Carahsoft Rider to Manufacturer Commercial Supplier Agreements
(for U.S. Government End Users)
Revised 20161213

1. **Scope.** This Carahsoft Rider and the Manufacturer's Commercial Supplier Agreement (CSA) establish the terms and conditions enabling Carahsoft to provide Software and Services to U.S. Government agencies (the "Client" or "Licensee").

2. **Applicability.** The terms and conditions in the attached Manufacturer's CSA are hereby incorporated by reference to the extent that they are consistent with Federal Law (e.g., the Anti-Deficiency Act (31 U.S.C. § 1341(a) (1) (B)), the Contracts Disputes Act of 1978 (41. U.S.C. § 601-613), the Prompt Payment Act, the Anti-Assignment statutes (31 U.S.C. **§** 3727 and 41 § U.S.C. 15), 28 U.S.C. § 516 (Conduct of Litigation Reserved to Department of Justice (DOJ), and 28 U.S.C. § 1498 (Patent and copyright cases)). To the extent the terms and conditions in the Manufacturer's CSA is inconsistent with the Federal Law (*See* FAR 12.212(a)), they shall be deemed deleted and unenforceable under any resultant orders under Carahsoft's Multiple Award Schedule Contract, GS-35F-0119Y, including, but not limited to the following:

(a) **Contracting Parties.** The Government customer (Licensee) is the "Ordering Activity", defined as an entity authorized to order under Government contracts as set forth in General Services Administration Order OGP 4800.2I, as may be revised from time to time. The Licensee cannot be an individual because any implication of individual licensing triggers the requirements for legal review by Federal Employee unions. Conversely, because of competition rules, the contractor must be defined as a single entity even if the contractor is part of a corporate group. The Government cannot contract with the group, or in the alternative with a set of contracting parties.

(b) **Changes to Work and Delays.** Subject to General Services Administration Acquisition Regulation (GSAR) 552.238-81 Modifications (Federal Supply Schedule) (APR 2014) (Alternate I – APR 2014) and GSAR 552.212 -4 (f) Contract Terms and Conditions – Commercial Items, Excusable Delays (MAY 2015) (Alternate II – JUL 2009) (FAR Deviation – JUL 2015) (Tailored) regarding which of the GSAR and the FAR provisions shall take precedence.

(c) **Contract Formation.** Subject to FAR Sections 1.601(a) and 43.102, the Government Order must be signed by a duly warranted contracting officer, in writing. The same requirement applies to contract modifications affecting the rights of the parties. All terms and conditions intended to bind the Government must be included within the contract signed by the Government.

(d) Audit. During the term of this CSA: (a) If Ordering Activity's security requirements included in the Order are met, Manufacturer or its designated agent may audit Ordering Activity's facilities and records to verify Ordering Activity's compliance with this CSA. Any such audit will take place only during Ordering Activity's normal business hours contingent upon prior written notice and adherence to any security measures the Ordering Activity deems appropriate, including any requirements for personnel to be cleared prior to accessing sensitive facilities. Carahsoft on behalf of the Manufacturer will give Ordering Activity written notice of any non-compliance, including the number of underreported Units of Software or Services ("Notice"); or (b) If Ordering Activity's security requirements are not met and upon Manufacturer's request, Ordering Activity will run a self-assessment with tools provided by and at the direction of Manufacturer ("Self-Assessment") to verify Ordering Activity's compliance with this CSA.

(e) Termination. Clauses in the Manufacturer's CSA referencing suspension, termination or cancellation of the Manufacturer's CSA, the License, or the Customer's Account are hereby deemed to be deleted. Termination, suspension or cancellation shall be governed by the GSAR 552.212-4 and the Contract Disputes Act, 41 U.S.C. §§ 601-613, subject to the following exceptions:

> Carahsoft may request cancellation or termination of the CSA on behalf of the Manufacturer if such remedy is granted to it after conclusion of the Contracts Disputes Act dispute resolutions process referenced in Section (q) below or if such remedy is otherwise ordered by a United States Federal Court.

(f) Consent to Government Law / Consent to Jurisdiction. Subject to the Contracts Disputes Act of 1978 (41. U.S.C §§ 7101-7109) and Federal Tort Claims Act (28 U.S.C. §1346(b)). The validity, interpretation and enforcement of this Rider and the CSA will be governed by and construed in accordance with the laws of the United States. All clauses in the Manufacturer's CSA referencing equitable remedies are deemed not applicable to the Government order and are therefore deemed to be deleted.

(g) Force Majeure. Subject to GSAR 552.212 -4 (f) Contract Terms and Conditions – Commercial Items, Excusable Delays (MAY 2015) (Alternate II – JUL 2009) (FAR Deviation – JUL 2015) (Tailored). Unilateral Termination by the Contractor does not apply to a Government order and all clauses in the Manufacturer's CSA referencing unilateral termination rights of the Manufacturer's CSA are hereby deemed to be deleted.

(h) Assignment. All clauses regarding Assignment are subject to FAR Clause 52.232-23, Assignment of Claims (MAY 2014) and FAR 42.12 Novation and Change-of-Name Agreements, and all clauses governing Assignment in the Manufacturer's CSA are hereby deemed to be deleted.

(i) Waiver of Jury Trial. All clauses referencing waiver of Jury Trial are subject to FAR Clause 52.233-1, Disputes (MAY 2014), and all clauses governing waiver of jury trial in the Manufacturer's CSA are hereby deemed to be deleted.

(j) Customer Indemnities. All of the Manufacturer's CSA clauses referencin**g** Customer Indemnities are hereby deemed to be deleted.

(k) Contractor Indemnities. All of the Manufacturer's CSA clauses that (1) violate DOJ's right (28 U.S.C. 516) to represent the Government in any case and/or (2) require that the Government give sole control over the litigation and/or settlement, are hereby deemed to be deleted.

(l) Renewals. All of the Manufacturer's CSA clauses that violate the Anti-Deficiency Act (31 U.S.C. 1341, 41 U.S.C. 11) ban on automatic renewal are hereby deemed to be deleted.

(m) Future Fees or Penalties. All of the Manufacturer's CSA clauses that violate the Anti-Deficiency Act (31 U.S.C. 1341, 41 U.S.C. 11), which prohibits the Government from paying any fees or penalties beyond the Contract amount, unless specifically authorized by existing statutes, such as the Prompt Payment Act, or Equal Access To Justice Act 31 U.S.C. 3901, 5 U.S.C. 504 are hereby deemed to be deleted.

(n) Taxes. Taxes are subject to GSAR 552.212-4(k) Contract Terms and Conditions – Commercial Items, Taxes (MAY 2015) (Alternate II – JUL 2009) (FAR Deviation – JUL 2015) (Tailored) and GSAR 552.212-4 (w) (1) (x) Contract Terms and Conditions – Commercial Items, Taxes (MAY 2015) (Alternate II – JUL 2009) (FAR Deviation – JUL 2015) (Tailored).

(o) Third Party Terms. Subject to the actual language agreed to in the Order by the Contracting Officer. Any third party manufacturer will be brought into the negotiation, or the components acquired separately under Federally-compatible agreements, if any. Contractor indemnities do not constitute effective migration.

(p) Installation and Use of the Software. Installation and use of the software shall be in accordance with the Rider and Manufacturer's CSA, unless an Ordering Activity determines that it requires different terms of use and Manufacturer agrees in writing to such terms in a valid task order placed pursuant to the Government contract.

(q) Dispute Resolution and Venue. Any disputes relating to the Manufacturer's CSA and to this Rider shall be resolved in accordance with the FAR, the GSAR and the Contract Disputes Act, 41 U.S.C. §§ 7101-7109. See GSAR 552.212-4 (w) (1) (iii) Contract Terms and Conditions – Commercial Items, Law and Disputes (MAY 2015) (Alternate II – JUL 2009) (FAR Deviation – JUL 2015) (Tailored). The Ordering Activity expressly acknowledges that Carahsoft, as the vendor selling the Manufacturer's licensed software, shall have standing under the Contract Disputes Act to bring such claims that arise out of licensing terms incorporated into Multiple Award Schedule Contract GS-35F-0119Y.

(r) Limitation of Liability: Subject to the following:

Carahsoft, Manufacturer and Ordering Activity shall not be liable for any indirect, incidental, special, or consequential damages, or any loss of profits, revenue, data, or data use. Further, Carahsoft, Manufacturer and Ordering Activity shall not be liable for punitive damages except to the extent this limitation is prohibited by applicable law. This clause shall not impair the U.S. Government's right to recover for fraud or crimes arising out of or related to this Government Contract under any federal fraud statute, including the False Claims Act, 31 U.S.C. §§ 3729-3733.

(s) Advertisements and Endorsements. Unless specifically authorized by an Ordering Activity in writing, such use of the name or logo of any U.S. Government entity is prohibited.

(t) Public Access to Information. Manufacturer agrees that the CSA and this Rider contain no confidential or proprietary information and acknowledges the CSA and this Rider will be available to the public.

(u) Confidentiality. Any provisions that require the Licensee to keep certain information confidential are subject to the Freedom of Information Act, 5 U.S.C. §552, and any order by a United States Federal Court. The Licensee may provide information to other components of the United States Government pursuant to proper requests for such information as permitted by law, regulation or policy (e.g., disclosures to Congress, auditors, Inspectors General, etc.).

This Master Services Agreement ("**MSA**") is effective as of the date set forth in the Order Form ("**Effective Date**") and is between **Datapipe Government Solutions, Inc.** ("**Datapipe**"), a Delaware corporation with an address of 1902 Campus Commons Drive, Suite 510, Reston, VA 20191 and Government Ordering Activity ("**Client**"). Datapipe and Client are referred to in this MSA individually as a "**Party**" and collectively as the "**Parties**."

BACKGROUND

Client desires to obtain from Datapipe, and Datapipe desires to provide to Client, certain IT infrastructure and/or managed services as more particularly described in this MSA and identified on one or more Service Schedules and Order Forms. Each Party acknowledges the receipt and sufficiency of adequate consideration as further detailed in this MSA.

GENERAL TERMS AND CONDITIONS

1. DEFINITIONS.

"Affiliate" means any Person that a Party controls, that controls a Party, or that is under common control with a Party. For purposes of this definition, "control" shall mean beneficial ownership, whether directly or indirectly, of the securities entitled to vote in the election of directors (or, in the case of an entity that is not a corporation, of the election of the corresponding management authority) in the entity of (i) more than 50% of the securities or (ii) such lesser percentage of securities as is the maximum ownership permitted in the country where the entity exists.

"Audit" means a security audit performed by Client or its agent pursuant to Section 8.3 of this MSA.

"**AUP**" means the attached Datapipe Acceptable Use Policy located at http://www.datapipe.com/about-us-legal-acceptable-use-policy.htm, as may be amended from time to time. For certain Services, the AUP may also include the acceptable use policy of a Third Party service provider, such as Amazon, Inc.

"**Business Day**" means each day, Monday through Friday, 8:00 a.m. to 5:00 p.m., excluding any day government agencies in the country in which the Services are provided are required or permitted to be closed. The specific time zone shall be determined based on the location of the Facility providing the relevant Service.

"**Client Content**" means all data and information, including, without limitation, data text, software, scripts, video, sound, music, graphics and images that are created, uploaded, stored or transferred by or for Client or its Affiliate in connection with the use of any of the Services.

"**Client-Licensed Software**" means software products for which Client has obtained license entitlements from the publishers of those products or from Third Party vendors.

"**Client Portal**" means Datapipe's in-house ticketing system found at https://one.datapipe.com or such other URL as may be designated by Datapipe from time to time.

"**Client Software**" means the object code versions of any software, if any, provided to Datapipe by Client or otherwise utilized by Client in connection with the Services.

"**Datapipe Software**" means the object code versions of any software (and any updates thereto), published by Datapipe and utilized by Client in connection with the Services and as may be more particularly described in the Order Form(s). For clarity, the definition of Datapipe Software shall not include Third Party Software.

"**Datapipe Support**" means the Datapipe Help Desk, which is the primary point of contact for all queries and communications regarding Service incidents. Datapipe Support is reachable by telephone (888-749-5821), e-mail (support@datapipe.com), or via the Client Portal and is available 24 hours a day, 7 days a week, 365 days a year (366 days in a leap year).

"**Delivery Date**" means as to each Order Form, the documented date that all Services referenced in such Order Form are deployed by Datapipe and are made available to Client.

"**DMCA**" means the Digital Millennium Copyright Act, 17 USLA §512C, a United States copyright law or any similar laws of the country in which the Services are being provided.

"**End User**" means any individual or entity that Client has authorized or allowed to directly or indirectly: (a) access or use Client Content; or (b) otherwise interface, access or use the Services.

"**Facility**" means a Datapipe facility used by Datapipe to provide the Services as indicated in the corresponding Order Form(s) including, but not limited to, the Datapipe facility within a Datapipe Cloud Zone (as defined in the Stratosphere Elastic Cloud Services Schedule), in which the Services are provided.

"**FAR**" means the Federal Acquisition Regulation.

"**ITAR Data**" means International Traffic in Arms Regulations.

"**Minor Service Modification**" means any consumption-based modifications to the Services or Service Components of $1,000.00 or less which are submitted by Client via e-mail or the Client Portal and subsequently approved by Datapipe. Notwithstanding the foregoing, storage component modifications submitted by Client via e-mail or the Client Portal and subsequently approved by Datapipe may exceed $1,000.00.

