**" or "**Us**") products and services, including Snowflake's software-as-a-service offering, and any equipment (including servers or networks) used in connection therewith (collectively, "**Offerings**") by you or someone on your behalf ("**You**" or "**Your**") under your agreement with Snowflake for such Offerings ("**Agreement**"). The restrictions set forth in this AUP are not exhaustive. You may not use the Offerings:

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 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 any 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 any Offerings in a way that violates the Agreement or use any Offerings to access or use any intellectual property in or related to the Offerings except as permitted under the Agreement;
6. to copy the Offerings, or any part, feature, function or user interface thereof except as expressly allowed for Client Software under the Agreement; or
7. in order to benchmark Offerings or to build similar or competitive products or services.

Any capitalized terms used but not defined herein shall have the meaning set forth in the Agreement or the Documentation, as applicable. 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 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 Offerings.

Last Updated: 2018November19

Exhibit B

Snowflake Customer Data Processing Addendum
(June 30, 2020)

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**") (such agreement, the "**Agreement**"). This DPA shall be effective on the effective date of the Agreement, unless this DPA is separately executed in which case it's effective on the date of the last signature ("**Effective Date**"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. Unless otherwise specified and agreed to by the Parties in writing, this DPA shall be considered sufficient fulfillment of Snowflake's obligations to comply with applicable laws, under NASPO Agreement, Section 31 Data Privacy.

1. Definitions.

"**Account**" means Customer's account in the Services 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 who is the Data Controller 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 applicable to the respective party in its role in the Processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Law and the CCPA.

"**Data Subject**" means the identified or identifiable natural person to whom Customer Personal Data relates.

"**EU Data Protection Law**" means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**").

"**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.

"**Privacy Shield**" means the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Framework self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C(2016)4176 of 12 July 2016 and by the Swiss Federal Council on January 11, 2017 respectively.

"**Privacy Shield Principles**" means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of 12 July 2016 (as may be amended, superseded or replaced).

"**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, organisation, 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 in accordance with 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 under the Agreement, including but not limited to support and technical services.

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

"**Standard Contractual Clauses**" means the Standard Contractual Clauses for Processors as approved by the European Commission in the form set out in Annex A**.**

"**Sub-processor**" means any third-party Data Processor 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.

3. Roles and Scope of Processing.

3.1 **Role of the Parties**. As between Snowflake and Customer, Customer is either the Data Controller of Customer Personal Data, or if Customer is acting on behalf of a third-party Data Controller, then a Data Processor, and Snowflake shall Process Customer Personal Data only as a Data Processor acting on behalf of Customer and, with respect to CCPA, as a "service provider" as defined therein. To the extent any Service 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 Customer's complete and final instructions to Snowflake for the Processing of Customer Personal Data. Any Processing outside the scope of these instructions will require prior written agreement between Customer and Snowflake.

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

(a) No entity other than Customer may provide further Processing instructions to Snowflake and Customer must accordingly communicate any additional Processing instructions from its Authorized Affiliates directly to Snowflake;

(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 or 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) Duration: Notwithstanding expiry or termination of the Agreement, this DPA and Standard Contractual Clauses (if applicable) will remain in effect until, and will automatically expire upon, deletion of all Customer Personal Data as described in this DPA.

(c) Purpose: Snowflake shall Process Customer Personal Data only for the Purposes.

(d) Nature of the Processing: Snowflake provides Services as described in the Agreement.

(e) 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).

(f) Types 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, usage data, cookies data, location data).

(g) 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' (as defined in the GDPR) 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, and the Processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

4. Sub-processing.

4.1 **Authorized Sub-processors**. Customer specifically authorizes the engagement of those Sub-processors listed at https://www.snowflake.com/legal/snowflake-sub-processors/ ("**Sub-processor Site**") as of the Effective Date 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 in 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 in this DPA.

4.3 **Changes to Sub-processors.** Snowflake shall make available on its Sub-processor Site a mechanism for Customer to subscribe to notifications of new Sub-processors. Snowflake shall provide such notification 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, Customer may object in writing to Snowflake's appointment of the new Sub-processor, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss Customer's concerns in good faith with a view to achieving resolution. If Customer can reasonably demonstrate 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 terminate 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 by providing written notice to Snowflake. 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 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 Policy found at https://www.snowflake.com/legal ("**Security Policy**"). 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. Snowflake may review and update its Security Policy from time to time, provided that any such updates shall not materially diminish the overall security of the Services or Customer Personal Data.

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**. Customer acknowledges that Snowflake will not assess the contents of Customer Personal Data to identify information subject to any specific legal requirements.

6. Customer Audit Rights.

6.1 Upon written request and at no additional cost to Customer, Snowflake shall provide Customer, 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 (i) Snowflake's ISO 27001 and PCI-DSS third-party certifications, (ii) Snowflake's SOC 1 Type II audit reports, SOC 2 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 (including inspection) of Snowflake's facilities. Following receipt by Snowflake of such request, Snowflake and Customer shall mutually agree in advance on the details of the audit, including 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 Snowflake's Confidential Information.

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. Expenses incurred by 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.

7.2 **Transfer Mechanisms.** For any transfers by Customer of Customer Personal Data from the European Economic Area and/or its member states, United Kingdom and/or Switzerland (collectively, "**Restricted Countries**" to Snowflake in a country which does not ensure an adequate level of protection (within the meaning of and to the extent governed by the Data Protection Laws of the Restricted Countries) (collectively, "**Third Country**"), such transfers shall be governed by a valid mechanism for the lawful transfer of Customer Personal Data recognized under Data Protection Laws, such as those directly below:

(a) **For transfers to Snowflake Inc:** Snowflake Inc. shall remain certified under the Privacy Shield and shall comply with the Privacy Shield Principles. If for any reason Inc. ceases to be certified under the Privacy Shield or it determines it can no longer meet its obligations to provide the same level of protection as required by the Privacy Shield Principles, Snowflake shall promptly notify Customer and shall work with Customer to take reasonable and appropriate steps to remediate.

(b) **For transfers not covered by 7.2.1 above:** To the extent the transfer mechanism identified in Section 7.2.1) does not apply to the transfer, is invalidated and/or Snowflake Inc. is not self-certified to the Privacy Shield, and Snowflake is located in a Third Country, Snowflake agrees to abide by and Process Customer Personal Data from the Restricted Countries in compliance with the Standard Contractual Clauses and for these purposes Snowflake shall be the "data importer" and Customer is the "data exporter" under the Standard Contractual Clauses (notwithstanding that Customer may be an entity located outside of the Restricted Country).

(c) Notwithstanding the foregoing, if Snowflake has adopted Binding Corporate Rules (BCRs) for Processors that cover the transfer of Customer Personal Data to a Third Country, then such BCRs shall govern the transfer of Customer Personal Data.

8. **Return or Deletion of Data.** Customer may retrieve or delete all Customer Personal Data upon expiration or termination of the Agreement 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. Notwithstanding the foregoing, Snowflake shall not be required to delete Customer Personal Data to the extent Snowflake is required by applicable law or order of a governmental or regulatory body to retain some or all of the Customer Personal Data. Where Snowflake is required to retain Customer Personal Data as set forth in the preceding sentence, then Snowflake will notify Customer of such requirement, to the extent legally permitted.

9. **Security Incident Response.**

9.1 **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 shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident.

9.2 **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.

10. **Cooperation.**

10.1 **Data Subject Requests.** To the extent legally permitted, Snowflake shall promptly notify Customer if Snowflake receives a request from a Data Subject that identifies Customer and seeks to exercise the Data Subject's right to access, rectify, erase, transfer or port Customer Personal Data, or to restrict the Processing of Customer Personal Data ("**Data Subject Request**"). The Service provides Customer with a number of controls that Customer may use to assist it in responding to a Data Subject Request and Customer will be responsible for responding to any such

Data Subject Request. To the extent that Customer is unable to access the relevant Customer Personal Data within the Services using such controls or otherwise, taking into account the nature of the Processing, Snowflake shall (upon Customer's written request) provide commercially reasonable cooperation to assist Customer in responding to any Data Subject Requests.