"**Monthly Recurring Fee**" means the amount to be paid monthly by Client for the applicable Service(s) as specified in the Order Form(s), e-mail(s), ticket(s) or other methods approved by the Parties.

"**Monthly Remittance Date**" means the day of each month the Monthly Recurring Fee shall be due and payable by Client and shall be based on the Order Form Commencement Date, except as provided in this definition. All Services shall be invoiced to reflect a uniform Monthly Remittance Date. If the Monthly Remittance Date is a day which does not exist in a particular calendar month, then the Monthly Remittance Date shall be the last date of such month (e.g. if the Monthly Remittance Date is the 30th of every month, then in February, the Monthly Remittance Date shall be either February 28th or 29th, depending on the year).

"**Order Form**" means any order form executed by both Client and Datapipe, which incorporates the terms of this MSA by reference. Each Order Form will be considered a separate agreement from any other Order Form. Each Order Form shall be governed by this MSA and applicable Service Schedule(s) and shall become effective on the Order Form Commencement Date.

"**Order Form Commencement Date**" means the commencement date set forth and identified as such on any Order Form.

"**Order Form Expiration Date**" means the expiration date set forth and identified as such on any Order Form.

"**PII**" means any data contained within the Client Content that could potentially identify a specific individual.

"**Person**" means any natural person, corporation, limited liability company, trust, joint venture, association, company, partnership, governmental authority or other entity.

"Privacy Policy" means the attached Datapipe privacy policy located at http://www.datapipe.com/legal/privacy_policy_safe_harbor or such other URL as designated by Datapipe from time to time, as may be amended from time to time. For certain Services, the Privacy Policy may also include the privacy policy of a Third Party service provider such as Amazon, Inc.

"**Reasonable efforts**" means, with respect to a given obligation, the efforts that a comparably-situated service provider to that of Datapipe would use to comply with that obligation as promptly as reasonably possible.

"**Renewal Term**" means the automatic renewal of the initial Service Term specified in each Order Form.

"**Services**" means all of the services (a) ordered by Client or its Affiliate as set forth on the corresponding Order Form(s) governed by this MSA and the corresponding Service Schedule(s); and/or

(b) accessed, and/or utilized by Client via the APIs or the Client Portal or Cloud Portal (as defined in the Stratosphere Elastic Cloud Services Schedule). The Services may be modified as provided in the Order Form(s) and Service Schedule(s).

"**Service Component(s)**" means each particular element or portion of the Services.

"**Service Schedule(s)"** means the schedules for Services attached to this MSA that correspond to the Services being provided to Client.

"Service Term" means as to each Service ordered by Client, the period commencing on the Order Form Commencement Date with respect to each particular Order Form and ending on the Order Form Expiration Date designated in that Order Form.

"**SLA**" means the Service Level Agreement for each Service type as set forth in the applicable Service Schedule.

"**Subsidiary**" means an Affiliate controlled by a Party.

"Suggestions" means any communications, comments, questions, suggestions, or related materials provided to Datapipe by Client or any End User, whether by letter, e-mail, telephone, or otherwise, suggesting or recommending changes to the Services, including, without limitation, new features or functionality.

"Term" means the Service Term and any corresponding Renewal Term.

"**Third Party**" means a Person that is not a Party or an Affiliate of a Party.

"**Third Party Fee Increase**" means any documented increase in Datapipe's direct costs associated with Third Party Software.

"**Third Party Hardware**" means the equipment manufactured by a Third Party, if any, that Datapipe provides for Client's use or availability to use under the terms of this MSA.

"**Third Party Software**" means those various additional Third Party software applications or services which may be licensed from time to time by Datapipe for Client's use in conjunction with the Services.

"**TPS Agreements**" means those agreements for products and services provided by Third Parties which are entered into directly between Client and such Third Party. TPS Agreements are separate and independent from this MSA, and Datapipe is not a party to and is not responsible for the performance of any TPS Agreements.

2. DELIVERY OF SERVICES.

2.1. <u>General</u>. Datapipe and/or its Affiliates will provide the Service(s) and/or Service Component(s) in accordance with this MSA. The description, charges, and other terms applicable to the individual Services are set forth in the applicable Service Schedule(s) and Order Form(s). Client may order additional Services by updating or amending this MSA through the execution of additional Order Form(s) or a Minor Service Modification. The Service(s) shall be subject to the SLA set forth in the applicable Service Schedule(s).

2.2. <u>Client Affiliates</u>. The benefits, obligations and privileges of the MSA shall extend to all entities that constitute "Client", including all Affiliates, even though each such entity is not specifically named as a party to the MSA. As such, Client and its successors and assigns will be and remain liable for all of the obligations of all entities that constitute "Client" under the MSA, including all Affiliates, and Datapipe will look to Client and its successors and assigns for enforcement of Datapipe's rights under the MSA.

3. TERM AND TERMINATION; SUSPENSION.

3.1. <u>Term</u>. The term of this MSA will commence on the Effective Date and shall remain in effect until the expiration of the latest Term unless earlier terminated in accordance with the provisions of this MSA or otherwise agreed to in writing between the Parties. Each Order Form shall commence on its respective Order Form Commencement Date and continue in effect until its respective Order Form Expiration Date, subject to any applicable Renewal Term.

3.2. Renewal Term. Upon the expiration of each Term, each expiring Order Form shall be subject to automatic renewal for the same period as the initial Service Term or any agreed upon Renewal Term, as the case may be, unless: (i) Client notifies Datapipe in writing of its intent to terminate a certain Order Form/Service Schedule or this MSA in its entirety no less than 30 days prior to the end of the then current Term of the applicable Order Form, or (ii) Datapipe notifies Client in writing of its intent to terminate a certain Order Form/Service Schedule or this MSA in its entirety no less than 30 days prior to the end of the then current Term of the applicable Order Form. Client shall remit payment to Datapipe for all Services through and including the date of termination of the Term. In the event Client's Customer or end-user is the United States Federal Government, Renewal Term may be subject to the period of performance (base period and any exercised option periods) set by the Client's Federal Government Customer or end-user.

3.3. Termination for Cause. Either Party may terminate this MSA or any Order Form (and associated Service Schedule(s)), in whole or in part, in the event that the other Party (i) breaches any material term or condition of this MSA and fails to cure such breach within 30 days of receiving written notice thereof or (ii) becomes insolvent, makes an assignment for the benefit of creditors, files a petition for bankruptcy, is the subject of a petition for bankruptcy which is not dismissed within ninety (90) days from the filing thereof, becomes the subject of any receivership or admits in writing its inability to pay its debt generally as they become due. In the event this MSA is terminated by Datapipe for cause, Client shall pay Datapipe for all Services through the remaining balance of the then-current Term of each Order Form. Datapipe may terminate this MSA or any Order Form (and associated Service Schedule) if any suspension event described in Section 3.7 is not cured by the Client within the applicable cure period or if such suspension event cannot be cured.

3.4. End of Services. Upon the termination of this MSA or any Order Form or Service Schedule for any reason: (i) all rights and licenses granted by either Party under the applicable Order Form and/or Service Schedule(s) shall cease immediately; (ii) each Party shall return to the other Party, or destroy all Confidential Information (as defined herein) of the other Party within 30 days following such termination, except as may be required to comply with any applicable legal or accounting record-keeping requirements; (iii) any and all payment obligations of Client under this MSA will immediately become due, including but not limited to Services set forth in an Order Form and due through the Order Form Expiration Date; (iv) Datapipe shall remove all Client Content from any Third Party Hardware; and (v) Client shall erase and remove all copies of all Datapipe Software and Third Party Software from any computer equipment and media in Client's possession, custody or control. In no event will Client Content be retained by Datapipe more than fourteen (14) days following termination of this MSA or any Order Form.

3.5. Survival. All terms and provisions which should by their nature, survive the termination or expiration of this MSA including, but not limited to Sections 1, 4, 5, 7, 8, 11 and 12, shall so survive. Notwithstanding the foregoing, in the event Client continues to use any Services following termination of this MSA or any Order Form, Client shall be responsible for payment of such Services at Datapipe's then-current market rates.

3.6. IP Addresses. Upon expiration or termination of this MSA or any Service Schedule, Client must discontinue use of the terminated or expired Services and relinquish use of the IP addresses and server names assigned to Client by Datapipe in connection with the terminated or expired Services, including pointing the DNS for Client's domain name(s) away from any Services provided by Datapipe. Datapipe may, as it deems necessary, make modifications to DNS records on Datapipe managed or operated DNS servers and services to ensure compliance with this Section.

3.7. Suspension.

3.7.1. Subject to Section 3.7.2, Datapipe may suspend your right to access or use any portion or all of the Services without liability if: (i) Datapipe reasonably believes the Services have been accessed or manipulated by a Third Party without Client's consent; (ii) Datapipe reasonably believes that suspension of Services is necessary to protect Datapipe's network or other Datapipe customers and the continued use of the Services by Client may adversely and materially impact the services or the systems or content of any other Datapipe customer; (iii) suspension is required by law, statute, regulation, rule or court order; or (iv) in response to a take-down notice served upon Datapipe pursuant to the DMCA, unless Client serves Datapipe with a compliant counter-notice pursuant to the provisions of the DMCA within 48 hours of Datapipe providing Client with such take-down request; (v) Services are being used (or have been or will be used) by Client in violation of the AUP or MSA; or (vi) a payment for Services is overdue by more than 30 days as set forth in Section 4.2 and not being properly disputed pursuant to Section 4.5.

3.7.2. For Sections 3.7.1 (i), (ii), (iii), and (iv), Datapipe will give Client reasonable advance written notice of a suspension and a reasonable chance to cure the grounds on which the suspension is based and will cooperate with Client to the extent reasonably required by Client to resolve the issue, unless Datapipe determines, in Datapipe's reasonable judgment, that a suspension on shorter or contemporaneous notice is necessary to protect Datapipe or its other customers from operational, security, or other risk or the suspension is ordered by a court or other judicial or governmental body or required by law, statute, regulation, rule, legal proceeding or other governmental request, in which case Datapipe may suspend the Services immediately. For Sections 3.7.1 (v) or (vi), Datapipe will give Client at least thirty (30) days advance written notice prior to suspending the Services and will only suspend such Services if Client does not cure the grounds on which the suspension is based prior to the end of such notice period. For Section 3.7.1(vi), any suspension of Services shall continue until such time as all outstanding sums are remitted.

3.7.3. If Datapipe suspends Client's right to access or use any portion or all of the Service:

(a) Client remains responsible for all fees and charges during any period of suspension except with respect to a suspension which directly results from the negligent acts or omissions of Datapipe, in which case Client will receive a commensurate refund for applicable prepaid fees ;

(b) Client remains responsible for any applicable fees and charges for any Services which Client continues to have access to, as well as applicable data storage fees and charges, and fees and charges for in-process tasks completed after the date of suspension;

(c) Client will not be entitled to any SLA credits under the SLAs during any period of suspension; and

(d) Datapipe may limit Client's access to the portion of Client Content that is stored on any Service Components related to suspension, and Datapipe shall not be liable to Client for any damages or losses Client may incur as a result.

4. PAYMENT AND PAYMENT TERMS.

4.1. Fees. The Monthly Recurring Fee together with any fees specified on the Order Form, as the case may be, shall be billed to Client via invoice in advance for Services to be provided for the following calendar month, unless otherwise specified in the Order Form or Service Schedule(s). Non-recurring fees including, but not limited to, set-up fees shall be billed as incurred in any given month and fees for consumption-based Services such as conditioned power use overages or bandwidth use overages shall be invoiced in arrears ("**Additional Fees**"). All payments shall be made in the currency specified in each

Order Form and shall be sent to the mailing address designated by Datapipe's Billing Department. Client shall remit payment on or before the due date set forth on all future invoices which due date shall be designated as the monthly anniversary of the initial invoice due date. All amounts payable under this MSA will be made without setoff or counterclaim, and without any deduction or withholding.

4.2. Late Payments. Late payments shall accrue interest at the greater of a rate of .05% per month or the maximum amount permitted by law.

4.3. Taxes. Fees for Services are exclusive of all taxes, duties, levies and similar fees now in force or enacted in the future or imposed on the provision of the Services by any governmental authority, including, but not limited to any excise or value-added tax, all of which Client will be responsible for and will pay in full, exclusive of taxes on Datapipe's income. If Client claims exemption from any taxes arising from the provision of the Services, Client shall provide Datapipe with documentation required by the taxing authority to support such exemption.

4.4. Fee Disputes. Client may dispute in good faith any portion of an invoice provided Client: (i) pays the full undisputed portion of invoice by its due date, (ii) provides Datapipe with a written statement and supporting documentation regarding the dispute within 30 days from the date of the relevant invoice, and (iii) negotiates in good faith with Datapipe to resolve the dispute. Any invoice or portion of an invoice not disputed in accordance with this Section shall be deemed undisputed. If the dispute is not resolved within 45 days from Datapipe's receipt of Client's written statement, either Party may pursue its rights or remedies available either at law or pursuant to this MSA. No interest shall accrue on any payment that is disputed in good faith by Client while such dispute is pending. Notwithstanding the foregoing, if such dispute is later resolved in favor of Datapipe, such amount shall be subject to the monthly finance charge rate indicated in Section 4.2 from the original due date until payment in full has been received by Datapipe.

4.5. Pricing Changes. Datapipe shall not raise the Monthly Recurring Fee or Minimum Monthly Recurring Fee for Services provided under any Order Form before the initial Order Form Expiration Date except in the case of a material change in the Services agreed to in writing by both Parties or a change in pricing due to a Third Party Fee Increase incurred by Datapipe in connection with the provision of the Services. At least sixty (60) days prior to the conclusion of the Service Term or Renewal Term of any applicable Order Form, Datapipe shall inform Client of any proposed increase in fees for Services to go into effect as of the renewal date for the applicable Order Form ("**Increase Notice**"). Notwithstanding the foregoing, Client shall have 60 days' after receipt of the Increase Notice in which to terminate this MSA or corresponding Order Form(s)/Service Schedule(s) by providing Datapipe with written notice of termination ("**Increase Termination Notice**"). Should Client fail to provide the Increase Termination Notice within this 60-day period, Client shall have waived its right to terminate and the Monthly Recurring Fee increase shall be in effect for the remainder of the Renewal Term. Any such increases accepted by Client shall be effective as of the next applicable Monthly Remittance Date after the expiration of the 60-day notice period. In the case of a material change in the Services, the Parties will execute an Order Form or other form of written amendment. Notwithstanding the foregoing, all pricing changes shall be in accordance with the terms and conditions of Carahsoft Technology Corporation's (Carahsoft's) Multiple Award Schedule (MAS) Contract.

5. CONFIDENTIAL INFORMATION.

5.1. Confidential Information. "**Confidential Information**" shall include all information, whether in tangible or intangible form, that is marked or designated as confidential or that, under the circumstances of its disclosure, should be considered confidential. Such information shall include, but is not limited to, any nonpublic information (written, oral or electronic) disclosed by one Party to the other Party as well as the following information of the respective Parties, without limitation: (a) customer lists and the names of customer contacts, e-mail addresses, business plans, technical data, product ideas, personnel, contracts and financial information; (b) trade secrets, techniques, processes, know-how, business methodologies, schematics, employee suggestions, development tools and processes, computer printouts, computer programs, design drawings and manuals, and improvements; (c) plans for future products and developments; (d) information about costs, profits, markets and sales; (e) all documents, books, papers, drawings, models sketches, and other data of any kind and description, including electronic data recorded or retrieved by any means, that have been or will be disclosed, as well as written or oral instructions or comments; (f) any data or information stored on the Third Party Hardware; and (g) the contents of this MSA. Information shall not be deemed Confidential Information if such information: (i) can be shown was known by the receiving Party prior to receipt from the disclosing Party directly or indirectly from a source other than one having an obligation of confidentiality to the disclosing Party; (ii) can be shown was known independently of disclosure by the disclosing Party to the receiving Party directly or indirectly from a source other than one having an obligation of confidentiality to the disclosing Party; or (iii) becomes publicly known or otherwise ceases to be secret or confidential, except as a result of a breach of this MSA, any Service Schedule or any obligation of confidentiality by the receiving Party. The receiving Party may disclose Confidential Information pursuant to the requirements of a governmental agency or by operation of law, provided that, unless restricted by order of a governmental agency or otherwise restricted by law, the receiving Party provides reasonable notice to the other Party of the required disclosure so as to permit the other Party a reasonable period of time to respond to such request for disclosure.

5.2. Nondisclosure of Confidential Information. Each Party agrees not to use, disclose, sell, license, publish, reproduce or otherwise make available the Confidential Information of the other Party to any third party, and further agrees not to use the Confidential Information of the other Party except and only to the extent permitted under or necessary to perform their respective obligations under this MSA. Each Party agrees to secure and protect the other Party's Confidential Information with the same degree of care and in a manner consistent with the maintenance of such Party's own confidential and proprietary rights in the information (but in no event less than reasonable care) and to take appropriate action by instruction or agreement with its employees, consultants, affiliates or other agents who are permitted access to the other Party's Confidential Information to satisfy its obligations under this Section. The foregoing obligations of confidentiality shall survive the termination or expiration of this MSA.

5.3. Maintenance of Confidentiality. Client acknowledges that Datapipe may require that employees and other visitors of Client seeking access to a Facility execute a non-disclosure agreement which is consistent with Client's confidentiality obligations under this Section. Each Party agrees to immediately notify the other Party in the event of any unauthorized use or disclosure of the other's Confidential Information.

5.4. Injunctive Relief. Each Party acknowledges that unauthorized disclosure or use of Confidential Information of the other Party could cause irreparable harm and significant injury to such Party for which monetary damages alone would not be adequate. Accordingly, each Party may seek immediate temporary and permanent injunctive relief to remedy any breaches of the confidentiality provisions contained herein.

5.5. Disposition of Confidential Information. All Confidential Information and all copies thereof shall be and remain the property of the disclosing Party. Upon the written request from the disclosing Party, the receiving Party shall destroy and certify the destruction of, all Confidential Information of the disclosing Party with the exception of any copies which must be maintained pursuant to applicable law.

5.6. Prior NDA. In the event there is an effective pre-existing confidentiality, non-disclosure or similar agreement between Datapipe and Client ("**Prior NDA**") that contains terms more restrictive than the terms set forth in this Section 5, (i) the terms and conditions of such Prior NDA shall control; and (ii) the termination date of the Prior NDA shall be extended through the Term of this MSA (and any confidentiality obligations that survive the expiration of the Prior NDA shall so survive in accordance with its terms).

6. SOFTWARE OWNERSHIP AND USE.

6.1. Software Provided by Datapipe. Datapipe grants Client during the Term a nonexclusive, nontransferable (except as otherwise provided in this MSA), royalty-free worldwide license, to use the Datapipe Software and Third Party Software. Client shall have the right to grant sublicenses solely to its authorized End Users of (i) the Datapipe Software and (ii) the Third Party Software to the extent such license grant is permitted by the agreement between Datapipe and the provider of such Third Party Software. Datapipe shall use reasonable commercial efforts to install and maintain the Datapipe Software and Third Party Software on the Third Party Hardware such that the Datapipe Software and Third Party Software operate in accordance with applicable specifications. Client shall not, and shall not permit others to: (a) modify, copy, or otherwise reproduce the Datapipe Software or Third Party Software in whole or in part; (b) reverse engineer, decompile, disassemble, or otherwise attempt to derive the source code for or structure of the Datapipe Software or Third Party Software; (c) distribute, sublicense, assign, share, timeshare, sell, rent, lease, grant a security interest in, or otherwise transfer the Datapipe Software or Third Party Software or Client's right to use the Datapipe Software or Third Party Software (except as otherwise provided in this MSA); or (d) remove, modify or obscure any copyright, trademark or other proprietary notices or labels on the Datapipe Software or Third Party Software. All rights not expressly granted to Client are reserved by Datapipe or Datapipe's licensors and suppliers. The Third Party Software is provided to Client by Datapipe "AS IS." Datapipe will, to the extent permitted by its vendors to pass through any warranties and indemnifications provided by the manufacturer of the Third Party Software.

6.2. Software Provided by Client. For the sole purpose of providing the Services to Client during the Term, Client grants Datapipe a nonexclusive, nontransferable, royalty-free worldwide license, without the right to grant sublicenses, to use the Client Software. Datapipe shall not, and shall not permit others to: (a) modify, copy, or otherwise reproduce the Client Software in whole or in part; (b) reverse engineer, decompile, disassemble, or otherwise attempt to derive the source code for or structure of the Client Software; (c) distribute, sublicense, assign, share, sell, lease, grant a security interest in, or otherwise transfer the Client Software or Datapipe's right to use the Client Software; or (d) remove any proprietary notices or labels on the Client Software. All rights not expressly granted to Datapipe are reserved by Client or Client's licensors and suppliers.

6.3. THIRD PARTY SOFTWARE, MICROSOFT SOFTWARE. Third Party Software may consist of certain software licensed to Datapipe from Microsoft Corporation. Client agrees that its use of Microsoft products on the Third Party Hardware is governed by both the terms of this MSA and Microsoft's Customer License Terms, a copy of which is attached and located at https://datapipe.box.com/customer-license-terms (password: datapipe) or such other URL as designated by Datapipe from time to time, as may be amended from time to time. For avoidance of doubt, the Customer License Terms are a TPS Agreement, as defined in this MSA. Client acknowledges that the terms of Datapipe's license agreement with Microsoft may require Datapipe to provide Microsoft with Client's name and address, and Client consents to such disclosure.

If Client deploys any Microsoft software products in connection with License Mobility Through Software Assurance benefits, Client further understands, agrees and consents that:

(a) Datapipe may share with Microsoft anonymized information related to Client's License Mobility verification status in the event of any software audit,

(b) Datapipe may cooperate with Microsoft to investigate and remedy any potential non-compliance related to Client's use of License Mobility benefits, and

(c) Datapipe may terminate any and all Services related to License Mobility benefits if Microsoft determines Client is out of compliance with the requirements for those benefits.

6.4. THIRD PARTY SOFTWARE, GENERALLY. Client may deploy certain Client-Licensed Software in connection with the Services. The following terms apply to all Client-Licensed Software:

(a) Client represents that it owns or has the right to use all Client-Licensed Software provided in connection with the Services and will promptly provide Datapipe with evidence of same via e-mail to Licensing@datapipe.com upon request. Client shall further provide Datapipe with evidence of any updated and/or additional licenses throughout the Term.

(b) Pursuant to agreements with its vendors, Datapipe may be required to deploy Client-Licensed Software on physical servers that are dedicated to Client and not accessible to other Datapipe customers. To the extent Client fails to provide to Datapipe within a reasonable time with evidence that it owns or has the right to use Client-Licensed Software in accordance with Section 6.4(a), Datapipe may be required to procure its own licenses for the deployment of Client-Licensed Software and Client may incur additional charges as a result.

(c) Client must either supply as Client-Licensed Software, or request that Datapipe supply, all licenses associated with each particular software product line in connection with the Services. For example, if Microsoft Office is to be deployed as part of Client's solution, all installations of that product family must either be provided by Datapipe or provided by Client in the form of Client-Licensed Software.

7. CLIENT OBLIGATIONS AND REPRESENTATIONS.

7.1. General. Client represents that:

7.1.1. Client has the legal right and authority to enter into this MSA including any Order Form(s) or other related documents, and will continue to have such legal right and authority during the Term.

7.1.2. Client and any End Users will use the Services only for lawful purposes and in accordance with this MSA. Client will comply with all applicable laws and regulations in connection with its use of the Services.

7.2. Data Retention. Client is responsible for properly configuring and using the Services and taking those steps Client deems necessary to maintain appropriate security, protection and backup of Client Content, which may include the use of encryption technology to protect Client Content from unauthorized access, and routine archiving of Client Content. Client acknowledges that unless otherwise specified in an Order Form, Datapipe shall not create or maintain an archive or backup of Client Content. Client log-in credentials and private keys generated by the Services are for Client's internal use only and Client may not sell, transfer or sublicense them to any other entity or person, except that Client may disclose Client's private key to Client's agents and subcontractors performing work on Client's behalf. Client agrees to immediately notify Datapipe of any unauthorized use of Client's Services or any other breach of security. Client agrees to cooperate with Datapipe's reasonable investigation of Service outages, security problems, and any suspected breach of this MSA. Nothing in this Section 7.2 shall relieve Datapipe of any obligations specifically agreed to between the Parties in an Order Form.

7.3. Restrictions on Use of Third Party Hardware. Third Party Hardware shall remain the property of Datapipe or Datapipe's service providers and Client shall not take, nor attempt to take, any right, title, or interest in or permit any third party to take any right, title, or interest in any Third Party Hardware. Client shall not transfer, sell, assign, sublicense, pledge, or otherwise dispose of, encumber or attach a lien or encumbrance upon or against any Third Party Hardware or any interest in such equipment.

7.4. Acceptable Use Policy / Privacy Policy. Client shall comply with the AUP and Privacy Policy. Client may opt to receive e-mail notification of any changes to the AUP and Privacy Policy ("**Policy Change**") by way of its participation in the Datapipe Policy Change Opt-In System (the "**Policy Notification System**"). For purposes of initial registration in the Policy Notification System, Client shall open a ticket in the Client Portal requesting to opt-in. Notice of any Policy Change shall be sent to Client's e-mail address set forth in Section 12.18 under "Legal Contact" (the "**Notification E-Mail Address**"). Client must notify Datapipe in accordance with Section 12.10 in the event of any change to the Notification E-mail Address.

7.5. No Lease. This MSA is a services agreement and is not intended to and will not constitute a lease of any real or personal property.

7.6. End User Violations. Client will be deemed to have taken any action in which Client permits, assists or facilitates any person or entity to take related to this MSA, Client Content or its use of the Services. Client is responsible for End Users' use of Client Content and the Services. Client will exercise commercially reasonable efforts to notify end users of their obligations under this MSA and that the terms of Client's agreement with each End User are consistent with this MSA. If Client becomes aware of any violation of the Client obligations under this MSA by an End User, Client will immediately terminate such End User's access to the Client Content and Service.

7.7. High Risk. Client may not use the Services in any situation where failure or fault of the Services could lead to death or serious bodily injury of any person, or to physical or environmental damage. By way of illustration, but without limitation thereof, Client may not use, or permit any other person to use, the Services in connection with aircraft or other modes of human mass transportation, nuclear or chemical facilities, or critical medical support devices.