10.2 **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.

10.3 **Government Inquiries.** If compelled to disclose Customer Personal Data to a law enforcement or governmental entity, then Snowflake will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy to the extent Snowflake is legally permitted to do so.

11. Relationship with the Agreement.

11.1 The parties agree that this DPA shall replace and supersede any existing data processing addendum, attachment or exhibit (including the Standard Contractual Clauses (as applicable)) that Snowflake and Customer may have previously entered into in connection with the Services.

11.2 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 withthe 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 Associates Agreement between Customer and Snowflake ("**BAA**"), then the BAA shall prevail solely with respect to such HIPAA Data.

11.3 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 DPA and 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 either of the parties' obligations under the Agreement, each party agrees that any regulatory penalties incurred by the 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.

11.4 In no event shall this DPA or any party restrict or limit the rights of any Data Subject or of any competent supervisory authority.

11.5 This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement.

Annex A
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

THE PARTIES HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

1. Definitions

For the purposes of the Clauses:

'personal data', **'special categories of data'**, **'process/processing'**, **'controller'**, **'processor'**, **'data subject'** and **'supervisory authority'** shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

'the data exporter' means the controller who transfers the personal data;

'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

3. Third-party beneficiary clause

3.1 The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

3.2 The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.3 The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3.4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

5. Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may

remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

6. Liability

6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

6.3 The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

6.4 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

7. Mediation and jurisdiction

7.1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

7.2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8. Cooperation with supervisory authorities

8.1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

9. Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

10. Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

11. Subprocessing

11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

11.2 The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has

assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

11.3 The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

11.4 The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. Obligation after the termination of personal data processing services

12.1 The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2 The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed by the parties.

Data exporter*:* The data exporter is the entity identified as the "Customer" in the Data Processing Addendum in place between data exporter and data importer and to which these Clauses are appended ("**DPA**").

Data importer*:* The data importer is **Snowflake** (as defined in the DPA) to the extent based in a Third Country (as defined in the DPOA and described in Section 7.2.2). Snowflake provides enterprise cloud computing solutions, which process Customer Personal Data upon the instruction of the Customer in accordance with the terms of the Agreement.

Description of Data Processing: Please see Section 3.5 (Details of Processing) of the DPA for a description of the categories of data subjects, categories of data, special categories of data and processing operations.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Please see the Security Policy at https://www.snowflake.com/legal, which describes the technical and organisational security measures implemented by Snowflake.

Appendix 3 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and sets out the parties' interpretation of their respective obligations under specific Clauses identified below. Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

Clause 5(a): Suspension of data transfers and termination:

1. If the data exporter intends to suspend the transfer of personal data and/or terminate the Standard Contractual Clauses, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("**Cure Period**").
2. If after the Cure Period the data importer has not or cannot cure the non-compliance, then the data exporter may suspend or terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(f): Audit:

1. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures described in Section 6 (Customer Audit Rights) of the DPA.

Clause 5(j): Disclosure of subprocessor agreements

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.
2. The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter.
3. Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably can in connection with such subprocessing agreement to data exporter.

Clause 6: Liability

1. Any claims brought under the Clauses shall be subject to any aggregate limitations on liability set out in the Agreement. In no event shall any party limit its liability to a data subject with respect to any data subject rights under these Clauses.

Clause 11: Onward subprocessing

4. The parties acknowledge that Article 28 of the GDPR allows for the general written authorisation of a subprocessor subject to notice of, and the opportunity to object to, the subprocessor. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of the Standard Contractual Clauses, to engage onward subprocessors. Such consent is conditional on data importer's compliance with the requirements set out in Section 4 (Sub-processing) of the DPA.