7.8. Client Responsibility. Client shall be responsible for maintaining the confidentiality of its account numbers and passwords for using the Client Portal and for restricting and granting access thereto. Notwithstanding anything to the contrary, Client is responsible and liable for all activities that occur utilizing Client's account (including all payments owed for Orders placed under this MSA), regardless of whether such activities are conducted by Client or any third party, and regardless of whether such Orders are authorized by Client. Datapipe does not have any obligation to verify that any individual using Client's account and password via the Client Portal has Client's authorization.

8. DATAPIPE OBLIGATIONS, REPRESENTATIONS AND DISCLAIMER OF WARRANTIES.

8.1. General. Datapipe represents that:

8.1.1. Subject to the specifications listed in each of the applicable Service Schedules and Order Forms, Datapipe shall use commercially reasonable efforts to maintain acceptable performance of the Services.

8.1.2. Its experienced and qualified personnel will provide the Services in a high quality and professional manner and in conformance with the specifications set forth in this MSA, the Order Form(s) and Service Schedule(s).

8.1.3. The Services, Third Party Hardware, Third Party Software and Datapipe Software will not infringe upon or misappropriate any Third Party's copyright, patents, trade secrets, trademark, trade name, or other proprietary or intellectual property right.

8.2. Rights. Datapipe owns or has the authority to use or license the Third Party Hardware, the Third Party Software and the Datapipe Software.

8.3. Security Audit. Upon prior reasonable advance written notice and with Datapipe's reasonable assistance, Client may conduct or cause a third party to conduct a security audit of Datapipe's operations and systems involved in or related to Datapipe's performance of Services under this MSA. Audits shall be conducted no more frequently than semi-annually, unless the Parties agree otherwise. Each auditor may be required to execute Datapipe's standard form of Non-Disclosure Agreement as a pre-condition to and prior to performing any Audit. To the extent any Audit requires Datapipe to commit more than one employee to more than one business day of Audit-related assistance, Datapipe may invoice Client $750.00 USD for each day or partial day with respect to each Datapipe employee.

8.4. Selection of Third Party Hardware and Third Party Software; Manufacturer Warranty. All Third Party Hardware and Third Party Software are provided AS-IS, WITHOUT ANY EXPRESS WARRANTY. Client's use of the Third Party Hardware and Third Party Software are subject to and controlled by the terms of any manufacturer's or supplier's terms of use. Client acknowledges that it has selected the Third Party Hardware and/or Third Party Software and that it has not relied on any statements made by Datapipe in doing so.

8.5. Substitution of Third Party Hardware, Third Party Software and/or Datapipe Software. Datapipe reserves the right to substitute hardware or software in connection with Third Party Hardware, Third Party Software and/or Datapipe Software as the case may be ("**Solution Component Substitution**") provided such Solution Component Substitution allows for the same or an increased level of performance relative to the then-existing component and is at no additional cost to Client. If necessary, Datapipe will coordinate any Solution Component Substitution which may impact the solution with Client so as to minimize any such potential impact.

8.6. DISCLAIMER OF ACTIONS CAUSED BY AND/OR UNDER THE CONTROL OF THIRD PARTIES. CLIENT ACKNOWLEDGES THAT DATAPIPE DOES NOT AND CANNOT CONTROL THE FLOW OF DATA TO OR FROM PORTIONS OF THE INTERNET OR THROUGH EQUIPMENT CONTROLLED BY THIRD PARTIES, AND THAT, AT TIMES, SUCH DATA FLOW DEPENDS IN LARGE PART ON THE PERFORMANCE OF SERVICES, EQUIPMENT OR DATA PROVIDED OR CONTROLLED BY THIRD PARTIES, THE ACTIONS OR INACTIONS OF WHICH CAN IMPAIR OR DISRUPT CONNECTIONS TO THE INTERNET (OR PORTIONS THEREOF) AND THE INTENDED FLOW OF DATA. AT TIMES, ACTIONS OR INACTIONS OF SUCH THIRD PARTIES CAN IMPAIR OR DISRUPT CLIENT'S CONNECTIONS TO THE INTERNET (OR PORTIONS THEREOF). ALTHOUGH, DATAPIPE AGREES TO USE COMMERCIALLY REASONABLE EFFORTS TO, AMONG OTHER THINGS, COMPLY WITH ALL APPLICABLE LAWS AND REGULATIONS AND USE COMMERCIALLY REASONABLE EFFORTS TO TAKE ALL ACTIONS IT DEEMS NECESSARY AND APPROPRIATE TO MINIMIZE, REMEDY AND AVOID SUCH EVENTS, DATAPIPE CANNOT GUARANTEE THAT

SUCH EVENTS WILL NOT OCCUR. IT IS CLIENT'S RESPONSIBILITY TO ENSURE THAT THE INFORMATION TRANSMITTED AND RECEIVED BY CLIENT, ITS REPRESENTATIVES, AND ITS CUSTOMERS COMPLY WITH ALL APPLICABLE LAWS AND REGULATIONS. ACCORDINGLY, DATAPIPE DISCLAIMS ANY AND ALL LIABILITY RESULTING FROM OR RELATED TO SUCH EVENTS AND SHALL NOT BE LIABLE FOR THE INADVERTENT DISCLOSURE, TRANSMISSION, FLOW, CORRUPTION OR ERASURE OF DATA AND CONTENT USED, ACCESSED, UPLOADED, INTERFACED WITH, TRANSMITTED, RECEIVED OR STORED ON THE THIRD PARTY HARDWARE OR THROUGH THE SERVICES BY THIRD PARTIES, UNLESS CAUSED BY THE GROSS NEGLIGENCE OR WILLFUL MISCONDUCT OF DATAPIPE, ITS EMPLOYEES OR ANYONE UNDER DATAPIPE'S REASONABLE CONTROL, AND CLIENT ACCEPTS SUCH DISCLAIMER WITHOUT LIABILITY TO DATAPIPE. CLIENT FURTHER ACKNOWLEDGES THAT FROM TIME TO TIME, THE SERVICES MAY BE INACCESSIBLE OR INOPERABLE DUE TO A FORCE MAJEURE EVENT OR MAINTENANCE.

8.7. <u>NO OTHER WARRANTY</u>. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN THIS MSA, THE SERVICES ARE PROVIDED ON AN AS-IS BASIS, AND CLIENT'S USE OF THE SERVICES ARE AT ITS OWN RISK. DATAPIPE, ON BEHALF OF ITS PARENTS, AFFILIATES, SUBSIDIARIES, LICENSORS AND THIRD PARTY SERVICE PROVIDERS (THE "**DATAPIPE PARTIES**"), DOES NOT MAKE, AND DISCLAIMS, ANY AND ALL OTHER EXPRESS AND/OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. THE DATAPIPE PARTIES DISCLAIM ALL RESPONSIBILITY FOR ANY SITUATION WHERE THE SECURITY, AVAILABILITY OR STABILITY OF THE SERVICES IS COMPROMISED BY (A) ACTIONS OF CLIENT OR ANY END USER, (B) THE CLIENT SOFTWARE OR (C) ANY ACTIONS TAKEN BY DATAPIPE THAT ARE REQUESTED BY CLIENT AND NOT BASED ON THE ADVICE OR RECOMMENDATION OF DATAPIPE.

9. INTELLECTUAL PROPERTY OWNERSHIP.

9.1. <u>Ownership</u>. Except for the rights expressly granted in this MSA, no rights in either Party's respective technology or intellectual property is transferred from Datapipe to Client, or from Client to Datapipe, and all right, title and interest in and to such technology and intellectual property shall remain solely with each such Party. Each Party agrees that it will not, directly or indirectly, reverse engineer, decompile, disassemble or otherwise attempt to derive source code or other trade secrets from the other Party.

9.2. <u>Ownership of Client Content</u>. Client shall retain all right, title and interest (including copyright and other proprietary or intellectual property rights) in the Client Content and all legally protectable elements, derivative works, modifications and enhancements thereof, whether or not developed in conjunction with Datapipe, and whether or not developed by Datapipe, Client or any contractor, subcontractor or agent for Datapipe or Client. To the extent ownership of the Client Content does not automatically vest in Client by virtue of this MSA or otherwise, Datapipe agrees to transfer and assign, and hereby transfers and assigns to Client all right, title and interest in the Client Content and protectable elements or derivative works thereof. Datapipe shall not sell or otherwise transfer, reproduce or use the Client Content for any purpose except to provide the Services.

9.3. <u>Suggestions</u>. Should Client or any End Users provide any Suggestions to Datapipe or Datapipe's affiliates, Datapipe will own all right, title, and interest in and to the Suggestions, even if Client has designated the Suggestions as confidential. Datapipe and its affiliates will be entitled to use the Suggestions without restriction. Client irrevocably assigns to Datapipe all right, title, and interest in and to the Suggestions and agrees to provide Datapipe with any assistance Datapipe may reasonably require to document, perfect, and maintain Datapipe's rights in the Suggestions.

10. LIMITATIONS OF LIABILITY.

10.1. LIMITATION OF LIABILITY. NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, INCIDENTAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL DAMAGES UNDER THIS MSA OR ANY THEORY OF LIABILITY INCLUDING, WITHOUT LIMITATION, LOSS OF DATA, CONTENT OR BUSINESS INFORMATION, LOSS OF TECHNOLOGY, RIGHTS OR SERVICE, ANTICIPATED OR LOST REVENUE OR SAVINGS, LOSS OF CUSTOMERS OR CLIENTS, LOST PROFITS, LOST GOODWILL, LOST BUSINESS OR REPLACEMENT GOODS OR INTERRUPTION OR LOSS OF USE OF SERVICE OR EQUIPMENT OR ANY LOSS THAT COULD HAVE BEEN AVOIDED BY SUCH PARTY'S USE OF REASONABLE PRECAUTIONS OR DILIGENCE, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES WHETHER ARISING UNDER ANY THEORY OF LIABILITY, INCLUDING BUT NOT LIMITED TO CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR BREACH OF WARRANTIES. NOTWITHSTANDING ANYTHING ELSE CONTAINED IN THIS MSA, THE MAXIMUM CUMULATIVE LIABILITY OF EITHER PARTY OR ITS SUPPLIERS, CONTRACTORS AND SUBCONTRACTORS ARISING OUT OF OR RELATING TO THIS MSA FOR ANY REASON WHATSOEVER (INCLUDING WITHOUT LIMITATION ANY PERFORMANCE OR NON-PERFORMANCE HEREUNDER, REGARDLESS OF THE FORM OF THE CAUSE OF ACTION, WHETHER IN CONTRACT, TORT, STATUTE OR OTHERWISE, SHALL IN NO EVENT EXCEED **THE GREATER OF** THE FOLLOWING:

- THE PRODUCT OBTAINED BY MULTIPLYING SIX (6) TIMES THE INITIAL MONTHLY SERVICE FEE PAYABLE (WHETHER PAID OR PAYABLE) BY CLIENT TO DATAPIPE; OR
- THE TOTAL AMOUNT PAID BY CLIENT TO DATAPIPE UNDER THIS MSA DURING THE TWELVE MONTH PERIOD PRIOR TO THE EVENT GIVING RISE TO SUCH CLAIM.

THE FOREGOING LIMITATION OF LIABILITY SHALL APPLY REGARDLESS OF WHEN THE CLAIM OR CLAIMS GIVING RISE TO SUCH LIABILITY OR LIABILITIES SHOULD OCCUR. THIS LIMITATION OF LIABILITY IS CUMULATIVE AND NOT PER INCIDENT.

THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO EITHER PARTY'S CONFIDENTIALITY AND INDEMNIFICATION OBLIGATIONS UNDER THIS MSA. RATHER, THE MAXIMUM CUMULATIVE LIABILITY OF EITHER PARTY ARISING OUT OF OR RELATING TO ITS CONFIDENTIALITY AND INDEMNIFICATION OBLIGATIONS SHALL IN NO EVENT EXCEED **THE GREATER OF** THE FOLLOWING:

- THE TOTAL AMOUNT PAID OR TO BE PAID BY CLIENT TO DATAPIPE UNDER THIS MSA DURING THE THREE (3) YEAR PERIOD PRIOR TO THE EVENT GIVING RISE TO SUCH CLAIM; OR
- TWO HUNDRED FIFTY THOUSAND DOLLARS ($250,000).

NOTWITHSTANDING ANY LIMITATIONS SET FORTH IN THIS SECTION, CLIENT SHALL BE LIABLE FOR ALL SUMS DUE OR PAYABLE UNDER THIS MSA, REGARDLESS OF AMOUNT, TOGETHER WITH ANY ADDITIONAL FEES, ATTORNEY FEES AND/OR COSTS THAT MAY BE DUE DATAPIPE PURSUANT TO SECTION 12.12.

10.2. Basis of the Bargain; Failure of Essential Purpose. The Parties acknowledge that Datapipe has set its prices and entered into this MSA in reliance upon the limitations of liability and the disclaimers of warranties and damages set forth herein, and that the same form an essential basis of the bargain between the Parties. The Parties agree that the limitations and exclusions of liability and disclaimers specified in this MSA shall survive and apply even if found to have failed in their essential purpose.

10.3. Limited Remedy. As an essential part of this MSA, any credit payable by Datapipe under the SLA(s) shall be the sole and exclusive measure of financial damages and remedy for Client, and the sole and exclusive liability and obligation of Datapipe, arising out of or in any way relating to Datapipe's failure to meet the SLA(s). The Parties further acknowledge and agree that the pricing and other terms contained in this MSA reflect and are based upon the intended allocation of risk between the Parties and form an essential part of this MSA.

11. INDEMNIFICATION.

11.1. Datapipe Indemnity. Datapipe agrees to indemnify, defend and hold harmless Client and its directors, officers, employees, contractors, agents, successors, and assigns, (collectively, the **"Client Indemnified Parties"**) from and against any and all liability (including, without limitation, attorneys' fees and costs) incurred by the Client Indemnified Parties in connection with any actual or alleged claim (**"Datapipe Claim"**) by a Third Party arising out of (a) any injury to person or property caused by Datapipe; (b) any infringement or misappropriation of a Third Party's rights based on the use of the Services, the Third Party Software or the Datapipe Software, including, without limitation, any actual or alleged infringement or misappropriation of a Third Party's copyright, trade secret, trademark or other proprietary right; or (c) any violation by Datapipe of any applicable law, court order, rule or regulation in any jurisdiction in which the Services are provided.

11.2. Client Indemnity. Client agrees to indemnify, defend and hold harmless Datapipe and its directors, officers, employees, contractors, agents, successors, and assigns, (collectively, the "**Datapipe Indemnified Parties**"), from and against any and all liability (including, without limitation, attorneys' fees and costs) incurred by the Datapipe Indemnified Parties in connection with any actual or alleged claim ("**Client Claim**") by a Third Party arising out of: (a) any injury to person or property caused by Client; (b) Client's use of the Services, Datapipe Software or Third Party Software not arising out of an act or omission of Datapipe; (c) any breach by Client of this MSA or the TPS Agreements (d) any infringement by Client of a Third Party's rights based on the Client Content or Client Software; (e) any violation or non-compliance by Client with any applicable law, court order, rule or regulation in any jurisdiction; or (f) Client's failure to possess valid licensing entitlements with respect to any Client-Licensed Software.

11.3. Limitations. Notwithstanding the foregoing, Datapipe shall not have any liability or indemnification obligations to the Client Indemnified Parties under this MSA to the extent any Datapipe Claim is based in whole or in part upon or arises out of (a) use of the Services , Third Party Software or Datapipe Software in combination with equipment, materials, products or software where the use of the Services, Third Party Software or Datapipe Software alone would not be infringing; (b) compliance with designs, plans or other instructions provided to Datapipe by or for Client; (c) any repair, adjustment, modification, configuration or alteration to the Services, Third Party Software or Datapipe Software by or for Client; or (d) any refusal by Client to install and use a non-infringing version of the Services, Third Party Software, Datapipe Software or any part thereof (including, without limitation, any update, if such infringement could have been avoided by use of the most recent update) offered by Datapipe at no cost to Client.

11.4. Notice and Procedures. The Party seeking indemnity hereunder shall give the other prompt written notice of any Datapipe Claim or Client Claim (collectively referred to as the "Claim") for which indemnity is sought and shall provide (a) all related documentation in its possession or control relating to such Claim; and (b) reasonable assistance in the defense of such Claim. The Indemnifying Party shall control, at its sole cost and expense, the defense or settlement of any Claim and shall keep the indemnified Party reasonably apprised of the status. The indemnified Party shall have the right, but not the obligation, to participate in the defense of any Claim with counsel of its choice at its sole cost and expense.

12. MISCELLANEOUS PROVISIONS.

12.1. Force Majeure. Neither Party shall be liable for delays in delivery or performance of its obligations, or for failure to deliver or perform its obligations under this MSA due to a cause or circumstances beyond its reasonable control, including, without limitation, an act of nature, act of civil or military authority, act of terrorism, governmental priority, strike or other labor disturbance, flood, fire, explosion, epidemic, other hostilities, unavailability, interruption or delay of third-party telecommunications or services, the inability to obtain raw materials, supplies, or necessary power, the failure of third-party software, or the failure of the Internet (not resulting from the actions or inactions of such Party)(each, a "**Force Majeure Event**"). The Party claiming excuse due to a Force Majeure Event shall use its commercially reasonable efforts to promptly correct such failure or delay in performance and shall promptly notify the other Party of any delay or failure to perform which may be excused by this provision, which notification will also specify the expected date of resumption of performance. In the event of any such delay, the date of performance shall be extended for a period equal to the time lost by reason of the delay. If, however, either Party is unable to perform its obligations under this MSA for reasons excused by this provision for a period in excess of 30 consecutive days, the other Party may terminate this MSA or any applicable Order Form or Service Schedule by such Force Majeure Event without penalty upon written notice to the other Party.

12.2. Relationship of Parties. Datapipe and Client are independent contractors and this MSA will not establish any relationship of partnership, joint venture, employment, franchise or agency between Datapipe and Client. Neither Datapipe nor Client will have the power to bind the other or incur obligations on the other's behalf without the other's prior written consent, except as otherwise expressly provided herein. Datapipe and Client agree that, except as otherwise expressly provided in this MSA, there shall be no third party beneficiaries to this MSA. Datapipe and Client agree that this MSA is made for the benefit of the Parties and (where applicable) their successors and permitted assigns, and is not intended to benefit, or be enforceable by, anyone else.

12.3. Export Matters. Client agrees to comply with all regulations and requirements of the U.S. Departments of Commerce, State and Treasury, and any other United States or foreign agencies and authorities in connection with Client's use of the Services and to not, in violation of any laws, regulations or requirements transfer, or authorize the transfer, of any software or Services (a) into any destination without first obtaining any license or other approval that may be required, (b) to anyone on any of the lists found at http://export.gov/ecr/eg_main_023148.asp, or (c) to any end-user or for any end-use if such end-user or end-use is prohibited by part 744 of the United States Export Administration Regulations. By using the Services, Client represents that Client is not located in any destination described in (a) above, listed on, or controlled by any person who is listed on, any list described in (b) above, or engaged in any of the activities described in (c) above. Client assumes responsibility for compliance with laws, regulations and requirements applicable to export and re-export (including import) of items provided hereunder and for obtaining any required export and re-export (including import) licenses or other approvals that may be required. Client will not transfer to or through the Services any technical data, software or other items controlled for export under the ITAR Data or other applicable laws governing ITAR Data unless Datapipe has agreed in writing to the transfer.

12.4. Personal Information. Each Party shall comply with their respective obligations under applicable data protection legislation. Datapipe does not intend to have access to PII of Client in providing the Services. To the extent Datapipe has access to Client PII, such access will be incidental and Client will remain the data controller of Client PII at all times. Datapipe will use any PII to which it has access strictly for purposes of delivering the Services.

12.5. Severability. In the event any portion of this MSA is held to be unenforceable, the unenforceable portion shall be construed in accordance with applicable law as nearly as possible to reflect the original intentions of the Parties and the remainder of the provisions shall remain in full force and effect. Either Party's failure to insist upon or enforce strict performance of any provision of this MSA, or delay in doing so, shall not be construed as a waiver of any provision or right.

12.6. Assignment. Either Party may, upon written notice to the other Party, assign this MSA to (i) its Affiliates and (ii) any entity as a result of a merger or sale of all or substantially all of the assets of such Party to such entity and such entity agrees in writing to be bound by the terms of this MSA; provided that such entity is not a direct competitor of Client or Datapipe (as the case may be) in which case the non-assigning Party may terminate this MSA by providing written notice no later than 30 days after the effective date of assignment. This MSA will be binding on and inure to the benefit of the Parties respective permitted successors and permitted assigns.

12.7. Third Party Subcontractors. Datapipe may use Third Parties or Affiliates to provide all or part of the Services. Datapipe will be responsible for ensuring that any Third Parties and Affiliates providing Services comply with Datapipe's obligations under this MSA.

12.8. Notice. Any notice or communication required or permitted to be given pursuant to this MSA, if specified to be in writing, shall be deemed delivered (i) if by hand delivery, upon receipt thereof, (ii) if by next day delivery service upon such delivery, or (iii) if by e-mail, upon verified delivery evidenced by return e-mail of the recipient. Such notice will be deemed to have been served as of the date it is delivered. All notices shall be addressed to the legal Authorized Contact designated in Section 12.18.1.

12.9. Agreement. This MSA shall be governed by, and construed in accordance with, federal law. The application to this MSA of the United Nations Convention on the International Sale of Goods is excluded in its entirety. Neither the course of conduct between the Parties nor trade practice shall act to modify any provision of this MSA. Neither Party nor its representatives will be liable for loss or damage or deemed to be in breach of this MSA if its failure to perform its obligations results from compliance with any law, ruling, order, regulation, requirement of any federal, state or municipal government or department or agency thereof or court of competent jurisdiction. Any delay resulting therefrom will extend performance accordingly or excuse performance, in whole or in part, as may be reasonable.

12.10. Remedy. All remedies in this MSA are cumulative and neither the availability nor exercise of any such remedy shall prevent a Party from exercising any other remedy it would otherwise have under this MSA or by law.

12.11. Entire Agreement. This MSA and the terms and conditions of Carahsoft's MAS Contract constitutes the complete and exclusive agreement between the Parties with respect to the subject matter hereof, and supersedes and replaces any and all prior or contemporaneous discussions, negotiations, understandings and agreements, written and oral, regarding such subject matter.

12.12. Interpretation of Conflicting Terms. In the event of a conflict between or among the terms in this MSA, the MAS Contract, and any other document made a part hereof, the conflict shall be resolved in accordance with General Services Administration Acquisition Regulation (GSAR) 552.212-4(o) Order of Precedence.

12.13. Relationship Management.

12.13.1. Authorized Contacts. Datapipe shall, as of the Effective Date, assign the following contacts as Client's authorized contacts for the account (the "**Authorized Contacts**"):

BILLING CONTACT
In the case of Datapipe:

Name: Bruce Katz, Vice President
Address: 10 Exchange Place
12th Floor
Jersey City, New Jersey 07302

Telephone: 201-792-1918
Fax: 201-792-3090
E-mail: Billing@datapipe.com

LEGAL CONTACT
In the case of Datapipe:

Name: Michael Bross, General Counsel
Address: 10 Exchange Place
12th Floor
Jersey City, New Jersey 07302

Telephone: 201-792-1918
Fax: 201-792-3090
E-mail: GovLegal@Datapipe.com

12.14. Headings. The headings in this MSA are used for convenience of reference and shall not be deemed to modify or affect the interpretation of this MSA.

Acceptable Use Policy

Datapipe has formulated this Acceptable Use Policy in order to encourage the responsible use of Datapipe's services by our customers and other users ('Users'), and to enable us to provide our Users with secure, reliable and productive services.

General Conduct

The Datapipe network, including the web sites hosted by Datapipe (collectively, the 'Datapipe Network'), may be used only for lawful purposes. Users may not use the Datapipe Network in order to transmit, distribute or store material (a) in violation of any applicable law, (b) in a manner that will infringe the copyright, trademark, trade secret or other intellectual property rights of others or the privacy, publicity or other personal rights of others, or (c) that is obscene, threatening, abusive or hateful, including the advocating of terrorism and/or the killing of any individual or group.

Child Pornography

Datapipe will cooperate fully with any criminal investigation into a Customer's violation of the Child Protection Act of 1984 concerning child pornography. Customers are ultimately responsible for the actions of their clients over the Datapipe network, and will be liable for illegal material posted by their clients. According to the Child Protection Act, child pornography includes photographs, films, video or any other type of visual presentation that shows a person who is or is depicted as being under the age of eighteen years and is engaged in or is depicted as engaged in explicit sexual activity, or the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ or the anal region of a person under the age of eighteen years any written material or visual representation that advocates or counsels sexual activity with a person under the age of eighteen years. No credits will be issued for any interruption in service resulting from policy violations. Violations of the Child Protection Act may be reported to the U.S. Customs Agency at icpicc@customs.treas.gov.

System and Network Security

Users are prohibited from violating or attempting to violate the security of the Datapipe Network, including, without limitation, (a) accessing data not intended for such User or logging into a server or account which such User is not authorized to access, (b) attempting to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without proper authorization, (c) attempting to interfere with service to any user, host or network, including, without limitation, via means of overloading, 'flooding', 'mail bombing' or 'crashing', (d) forging any TCP/IP packet header or any part of the header information in any e-mail or newsgroup posting, or (e) taking any action in order to obtain services to which such User is not entitled. Violations of system or network security may result in civil or criminal liability. Datapipe will investigate occurrences which may involve such violations and may involve, and cooperate with, law enforcement authorities in prosecuting Users who are involved in such violations.

Operating System End Of Life

Customer agrees that it shall not utilize an operating system platform which has been declared by its manufacturer or creator, or determined by Datapipe to be End of Life (EOL). An EOL operating system platform typically means that no further changes to the platform will be made, no new releases or patches created, support for the platform ends, no testing is performed after the EOL date, and no technical support provided. Since the use of an EOL operating system exposes a Customer to unknown and unpreventable vulnerabilities, to the extent that a Customer elects to utilize an EOL operating system, such use shall only be permitted provided Customer executes the then-current form of Datapipe EOL Operating System Waiver.

E-Mail

Users may not send unsolicited e-mail messages, including, without limitation, bulk commercial advertising or informational announcements ('spam') in a way that could be reasonably expected to adversely impact the Datapipe Network, including, without limitation, using an e-mail account on Datapipe's network to send spam or bulk e-mail, or using the service of another provider to send spam or to promote a site hosted on or connected to the Datapipe Network. In addition, Users may not use the Datapipe Network in order to (a) send e-mail messages which are excessive and/ or intended to harass or annoy others, (b) continue to send e-mail messages to a recipient that has indicated that he/she does not wish to receive them, (c) send e-mail with forged TCP/IP packet header information, (d) send malicious e-mail, including, without limitation, 'mail bombing', (e) send or receive e-mail messages in a manner that violates the use policies of any other internet service provider, or (f) use an e-mail box exclusively as a storage space for data (g) Offering for sale or soliciting e-mail lists for the purposes of bulk e-mail.