Exhibit C

Snowflake Security Policy

(February 14, 2020)

Snowflake and Customer agree that this Security Policy is hereby incorporated into and made a part of their written agreement that references this policy (the "**Agreement**") and any capitalized terms used but not defined herein shall have the meaning set forth in the Agreement, as applicable. In the event of any conflict between the terms of the Agreement and this Security Policy, this Security Policy shall govern.

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 from a VPC/VNET 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 Policy, provided, however, that such updates shall be designed to enhance and not materially diminish the Security Program. This Security Policy fulfills Snowflake's obligations to comply with applicable laws related to data privacy and security, under Carahsoft NASPO Agreement Section 31, Data Privacy, Exhibit 1 to the Master Agreement: Software-as-a-Service, Section 9, Access to Security Logs and Reports, Section 10, Contract Audit, Section 11 Data Center Audit, and Section 13, Security.

1. **Snowflake's Audits & Certifications**
   - 1.1. The information security management system supporting the Service shall be assessed by one or more independent third-party auditors in accordance with the following audits and certifications ("**Third-Party Audits**"), on at least an annual basis:
     - ISO27001 (currently pending where Google is the Cloud Provider)
     - 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 (currently pending where Google is the Cloud Provider)
       - FedRAMP Ready in certain U.S. Regions (described in the Documentation)
       - HIPAA Compliance Report for Business Associates
   - 1.2. Third-Party Audits are made available to Customer as described in Section 8.2.1.
   - 1.3. To the extent Snowflake discontinues a Third-Party Audit, Snowflake will adopt or maintain an equivalent, industry-recognized framework.

2. **Hosting Location of Customer Data**
   - 2.1. Hosting Location. The hosting location of Customer Data is the Region offered by Snowflake and selected by Customer on an Order Form or as Customer otherwise configures via the services. Customer's obligations under this section are a prerequisite to Snowflake fulfilling its obligations under Exhibit 1 to the Master Agreement: Software-as-a-Service, Section 3, Data Location.

3. **Encryption**
   - 3.1. Encryption of Customer Data. Snowflake encrypts Customer Data at-rest using AES 256-bit (or better) encryption. Snowflake leverages 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. All Snowflake personnel access to the Cloud Environment is via a unique user ID and consistent with the principle of least privilege. All such access requires a VPN, with multi-factor authentication and passwords meeting or exceeding PCI-DSS length and complexity requirements.

4.2. 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 and testing 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 Policy.

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 Policy.

6. Physical and 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 270001 certification, shall include, but are not limited to, the following:

6.2.1. Physical access to the corporate office is controlled at building 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.[1]

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 do not have visibility to the content of Customer Data, it will be unlikely that Snowflake can provide information as to the particular nature of the Customer Data, or where applicable, the identities, number, or categories of affected data subjects. Snowflake's communications 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. Customer Rights & Shared Security Responsibilities

8.1. 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.

8.2. Customer Audit Rights.

8.2.1. Upon written request and at no additional cost to Customer, Snowflake shall provide Customer, 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 Policy in the form of (i) Snowflake's ISO 27001 and PCI-DSS third-party certifications, (ii) Snowflake's SOC 1 Type II audit report, SOC 2 Type II audit report, 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**").

[1] For clarity, where Customer's Agreement refers to the defined term "Security Breach", such reference shall be interpreted to refer to Security Incident, as defined herein.

8.2.2. Customer may also send a written request for an audit (including inspection) of Snowflake's facilities. Following receipt by Snowflake of such request, Snowflake and Customer shall mutually agree in advance on the details of the audit, including 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 are deemed Snowflake's Confidential Information.

8.2.3. Where the Auditor is a third-party (or Customer is using a third-party to conduct an approved Pen Test under Section 8.1), 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. Expenses incurred by Customer or the third party in connection with such audit, Pen Test, or review, shall be borne exclusively by Customer or the third party.

8.3. Sensitive Customer Data. Customer Data containing content regulated by PCI-DSS, HIPAA, FedRAMP, or containing any similarly regulated content may only be uploaded to Snowflake's Business Critical Edition or Virtual Private Snowflake Edition of the Service. Additionally, Customer must implement appropriate Customer-configurable security controls, including IP whitelisting and MFA for all User interactive logins (e.g., individuals authenticating to the Service).