Usenet

Users who post messages to Usenet newsgroups are responsible for becoming familiar with any written charter or FAQ governing use of such newsgroups and complying therewith. Regardless of such policies, Users may not (a) post the same message, or a series of similar messages, to one or more newsgroups (excessive cross-posting or multiple-posting, also known as 'Usenet spam'), (b) cancel or supersede posts not originally posted by such User, unless such User does so in the course of his/her duties as an official newsgroup moderator, (c) post any message with forged packet header information, or (d) post messages that are excessive and/or intended to annoy or harass others, including, without limitation, chain letters.

Suspension; Termination

Any User which Datapipe determines to have violated any element of this Acceptable Use Policy shall receive a written warning, and may be subject at Datapipe's discretion to a temporary suspension of service pending such User's agreement in writing to refrain from any further violations; provided, however, that if Datapipe deems it necessary, it may immediately suspend or terminate such User's service without issuing such a warning. Users which Datapipe determines to have committed a second violation of any element of this Acceptable Use Policy shall be subject to immediate suspension or termination of service without further notice.

Responsibility

Datapipe takes no responsibility for any material input by others and not posted to the Datapipe Network by Datapipe. Datapipe is not responsible for the content of any other web sites linked to the Datapipe Network; links are provided as Internet navigation tools only.

Privacy

Any User interacting with our site and providing Datapipe with name, address, telephone number, e-mail address, domain name or URL or any other personally identifiable information permits Datapipe to use such information for commercial purposes of its own, including contacting Users about products and services which may be of interest. For each visitor to our Web Site, our Web server recognizes only the visitor's domain name, not the e-mail address. We collect information volunteered by the visitor, such as form submittals and/or site registrations. This information is used to improve the content of our Web site, it is not shared with other organizations for commercial purposes. Any User who does not wish to receive further contacts from Datapipe should send Datapipe a specific request (i.e., stating do not use or do not share or both) by certified mail or by regular mail clearly marked 'Privacy-Urgent' addressed as follows: Datapipe, 10 Exchange Place, 12th Floor, Jersey City, New Jersey 07302.

Datapipe does not sell, rent or otherwise disclose its mailing lists to third parties.

Datapipe reserves the right to modify this Acceptable Use Policy at any time in its sole and absolute discretion.

(Rev. 10/1/01)

Datapipe Privacy Policy

Last Updated: *17 April, 2017*

PART I. GENERAL INFORMATION

Our commitment to privacy

Your privacy is important to us and maintaining your trust is our priority. To ensure that your privacy is protected and your privacy choices are respected, Datapipe, Inc. and its group companies (collectively "**Datapipe**", "**we**", "**our**" and "**us**") have set out in this Privacy Policy an explanation of our information practices as well as the decisions you may make regarding how your information is collected and used by us.

This policy covers the personal information that is collected via our websites datapipe.com, datapipe.net and their subdomains (the "**Website**") or through any other means, such as personal information that we process when we do business generally, or when you engage with us as a client or potential client in relation to the provision of any of our products or services (the "**Services**").

Introduction to Datapipe

Datapipe is a US-headquartered company which architects, deploys and manages hosting and other IT solutions for our clients. In practical terms, this means we at times act on behalf of our clients to work with third party vendors like Amazon Web Services and Microsoft to ensure that our clients have cloud solutions fit for their business purposes. We also provide a range of other services including our own data center services, systems management and IT security and compliance.

PART II. WHAT WE COLLECT AND HOW WE USE IT

Information you provide to us on the Website: In general, you can visit our publicly accessible websites without telling us who you are or revealing any information about yourself. However, you may give us personal information through our Website, for example, when you make enquiries about our Services or provide us with your contact information for the purpose of sending you white papers, signing up to our newsletter or obtaining a quote or arranging a consultation. Our clients are also able to provide us with updated billing information through our Website, if they wish to do so. When you communicate with us, we will keep copies of any communications that you send us.

We will also collect user account information (such as name, email addresses and telephone numbers) when you register an account with us. If you are an administrator or manager utilizing our Services and wish to set up accounts on behalf of other users (such as your employees), you must ensure you are fully authorized to do so, which means - for example - making sure that the individual concerned is aware of your use of their personal information, that you are lawfully entitled to disclose it to us and that they are informed of their rights in respect of that information. If you cannot ensure that such requirements are met, please do not provide us with the information.

Information we collect automatically through the website: We may also collect certain information through our Website by automated means, such as IP addresses, browser type and operating system, referring URLs, information about your visit including the URL clickstream to, through and from our Website, download errors, number of Website visits, and other page interactions. We collect this information automatically through the use of various technologies including through cookies. For further information about the cookies that we use on our website and how to exercise your cookie preferences, see our Cookies Policy.

Information which our clients provide to us. We also collect information which our clients and potential clients provide directly to us when conducting business with us. For example, we collect information when our clients (and their users) engage with Datapipe for us to provide or potentially provide Services. The types of information we may collect directly from our clients and their users may include names, usernames, email addresses, postal addresses, phone numbers, technical details of current and desired Services, policies and procedures, job titles, transactional information (including Services purchased), financial/billing information, as well as any contact or other information they choose to provide for us to undertake the Services. For example, such information will include any information that our clients instruct us to manage with respect to a third party cloud platform.

We may also collect personal information, such as your contact details, when you attend our events, take part in surveys or through other marketing interactions we may have with you.

Information we collect in the course of operating our business: We also collect information from our vendors, suppliers, consultants, professional advisers and other third parties for the purposes of managing and operating our business. For example, we will collect business contact information, financial information and other information necessary to engage our suppliers and other business partners and to evaluate their performance.

Information we may collect automatically when you use the Services. Usage information – we may keep track of user activity in relation to the types of Services our clients and their users use, the configuration of their computers, and performance metrics related to their use of the Services. Log information – we may log information about our clients and their users when you use one of the Services including Internet Protocol ("IP") address and Internet Service Provider ("ISP"). Information collected by cookies and other similar technologies – we use various technologies to collect information which may include saving cookies to users' computers. For further information about the cookies that we use on our Services and how to exercise your cookie preferences, see our Cookies Policy.

Use of information

We may use the information we collect as outlined above for the following purposes:

- Provide, operate, optimize and maintain the Website and Services;
- To deal with your online inquiries and requests, and to provide you with information, and access to resources that you have requested from us;
- Manage our Website and system administration and security;
- Improve the navigation and content of our Website;

- Process and complete transactions, and send related information, including transaction confirmations and invoices;
- Manage our clients' use of the Services, respond to inquiries and comments and provide client service and support;
- Analyze clients' use of the Services for trend monitoring, marketing and advertising purposes;
- Send clients technical alerts, updates, security notifications, and administrative communications;
- Investigate and prevent fraudulent activities, unauthorized access to the Services, and other illegal activities; and
- For other legitimate business purposes and any other purposes about which we notify clients and users.

Client Data

When our clients engage us to provide the Services, we may process and store data, some of which may be personal information, on their behalf pursuant to our Services agreements with them ("**Client Data**"). For example, our clients may upload and store personal information on Datapipe hosted and/or managed solutions that we offer and provide to them. In such cases, we are acting as a data processor in respect of the Client Data and will process such data only on our client's behalf and strictly in accordance with their instructions. It is our clients, as the data controllers, who control the use of the account and what information is uploaded.

If you have any questions or concerns about how Client Data is handled, you should contact the relevant client directly or refer to their privacy policies.

Alternatively, if you are a client and want to find out more about the optional security controls that you have elected for your account, or other data protection provisions, you can refer to your Services agreement or other applicable contractual documents with Datapipe, or contact us for further information.

Sharing and disclosure of information to third parties

We may share and disclose information about our clients and their users in the following circumstances:

- *Vendors, consultants and other third party service providers* – we may share information with third party vendors, consultants and other service providers who require access to your information to assist in the provision of the Website and the Services. In particular, where clients have requested that we deploy cloud services with a third party infrastructure provider (for example, AWS or Microsoft Azure), we will disclose certain limited client information to that infrastructure provider to provide the services client has requested, or where our clients have elected to implement certain security measures on their account, we may engage security management service providers;
- *Compliance with laws* – we may disclose information to a third party where we are legally required to do so in order to comply with any applicable law, regulation, legal process or government request, including in response to public authorities to meet national security or law enforcement requirements;

- *Vital interests and legal rights* - we may also disclose information where we believe it necessary in order to protect the vital interests of any person, or exercise, establish or defend our legal rights; and
- *Business transfers* – we may share or transfer information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business to another company.

PART III. INTERNATIONAL TRANSFERS AND SECURITY

Processing of information in the U.S. and elsewhere

Information collected outside of the United States, including in the European Economic Area and Switzerland, may be transferred to the United States. Your information may be stored on our servers in the United States and potentially in other countries whose data protection laws may be different to the laws in your country. We will protect your information in accordance with this Privacy Policy wherever it is processed.

In particular, please note that where clients have requested that we deploy cloud services with Datapipe or other infrastructure provider (for example, AWS or Microsoft Azure), that infrastructure provider may give you the option to choose the location or region in which you wish to host your data. In such circumstances, the client is solely responsible for deciding which location is adequate for the purposes of the data it wishes to host, taking into account the nature and the sensitivity of the data in question.

EU-US and Swiss-US Privacy Shield

When processing personal information from the European Economic Area and Switzerland, Datapipe, Inc. and its US subsidiaries have certified our compliance with the EU-US Privacy Shield and Swiss-US Privacy Shield and we commit to adhere to the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfers, Security, Data Integrity & Purpose Limitation, Access, Recourse, Enforcement and Liability. To access the Privacy Shield List and to find details of our certification, please see https://www.privacyshield.gov/.

Datapipe, Inc. and its US subsidiaries are subject to the investigation and enforcement powers of the Federal Trade Commission.

When we transfer personal information to third party agents, we will contractually require that they process your personal information only for the purposes described in this policy and to provide the same level of protection as the Privacy Shield Principles. It is our responsibility to ensure that our third party agents and service providers protect your data in accordance with the commitments contained in this Privacy Policy, and we will be responsible under the Privacy Shield for their processing of your data, unless we prove that we are not responsible for the damage.

If you believe your information has not been processed in accordance with the Privacy Shield Principles, you can make a complaint in the following ways:

(1) You can contact us directly at privacyshield@datapipe.com or at the mailing address below and we will respond to your complaint within 45 days of receipt:
ATTN: Legal Department, Datapipe, Inc., 10 Exchange Place, Jersey City, NJ 07302, USA

(2) We have further committed to cooperate and comply with the panel of the European data protection authorities (DPAs), or the Swiss Federal Data Protection and Information Commissioner (if you are from Switzerland), in the resolution of your Privacy Shield complaint.

If you are unsatisfied with the response you have received from us, or your complaint remains unresolved, you can contact your local DPA (contact details of the European DPAs are available here: http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm) which will investigate your complaint free of charge.
Where appropriate, your local data protection authority may refer your complaint to the US Department of Commerce or the Federal Trade Commission for further investigation.

Security
We use appropriate technical, organizational and administrative measures to help protect any information we process about our clients or their users. Please note that when a client instructs us to host data with a third party infrastructure provider, that provider will have its own technical, organizational and administrative measures to protect the data it processes. It is our clients' responsibility to assess the appropriateness of the security measures in place with any third party infrastructure provider before it instructs us to arrange hosting with that provider on its behalf.

In addition, we offer certain optional security protections that our clients may choose to deploy. These optional security protections are not provided by default and will not be implemented unless expressly agreed with our clients at the time they order Services from us. It is our clients' responsibility to assess the need for and appropriateness of these optional security protections, taking into account the nature and the sensitivity of their data.

Please note that no service is completely secure and so, while we endeavor to protect our clients' information using the measures described above, we cannot guarantee that unauthorized access, hacking, data loss or a data breach will not occur although we shall at all times utilize commercially reasonable measures to protect your Data. Although we will do our best to protect your personal information, you should only access the Services within a secure environment. You should always ensure that your login credentials and password are kept safe at all times. You should notify us as soon as possible if you become aware of any misuse of your password or your account, and immediately change your password within the service.

PART IV. YOUR PRIVACY RIGHTS

Update and access to your information

If you are from certain territories (such as the EU or Switzerland), you may have the right to access your personal information, or to correct, amend and delete any personal information we hold about you if it is inaccurate or processed in violation of the Privacy Shield Principles. You can send an email to privacyshield@datapipe.com, or call us on 201-792-1918 for this purpose. We will consider your request in accordance with the Privacy Shield Principles and any applicable laws. We may reject requests where, for example, the burden or expense of providing access to your information is disproportionate, or where your request violates the rights of third parties.

For any personal information that is stored or processed by us through the Services on our client's behalf (see "Client Data" section above), Datapipe is acting as a data processor. This means that if you wish to access, review, modify or delete any such personal information, you should direct your query to your client (the data controller). We will then help them to fulfil that request in accordance with their instructions and our Privacy Shield and other contractual commitments.