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

8.4.1. Snowflake does not assess the content of Customer Data 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), and the pseudonymization of Customer Data;

8.4.2. to be responsible for managing and protecting its User roles and credentials, including but not limited to (i) requiring that all Users keep credentials confidential and not share such information with unauthorized parties, (ii) reporting to Snowflake any suspicious activities in the Account or if 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;

8.4.3. 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

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

Exhibit D

SNOWFLAKE

SUPPORT POLICY AND SERVICE LEVEL AGREEMENT
(November 18, 2019)

This Snowflake Support Policy and Service Level Agreement ("**Policy**") is subject to the agreement between you ("**Customer**") and Snowflake Inc. ("**Snowflake**") under which Snowflake provides cloud data platform that references this Policy ("**Agreement**"). This Policy describes Snowflake's support offering provided by Snowflake's technical support team ("**Snowflake Support**") in connection with support requests related to bugs, defects, or errors in the Service causing it to fail to perform in material conformance with the Documentation ("**Errors**"). This Policy also describes the service level commitments applicable to certain editions of the Service. Customer shall receive Standard Support or Premier Support for the Edition of the Service as described 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 Agreement.

I. Support

1. General Support Offering. Customer shall designate one primary contact who has Snowflake administrator privileges and up to the number of additional contacts permitted for the Support Level then-currently procured by Customer as described in Table 4 ("**Customer Contacts**"). Snowflake shall provide English-speaking remote assistance to Customer Contacts for questions or issues arising from any Errors, 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.

2. 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://support.snowflake.net (or such successor URL as may be designated by Snowflake) (such website, the "**Snowflake Lodge**") and designating the appropriate severity level according to Table 1 below, (b) submitting the support request to support@snowflake.com if Customer Contacts cannot access the Snowflake Lodge, or (c) if applicable to Customer's Support Level, and in the event Customer Contacts cannot access Snowflake Lodge or email, they may contact Snowflake Support by phone at the intake phone number identified in the Snowflake Lodge solely for purposes of having the support request submitted on their behalf (collectively, 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.

3. 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's 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), and (d) provide contact information for the Customer Contact most familiar with the issue. Unless Customer expressly designates the Severity Level, the Support Case will default to Severity Level four. 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 enchancement or feature requests, Snowflake shall treat those tickets as closed once the request has been forwarded internally.

4. Premier Support. If Customer is receiving Premiere Support Level, 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 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 Lodge ("**Case Escalation**"). Any Support Case escalated by Customer will be directed to Snowflake's management team for consideration.

5. 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 desigated 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.

6. 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 Lodge. 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	**Standard Support**	**Premier Support**
	Initial Response Time Target	
Severity Level 1 (Critical Severity)	Four (4) Business Hours	One (1) Hour
Severity Level 2 (High Severity)	Eight (8) Business Hours	Two (2) Business Hours
Severity Level 3 (Medium Severity)	Two (2) Business Days	One (1) Business Day
Severity Level 4 (Low Severity)	Four (4) Business Days	Two (2) Business Days

7. 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. 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)**"). If the Customer Contact that submitted the Support Case is unresponsive or unreachable, Snowflake may downgrade the Severity Level by one level. 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 will discuss in an effort to come to mutual agreement. If disagreement remains after discussion, each party will escalate within its organization and use good faith efforts to mutually agree on the appropriate Severity Level.

Table 3: Global Snowflake Support Hours			
Snowflake Service Region	**Standard & Premier Support Business Hours**		
	Sev 1 (Premier)	**Sev 1 (Standard) & Sev 2-4**	**Excluded Holidays Sev 2-4**
North America	24x7x365	6AM-6PM PT Mon-Fri	Recognized U.S. Federal Holidays
EU	24x7x365	6AM-6PM CE Mon-Fri	Recognized EU Bank Holidays
Asia Pacific	24x7x365	6AM-6PM AEDT Mon-Fri	Recognized APAC Holidays

Table 4: Support Level Entitlements		
Entitlements	**Standard**	**Premier**
Toll-Free phone access 24x7	N	Y
Snowflake Lodge (knowledge-base, forums, articles, events, etc.)	Y	Y
Follow-the-Sun Case Management	N	Y
Number of Total Customer Contacts	5	10
Case Escalation	N	Y

II. Service Level Agreement for Premier Support Level

If Customer is receiving the Premier Support Level, target availability for the Snowflake Service is ninety-nine and nine tenths percent (99.9%) per calendar month (based on minutes of availability/total minutes per month) ("**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 5 below ("**Service Level Credits**"), credited against Customer's usage 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. As used in Table 5 below, "**Average Daily Snowflake Credits**" means Customer's actual Snowflake Credit consumption in the prior calendar month divided by the number of days in such month. Service Level Credits may not be exchanged for, or converted to, monetary amounts.

Table 5: Service Level Credit Calculation	
Availability	**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 – In April, Customer uses a total of three hundred (300) Snowflake Credits. Customer's Average Daily Snowflake Credits for April is ten (10) Snowflake Credits (e.g., 300 / 30 days in April). During that month, the availability of the Snowflake Service is 98%. Customer's Service Level Credit is thirty (30) Snowflake Credits (e.g., 3 x 10 Average Daily Snowflake Credits), which will 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) use of the Snowflake Service by Customer other than as authorized under the Agreement or Documentation; (b) Customer Data; (c) Customer or User equipment; (d) third party acts, or services and/or systems not provided by Snowflake; (e) general Internet problems, or other factors outside of Snowflake's reasonable control; (f) evaluation or proof-of-concept use of the Snowflake Service; or (g) Snowflake's preview features (e.g., beta functionality not intended for production use). Snowflake will have no obligations to provide support for Snowflake's preview features, third party software or services, or custom scripts or code not native to the

Snowflake Service. Additionally, if Customer desires technical or professional services from Snowflake, including but not limited to services related to data modeling, code development, migration, or product training, then Customer and Snowflake must enter into a mutually executed Statement of Work for such services.

Exhibit E

TECHNICAL SERVICES ADDENDUM

1. Technical Services. Under this Technical Services Addendum ("TSA"), certain consulting, training or educational services will be provided to Customer by or on behalf of Snowflake ("**Technical Services**") as further described in a Statement of Work or Order Form (as applicable) referencing this TSA or the Main Terms and executed by both parties describing: (a) the services to be performed, (b) Fees and (c) any applicable milestones, dependencies and other technical specifications or related information related to the Technical Services (each, a "**Statement of Work**" or "**SOW**"). All SOWs shall be deemed part of and subject to this TSA and Main Terms.

2. Changes to Scope. Any requirement(s) or deviations from the scope of work or terms that are not specifically included and described in an SOW will be considered outside the scope and must be procured separately through a formal, written, signed amendment or change order to the SOW ("**Change Order**") that may result in additional cost or modified terms.

3. Customer Obligations.

3.1 Assistance. Customer agrees to provide Snowflake with reasonable access to Customer Materials (defined below), resources, personnel, equipment or facilities to the extent such access is necessary for the provision of Technical Services. Snowflake shall have no liability and shall be excused from the performance of Technical Services with respect to its inability to perform such Technical Services to the extent caused by Customer's failure or delay to provide necessary Customer Materials in a timely manner.

3.2 Customer Materials. Customer hereby grants Snowflake a limited right to use any Customer materials provided to Snowflake in connection with Technical Services (the "**Customer Materials**") solely for the purpose of providing Technical Services to Customer. Customer will retain any of its rights (including all intellectual property rights) in the Customer Materials. Customer represents and warrants to Snowflake that Customer has sufficient rights in the Customer Materials to grant the rights granted to Snowflake in this Section and that the Customer Materials do not infringe or violate the intellectual property, publicity, privacy or other rights of any third party.