Limiting Use and Disclosure

Furthermore, we commit to giving you an opportunity to opt out if personal information we control about you is to be disclosed to any other independent third parties, or is to be used for a purpose materially different from those that are set out in this Privacy Policy. Where sensitive personal information is involved, we will always obtain your express opt-in consent to do such things. If you otherwise wish to limit the use or disclosure of your personal information, please write to us at the contact details further below.

Unsubscribe from our mailing list

You may at any time ask us to remove you from any mailing list on which you previously asked us to include you by sending us an email at privacyshield@datapipe.com, by calling us on 201-792-1918, or by clicking "Unsubscribe" in any e-mail communications we send you.

PART V. OTHER IMPORTANT INFORMATION

Changes to our Privacy Policy

If we change our Privacy Policy, we will post those changes on this page in addition to updating the "Last Updated" date at the top of this webpage. If we make material changes, we will notify our clients more directly, for example by posting a notification or message on our website or by emailing you prior to such changes taking effect. We encourage you to review this Privacy Policy frequently to stay informed of the latest modifications.

Children

Our Services are not directed to individuals under the age of 18. We do not knowingly collect personal information from such individuals. If you become aware that a child has provided us with information, please contact us at privacyshield@datapipe.com. If we become aware that a child under the age of 18 has provided us with personal information, we will take steps to delete such information.

How to contact us

If you have any questions, comments or concerns about this Privacy Policy, then please contact us via email at privacyshield@datapipe.com or at the following mailing address:

ATTN: Legal Department
Datapipe, Inc.
10 Exchange Place
Jersey City
NJ 07302
USA

TERMS AND CONDITIONS REGARDING USE OF MICROSOFT SOFTWARE

This document governs the use of Microsoft software, which may include associated media, printed materials, and "online" or electronic documentation (individually and collectively, "Licensed Products") provided by **Datapipe, Inc.** (hereinafter referred to as "Company"). Company does not own the Licensed Products and the use thereof is subject to certain rights and limitations of which Company must inform you. Your right to use the Licensed Products is subject to the terms of your agreement with Company, and to your understanding of, compliance with, and consent to the following terms and conditions, which Company does not have authority to vary, alter, or amend.

1. DEFINITIONS.

"Client Software" means software that allows a Device to access or utilize the services or functionality provided by the Server Software.

"Device" means each of a computer, workstation, terminal, handheld PC, pager, telephone, personal digital assistant, "smart phone," server or other electronic device.

"Server Software" means software that provides services or functionality on a computer acting as a server.

"Software Documentation" means any end user document included with server software.

"Redistribution Software" means the software described in Paragraph 4 ("Use of Redistribution Software") below.

2. **OWNERSHIP OF LICENSED PRODUCTS.** The Licensed Products are licensed to Company from an affiliate of the Microsoft Corporation (collectively "Microsoft"). All title and intellectual property rights in and to the Licensed Products (and the constituent elements thereof, including but not limited to any images, photographs, animations, video, audio, music, text and "applets" incorporated into the Licensed Products) are owned by Microsoft or its suppliers. The Licensed Products are protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. Your possession, access, or use of the Licensed Products does not transfer any ownership of the Licensed Products or any intellectual property rights to you.

3. **USE OF CLIENT SOFTWARE.** You may use the Client Software installed on your Devices by Company only in accordance with the instructions, and only in connection with the services, provided to you by Company. The terms of this document permanently and irrevocably supersede the terms of any Microsoft End User License Agreement that may be presented in electronic form during your use of the Client Software.

4. **USE OF REDISTRIBUTION SOFTWARE.** In connection with the services provided to you by Company, you may have access to certain "sample," "redistributable" and/or software development ("SDK") software code and tools (individually and collectively "Redistribution Software"). **YOU MAY NOT USE, MODIFY, COPY, AND/OR DISTRIBUTE ANY**

REDISTRIBUTION SOFTWARE UNLESS YOU EXPRESSLY AGREE TO AND COMPLY WITH CERTAIN ADDITIONAL TERMS CONTAINED IN THE SERVICES PROVIDER USE RIGHTS ("SPUR") APPLICABLE TO COMPANY, WHICH TERMS MUST BE PROVIDED TO YOU BY COMPANY. Microsoft does not permit you to use any Redistribution Software unless you expressly agree to and comply with such additional terms, as provided to you by Company.

5. **COPIES.** You may not make any copies of the Licensed Products; provided, however, that you may (a) make one copy of Client Software on your Device as expressly authorized by Company; and (b) you may make copies of certain Redistribution Software in accordance with Paragraph 4 (Use of Redistribution Software). You must erase or destroy all such Client Software and/or Redistribution Software upon termination or cancellation of your agreement with Company, upon notice from Company or upon transfer of your Device to another person or entity, whichever occurs first. You may not copy any printed materials accompanying the Licensed Products.

6. **LIMITATIONS ON REVERSE ENGINEERING, DECOMPILATION AND DISASSEMBLY**. You may not reverse engineer, decompile, or disassemble the Licensed Products, except and only to the extent that applicable law, notwithstanding this limitation, expressly permits such activity.

7. **NO RENTAL.** You may not rent, lease, lend, pledge, or directly or indirectly transfer or distribute the Licensed Products to any third party, and may not permit any third party to have access to and/or use the functionality of the Licensed Products except for the sole purpose of accessing the functionality of the Licensed Products in the form of software services in accordance with the terms of this agreement and any agreement between you and Company.

8. **TERMINATION.** Without prejudice to any other rights, Company may terminate your rights to use the Licensed Products if you fail to comply with these terms and conditions. In the event of termination or cancellation of your agreement with Company or Company's agreement with Microsoft under which the Licensed Products are licensed, you must stop using and/or accessing the Licensed Products, and destroy all copies of the Licensed Products and all of its component parts.

9. **NO WARRANTIES, LIABILITIES OR REMEDIES BY MICROSOFT. ANY WARRANTIES, LIABILITY FOR DAMAGES AND REMEDIES, IF ANY, ARE PROVIDED SOLELY BY COMPANY AND NOT BY MICROSOFT, ITS AFFILIATES OR SUBSIDIARIES.**

10. **PRODUCT SUPPORT.** Any support for the Licensed Products is provided to you by Company and is not provided by Microsoft, its affiliates or subsidiaries.

11. **NOT FAULT TOLERANT.** THE LICENSED PRODUCTS MAY CONTAIN TECHNOLOGY THAT IS NOT FAULT TOLERANT AND ARE NOT DESIGNED, MANUFACTURED, OR INTENDED FOR USE IN ENVIRONMENTS OR APPLICATIONS IN WHICH THE FAILURE OF THE LICENSED PRODUCTS COULD LEAD TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL, PROPERTY OR ENVIRONMENTAL DAMAGE.

12. **EXPORT RESTRICTIONS.** The Licensed Products are of U.S. origin for purposes of U.S. export control laws. You agree to comply with all applicable international and U.S. laws that apply to the Licensed Products, including the U.S. Export Administration Regulations, as well as end-user, end-use and destination restrictions issued by the U.S. and other governments. For additional information, see http://www.microsoft.com/exporting/.

13. **LIABILITY FOR BREACH.** In addition to any liability you may have to Company, you agree that you will also be legally responsible directly to Microsoft for any breach of these terms and conditions.

Government Managed Cloud Hosting Services Schedule

This Managed Cloud Hosting Services Schedule for Client ("**Managed Cloud Hosting Services Schedule**") to the MSA provides additional terms and conditions under which Client has elected to purchase Managed Cloud Hosting Services from Datapipe Government Solutions, Inc., (hereinafter, "Datapipe") as more particularly described in the Order Form(s). Unless otherwise defined herein, capitalized terms shall have the meanings ascribed to them in the MSA. The SLA governing the Managed Cloud Hosting Services is set forth as Exhibit "A" to this Managed Cloud Hosting Services Schedule for Client.

ADDITIONAL GENERAL TERMS AND CONDITIONS:
The following provisions shall be in addition to or supplement the corresponding provisions of the MSA, as the case may be:

1. DEFINITIONS (MSA SECTION 1).

"Client Portal" means Datapipe's in-house ticketing system found at https://one.datapipe.com or such other URL as may be designated by Datapipe from time to time.

"Cloud Infrastructure" means the hardware and software resources needed to deploy the cloud hosting environment. This includes the host servers, switches, firewalls, hypervisor, and virtual operating systems.

"Datapipe Equipment" means the dedicated hardware provided by Datapipe as described in the Datapipe Service Descriptions section as set forth in this Managed Cloud Hosting Services Schedule.

"Datapipe Network" means from the internal LAN-side Ethernet interface of the Border Routers to the Client Access Switch via all Datapipe-owned and managed networking hardware.

"**Disaster Declaration**" means the submission by the authorized Client representative of a ticket via the Client Portal declaring a disaster event and requesting that Datapipe initiate a restoration of the Production Environment at its Disaster Recovery Site.

"Disaster Recovery Site" means the secondary site data center located in Highlands Ranch, CO where Client production data will be replicated.

"**Emergency Maintenance**" means any critical unforeseen maintenance or upgrades needed for the security, redundancy or performance of client configuration, Datapipe infrastructure and/or the Datapipe Network.

"Managed Cloud Hosting Services" means the specific Services described in this Managed Cloud Hosting Services Schedule or any Order Form.

"**Minimum Level Resources**" means the committed minimum capacities for each resource used to provide Datapipe's Managed Cloud Hosting Services, per the Client's requirements. Minimum Level Resources shall be defined in the Order Form(s).

"**Monthly Remittance Date**" means the 10th day of each calendar month.

"Monthly Uptime Percentage" means the percentage of time Datapipe guarantees that the dedicated cloud hardware used to provide Managed Cloud Hosting Services is available to the Client and/or Client's end user, excluding Scheduled Maintenance and Emergency Maintenance.

"Order Form" means any order form executed by both Client and Datapipe, including, but not limited to Work Orders. Each Order Form will be considered a separate agreement from any other Order Form. Each Order Form shall be governed by the MSA and this Managed Cloud Hosting Service Schedule and shall become effective on the Order Form Effective Date.

"Order Form Commencement Date" means the date as defined in a specific Order Form.

"Order Form Effective Date" means the effective date set forth and identified as such on any Order Form.

“Order Form Expiration Date” means the expiration date set forth and identified as such on any Order Form.

“Parties” means Datapipe and Client collectively.

“Party” means Datapipe or Client individually.

“Person” means any natural person, corporation, limited liability company, trust, joint venture, association, company, partnership, governmental authority or other entity.

“Production Environment” means the environment that is replicated to the Disaster Recovery Site and is used by Client’s end customer as their primary environment for utilizing the software services being delivered by Client. Datapipe shall be responsible for the Production Environment up through and including the virtual operating system.

“**Restoration Success**” means that the Datapipe Equipment at the Disaster Recovery Site is fully functional and that such Datapipe Equipment and the Production Environment are both online and available for Client use.

“**Recovery Point Objective (“RPO”)**” means the maximum amount of permitted data loss upon Restoration Success.

“**Recovery Time Objective (“RTO”)**” means the duration of time between a Disaster Declaration and Restoration Success. RTO does not include any time required for external DNS or other external network protocols to be migrated by Third Party providers and other Third Party components and dependencies outside of Datapipe’s control.

“**Scheduled Maintenance**” means any maintenance at a facility in which the Services are provided or any component of the Services, of which Client is notified at least forty-eight (48) hours in advance. Notice of Scheduled Maintenance will be provided through the Datapipe ticketing system.

“Services” means all of the services (a) ordered by Client as set forth on the corresponding Order Form(s) governed by the MSA and this Managed Cloud Hosting Services Schedule. The Services may be modified as provided in the Order Form(s) and this Managed Cloud Hosting Services Schedule.

“Service Term” means as to each Service ordered by Client, the period commencing on the Order Form Commencement Date with respect to each particular Order Form and ending on the Order Form Expiration Date designated in that Order Form.

“SLA” means the Service Level Agreement set forth in this Managed Cloud Hosting Services Schedule.

“Term” means the Service Term and any corresponding Renewal Term.

“Third Party” means a Person that is not a Party or an affiliate of a Party.

2. GENERAL

The provisions and terms of the MSA may only be amended or waived by written amendment or waiver signed by authorized representatives of the GSA and Carahsoft Technology Corporation (Carahsoft), and shall automatically be subject to, incorporated into, and become part of the MSA and the Managed Cloud Hosting Services Schedule.

3. MANAGED CLOUD HOSTING SERVICES BILLING.

Client shall be billed in arrears for the usage of all usage-based Managed Cloud Hosting Services accessed or made use of by Client and any associated fees and minimum commitments for Services provided in the previous calendar month. Billing for storage shall be based upon the cumulative amount of storage used by all VMDK, VHD, or VHDx files, as seen by the hypervisor, and all data backup files. Billing for Virtual Machines (“VM”) shall be billed for all running VMs. Billing for Cloud Server Compute Resources – vCore Units shall be determined by the greater of the following two values from the previous billing cycle; (a) total amount of allocated vCPUs; or (b) total amount of allocated RAM (in gigabytes) divided by four (4) and rounded up to the nearest integer.

4. EXPORT MATTERS

Client may not provide access to the Managed Cloud Hosting Services to any person (including any natural person or government or private entity) that is located in or is a national of any country that is embargoed or highly restricted under US export regulations.

5. INTERPRETATION OF CONFLICTING TERMS

In the event of a conflict between the terms in the MSA, the MAS Contract, and this Managed Cloud Hosting Services Schedule, the conflict shall be resolved in accordance with GSAR 552.212-4(o) Order of Precedence.