4. Deliverables and Snowflake Technology.

4.1 **License to Deliverables.** Unless otherwise set forth in the applicable SOW, subject to this TSA, Snowflake hereby grants Customer a limited, non-exclusive, royalty-free, non-transferable worldwide license to use the Deliverables solely in connection with such Customer's use of the Snowflake Service during the period in which such Customer has valid access to the Snowflake Service. Customer may not reverse engineer, decompile, disassemble, translate, copy, reproduce, display, publish, create derivative works of, assign, sell, lease, rent, license, sublicense or grant a security interest in all or any portion of the Deliverables. "**Deliverables**" means anything provided to Customer under this TSA, including, but not limited to all deliverables, work product, code (including SQL queries) and any derivative, enhancement or modification thereof, but does not include any Customer Materials.

4.2 **License to Tools.** Notwithstanding any other provision of this TSA: (i) nothing herein shall be construed to assign or transfer any intellectual property rights in the proprietary tools, libraries, know-how, techniques and expertise ("Tools") used by Snowflake to develop the Deliverables, and to the extent such Tools are delivered with or as part of the Deliverables, they are licensed, not assigned, to Customer, on the same terms as the Deliverables or as otherwise agreed by Customer; and (ii) the term "Deliverables" shall not include the Tools. Tools are Snowflake Confidential Information.

4.3 Restrictions. Customer shall not (and shall not permit any third party to): (a) use, copy or distribute the Deliverables or Tools except as expressly permitted herein; (b) reverse engineer, decompile or disassemble any Deliverables; or (c) modify or create any derivative work of the Deliverables (unless expressly permitted in the applicable SOW).

4.4 Snowflake Ownership. Except as expressly provided in Section 4.1 (License to Deliverables), Snowflake does not grant any rights or licenses to Customer under its intellectual property rights, whether express or implied. Notwithstanding anything to thecontrary herein, except as expressly provided in Section 4.1(License to Deliverables), Snowflake and its suppliers haveand will retain all right, title and interest (including, without limitation, all patent, copyright, trademark, trade secret and other intellectual property rights) in and to (a) the Snowflake Service, (b) the Deliverables, (c) any Snowflake know-how, tools, methodologies, techniques or expertise used or embodied in any Expert Assistance or Deliverables, (d) any and all related and underlying technology and documentation, and (e) any modifications, improvements and derivative works thereof created by or for Snowflake (including to the extent incorporating Feedback) ("**Snowflake Technology**"). 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 Customer relating to Snowflake's products or services ("**Feedback**").

5 Access to Customer Data. Unless specifically set forth in an SOW, the parties agree that Snowflake will not have access to Customer Data, Customer systems, Customer networks or Customer applications (other than access to Customer's Snowflake account, if such access is contemplated in an SOW) in performance of the Technical Services and Customer will not grant Snowflake such access . If such access is specifically set forth in an SOW, then unless otherwise agreed to in an SOW, Snowflake's access to such Customer Data, systems, networks or applications is subject to the following terms and conditions,: (a) Customer is solely responsible for ensuring that both the duration and

configuration of the scope of access to Customer Data is strictly limited to the access required under the specific SOW; (b) such access may not extend past the Term of the applicable SOW and will be limited to the Snowflake Service; (c) Customer is solely responsible for access control management and must ensure that any access to Customer Data that Customer grants to Snowflake is limited to: (i) read-only access; and (ii) in Customer's Snowflake development environment only; (d) Customer will not grant Snowflake access to any other Snowflake environment (including, but not limited to test, prod or disaster recovery); (e) Snowflake may only access Customer Data through secure Customer workstations and networks that are provided, monitored, managed, configured, supported and maintained by Customer; (f) Customer must provide unique user ID/passwords to any Snowflake resource that requires access to Customer Data as described herein; (g) such credentials noted in (f) above will be solely managed by Customer and Customer will be responsible for any consumption generated from the supplied credentials and (h) Customer will not grant access to any Customer Data that is unencrypted or contains personal data.

6 Payment and Taxes. Customer will pay Snowflake the amounts and at the times set forth in the applicable SOW. Unless otherwise specified in the applicable SOW, Customer agrees to reimburse Snowflake for travel, lodging and meal expenses incurred in the course of providing Technical Services at any location other than Snowflake's site. Snowflake will invoice Customer for expenses incurred. Unless otherwise agreed to by the parties in the applicable SOW, all payments are non-refundable and shall be made in U.S. dollars within thirty (30) days from the date of Snowflake's invoice. Customer is responsible for paying all Taxes associated with its purchases hereunder other than taxes based on income, property, or employees of Snowflake If Snowflake has the legal obligation to pay or collect Taxes for which Customer is responsible under this Section, Snowflake will invoice Customer and Customer will pay that amount unless Customer provides Snowflake with a valid tax exemption certificate authorized by the appropriate taxing authority.. Taxes will not be deducted from payments to Snowflake, except as required by applicable law, in which case Customer will increase the amount payable as necessary so that, after making all required deductions and withholdings, Snowflake receives and retains (free from any liability for Taxes) an amount equal to the amount it would have received had no such deductions or withholdings been made. Upon Snowflake's request, Customer will provide to Snowflake its proof of withholding tax remittance to the respective taxing authority. Any late payments shall be subject to a service charge equal to 1.5% per month of the amount due or the maximum amount allowed by law, whichever is less.

7 Term and Termination. This TSA remains in effect until termination of the Main Terms or as terminated in accordance with this Section. Either party may terminate this TSA for convenience at any time by giving the other party thirty (30) days written notice, but such termination will not affect any SOW in effect at the time of termination (and this TSA will continue to survive and apply with respect to any such SOW until expiration or termination of such SOW hereunder). In addition, either party may terminate this TSA or any SOW if the other party: (a) fails to cure any material breach of this TSA or SOW within thirty (30) days after written notice of such breach; (b) ceases operation without a successor; or (c) seeks protection under any bankruptcy, receivership, trust deed, creditors arrangement, composition or comparable proceeding, or if any such proceeding is instituted against such party (and not dismissed within sixty (60) days thereafter). Sections 3 (Customer Obligations), 4 (Deliverables and Snowflake Technology), will survive any termination or expiration of this TSA. Section 6 (Payment and Taxes) will survive with respect to payments accrued prior to termination.

8 Technical Services Warranty. Snowflake warrants that any Technical Services will be performed in a professional and workmanlike manner in accordance with industry standards and substantially in accordance with the SOW. In the event of a breach of this warranty, Snowflake will use commercially reasonable efforts to re-perform the Technical Services to correct the non-conformity, at no charge to Customer, and if Snowflake is unable to correct the reported non-conformity after two attempts, either party may terminate the applicable SOW and Customer will receive a refund of any unused Fees Customer has pre-paid for the Technical Services purchased thereunder. The foregoing shall be Customer's sole and exclusive remedy for any breach of the warranty set forth in this Section. This warranty will not apply unless Customer makes a claim within thirty (30) days from the date such Technical Services were initially provided.

9 Independent Contractor. Snowflake's relationship with Customer will be that of an independent contractor. Neither party will have any authority to bind the other, to assume or create any obligation, to enter into any agreements, or to make any warranties or representations on behalf of the other. Nothing in this TSA shall be deemed to create any agency, partnership or joint venture relationship between the parties. Each party is solely responsible for all of its employees and agents and its labor cost and expenses and for any and all claims, liabilities or damages or debts of any type whatsoever that may arise on account of each party's activities or those of its employees or agents in the performance of this TSA. Snowflake reserves the right to use third-parties (who are under a covenant of confidentiality with Snowflake) to provide any Technical Services described hereunder.

Key Personnel. In accordance with Section 12. Changes in Subcontractor Representation in the Carahsoft NASPO Agreement, any applicable key administrative personnel shall be identified solely in the SOW upon mutual agreement of the Parties.