6. SERVICE INFORMATION.

Datapipe will collect certain information about Client’s usage of the Managed Cloud Hosting Services, including but not limited to CPU utilization, memory usage, IO performance, and error and information messages.

[THE BALANCE OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

EXHIBIT A

1. DATAPIPE SERVICE DESCRIPTIONS.

1.1. CLOUD STORAGE SERVICES.

Datapipe fully manages storage environment for backups, disaster recovery and production application storage capabilities. Tasks performed in maintaining the secure storage in cloud environment include:

- Manage Storage Allocation
- Provision Storage for use by virtual servers
- Monitoring, alerting and 24x7 response
- Allocation rebalancing
- Patch management
- Hardware maintenance

1.2. CLOUD SERVER COMPUTE RESOURCES.

Datapipe Cloud Server Compute Resources--VCore Service (hereinafter, "**VCore**") provides the use of dedicated computing resources that can be deployed across the Cloud Infrastructure to meet the needs of the Client's applications. Each increment of VCore includes guaranteed computing resources of up to 4GB of memory and one (1) virtual CPU Core and can be combined to create virtual machines to match Client's requirements (e.g., combining multiple VCore resources to create a (2) virtual CPU, 8GB RAM virtual machine).

The VCore service includes the services below:

- 24x7 Underlying Hardware Maintenance – Datapipe provides for the maintenance, repair or replacement of any failed underlying VCore hardware components.
- 24x7 Managed & Controlled IT Environment – VCore shall reside within Datapipe' 24x7 managed and controlled IT environment including controlled temperature & humidity, UPS and diesel generator power backup, fire detection and suppression systems, and physical security and electronic security.

Scalability

The Managed Cloud Hosting Services can scale up or down above the Minimum Level Resources, as defined in the Order Form, by up to twenty (20) percent of the Minimum Level Resources within 24 hours if needed, but only after proper change control procedures and written approvals have been completed per FEDRAMP requirements. The Managed Cloud Hosting Services can scale greater than twenty (20) percent above the Minimum Level Resources, if needed. In order to scale above the Minimum Level Resources, increments of the growth resources listed in the Order Form may be purchased with each purchase carrying a minimum one-month term. Any growth that is above twenty percent greater than the Minimum Level Resources, shall be provided within an agreed upon timeframe from receipt of written notice from an authorized Client representative regarding the need for additional resources and the associated capacity that is needed for each additional resource line item. Upon scaling the Managed Cloud Hosting Services equal to or by more than twenty (20) percent above the Minimum Level Resources, the Minimum Level Resources shall be adjusted to the new total resource quantities after the additional resources are added. This Minimum Level Resources adjustment shall apply to each of the resource types (Cloud Storage Services or Cloud Server Compute Resources) on an individual basis and will not require the Minimum Level Resources for all types to be adjusted simultaneously.

1.3. FEDRAMP MODERATE –COMPLIANT CLOUD SERVER MANAGEMENT

Datapipe FEDRAMP Moderate -Compliant Cloud Server Management - Datapipe provides administration, monitoring and alerting of the underlying Cloud hardware and Datapipe-provided network infrastructure, as well as the supported cloud server operating system(s) deployed. Management services provide support for the Managed Cloud Hosting Services and are available on a 24x7 basis for supported versions of Microsoft Windows and Unix/Linux operating systems.

Implementation Service – Datapipe Cloud Server Management Implementation Service provides the implementation and initial implementation testing of the monitoring, alerting and O/S administration tools for the cloud servers deployed.

24x7 Operating System Administration – Datapipe provides administration of supported cloud server operating system. This includes operating system hardening, patching and troubleshooting.

Operating System Hardening - Datapipe hardens supported operating systems based on either DISA Security Technical Implementation Guide (STIG) benchmarks or the CIS benchmarks based on Client requirements.

24x7 Monitoring and Alerting – Datapipe monitors the performance, availability, network connectivity, and security of supported cloud server as defined in Datapipe's FedRAMP certified System Security Plan. Datapipe uses monitoring information to help spot and address system bottlenecks.

Routine Preventative Maintenance - Datapipe shall schedule preventative maintenance windows to apply maintenance patches and perform preventive maintenance activities as required for the operating systems and software components that Datapipe supports. Preventative maintenance periods are scheduled during times that are convenient to the Client.

24x7 Help-Desk-to-Help-Desk Technical Support – Designated Client support personnel may contact Datapipe Technical Support at any time on a 24x7 basis for technical assistance via email and phone calls.

Support Requests – For all support requests, change requests, or incidents a ticket (otherwise known as a "ticket") shall be created within the Datapipe ticketing system. Following the submission of the ticket, Datapipe's response time will match the agreed upon severity of the ticket as described in Section 4 of Exhibit A of this Service Schedule. Datapipe and Client agree that no work shall be completed until a ticket has been created within the Datapipe ticketing system. If the Datapipe ticketing system is unavailable, the timer for purposes of SLA response measurements shall not begin until a call has been placed into Datapipe's support team.

When creating a ticket in the Datapipe ticketing system the requestor/creator shall specify the type of ticket (Incident or Service Request) in the drop down menu when creating a ticket

Datapipe's ticket system will send an email notification to the requestor/creator of the ticket as well as the approver when a ticket is closed by Datapipe support personnel.

Managed Backups – Datapipe will provide daily incremental and weekly full backups of all environments, and those backups will be stored onsite for thirty (30) calendar days.

Datapipe will provide Offsite backups for Client's Production environment once per week and those backups will be stored for ninety (90) days in a secure offsite location per Datapipe's FedRAMP (Federal Risk and Authorization Management Program) backup procedures.

Datapipe will monitor that the local backup procedure for each environment is running successfully and not failing. If there is a failure, the backup system will automatically re-attempt the backup until a successful backup has occurred. If any attempts or re-attempts of nightly backups are in a failed state the following morning, Datapipe support personnel will open a Severity 1 ticket within the Datapipe ticketing system and work to resolve the issue to ensure the backup successfully occurs. Only after confirmation that a successful backup has occurred will Datapipe support personnel close the ticket for the backup failure.

1.4. BASE INFRASTRUCTURE AND SECURITY SERVICES – FEDRAMP/FISMA COMPLIANT

The Managed Cloud Hosting Services provides a fully managed government application environment that is architected for FEDRAMP security guidelines in accordance with Datapipe's FedRAMP certified System Security Plan.

24x7 System Administration & Maintenance Services - Datapipe shall provide 24x7 system administration and maintenance services for all elements of the Managed Cloud Hosting Services as defined in Datapipe's FedRAMP certified System Security Plan. Servers are configured and patches are applied per predefined change control and patching procedures to ensure a controlled, high-availability environment. Datapipe will install and implement Client's environment, and will provide for the maintenance, repair or replacement of all hosted components of the Client's cloud environment. These services include 24x7 managed network services as defined in the Order Form.

24x7 Managed Security Services - The Managed Cloud Hosting Services environment leverages robust security controls to enable FEDRAMP Moderate compliance. Security controls include: continuous monitoring, managed firewalls, IDS, device hardening, security vulnerability scans, enhanced remote access security and managed authentication, change control, configuration management, ongoing formal security training of administrative personnel, and security process documentation.

Some of the tools and processes that the Datapipe team uses to secure the Managed Cloud Hosting Services include:

- Keystroke Logging Software
- Vulnerability Scanners
- IT Infrastructure and Network Monitoring
- Dual factor Remote Access Authentication
- Host-based Intrusion Detection
- Network Intrusion Detection
- Administration of Dedicated Firewall
- Continuous Monitoring Program
- Formal Emergency Incident Response
- Formal Change Control Tools and Process
- Formal Configuration Management
- Contingency Planning
- Formal Security Training
- Government Certification and Accreditation Audit Support
- Ongoing FEDRAMP Compliance Monitoring and Administration

2. DATAPIPE DEDICATED CLOUD HARDWARE AVAILABILITY GUARANTEE.

2.1. DATAPIPE MANAGED CLOUD HOSTING SERVICE 99.5% AVAILABILITY GUARANTEE.

Datapipe guarantees that the dedicated cloud hardware used to provide Managed Cloud Hosting Services shall maintain a Monthly Uptime Percentage of 99.5% (excluding Scheduled Maintenance and Emergency Maintenance) (any such failure to meet the foregoing guarantee considered a "**Covered Cloud Outage**"). Upon written request, Datapipe will calculate Client's Covered Cloud Outage for the previous month. Client shall provide such written request within thirty (30) days of the end of the month in question. Should Datapipe not meet the Monthly Uptime Percentage guarantee, Datapipe shall, as Datapipe's sole obligation and Client's sole and exclusive remedy for failure to meet the foregoing guarantee, credit Client's account for every one (1) consecutive hour of Covered Cloud Outage with a sum equal to the prorated average fee for one hour of Managed Cloud Hosting Services as calculated based on the prior month's usage for one hour of Managed Cloud Hosting Services for the affected dedicated cloud hardware, subject to a maximum credit during any calendar month as limited by Section 6 of this Managed Cloud Hosting Services Schedule ("**Standard Service Credit**").

3. DISASTER RECOVERY SERVICE LEVEL TERMS

3.1. Recovery Objective Service Levels. Subject to the limitations provided in Section 6 and provided Client maintains the corresponding Services at the Disaster Recovery Site, Datapipe will ensure that in the event of any Disaster Declaration, the Production Environment can achieve Restoration Success with a maximum RTO of 24 hours (the "**Recovery Time Objective Service Level**") and a maximum RPO of 24 hours (the "**Recovery Point Objective Service Level**"). Client is solely responsible for restoring all other aspects of the Solution, including, but not limited to the database, web and application tiers. For all non-Production environments, only a Recovery Time Objective Service Level is in place. The Recovery Time Objective Service Level for non-Production environment shall be four (4) weeks from the time a total loss of service is declared for the Primary site data center. The determination of a total loss of service at the Primary site data center shall be the sole responsibility of Datapipe, and this determination will be made within seven (7) calendar days of a Disaster Declaration being declared for the Production environment.

3.2. Recovery Objective Service Level Remedy. If Datapipe fails to meet the Recovery Point Objective Service Level or Recovery Time Objective Service Level (collectively the "**Recovery Objective Service Level**"), Client may request in writing a service credit for the Recovery Objective Service Level for that month within ten (10) business days of the associated Disaster Declaration in which Client believes the Recovery Objective Service Level was not met. The Recovery Objective Service Level is not a guarantee of performance, and Client shall only be eligible for a service credit with respect to the Recovery Objective Service Level as defined in this paragraph with respect to this Service Level. Datapipe shall, upon Client's written request to be submitted no later than ten (10) days following the associated Disaster Declaration in which Client believes the Recovery Objective Service Level was not met, credit Client's account with (a) one (1) day of prorated Monthly Recurring Fee directly related to the Production Environment for each additional one (1) hour segment that exceeds the Recovery Time Objective Service Level, and (b) one day of prorated Monthly Recurring Fee for each additional one (1) hour segment that exceeds the Recovery Point Objective Service Level, subject to a maximum credit equal to the applicable Monthly Service Fee directly related to the Production Environment in such calendar month (the "**Recovery Objective Service Level Remedy**"). The Recovery Objective Service Level shall not apply if the failure to meet the Recovery Objective Service Level was as a result of Scheduled Maintenance, Emergency Maintenance, delays due to Client requests or delays due to Client's failure to timely respond to requests from Datapipe during the restoration process.

3.1.3 Recovery Objective Service Level Requirements. Client must comply with the following in order to be eligible for the Recovery Objective Service Level and Recovery Objective Service Level Remedy:

- Complete failover testing to the disaster recovery solution at least once per calendar year.
- Update SEAP documents to specify which individuals are authorized to define/declare a failover event.

4. INCIDENT MANAGEMENT.

4.1. SEVERITY LEVEL DEFINITIONS

"**Severity Level 1**" means the total outage of service or availability of network connectivity, (internet or internal), or mission critical application availability such that Client cannot continue to operate its business due to the severity of the outage.

"**Severity Level 2**" means a material degradation of service or availability of network connectivity (internet or internal), or network device failure, mission critical application availability, or production hardware components such that Client can continue operating its business, but in a negatively impacted and degraded mode.

"**Immediate Support Request**" means a ticket created in the Datapipe ticket system with respect to a Severity Level 1 or Severity Level 2 event, which ticket creation is immediately followed by Client initiating and participating in a telephone conversation with Datapipe support with respect to the contents of that ticket.

4.2. VULNERABILITY LEVEL DEFINITIONS

Datapipe uses the following vendor-supplied classification (currently Nessus but subject to change) as its default risk rating. Datapipe may override the vendor rating to a lower or higher classification per FedRAMP Program Management Office approved processes.

"Critical" means any vulnerability that is categorized as "Critical" within the vulnerability scanner Datapipe uses to scan Client's environment based on the Center for Internet Security (CIS) baselines Datapipe uses per Datapipe's FedRAMP documentation

"High" means any vulnerability that is categorized as "High" within the vulnerability scanner Datapipe uses to scan Client's environment.

"Medium" means any vulnerability that is categorized as "Medium" within the vulnerability scanner Datapipe uses to scan Client's environment.

"Low" means any vulnerability that is categorized as "Low" within the vulnerability scanner Datapipe uses to scan Client's environment.

4.3. COMMUNICATION DURING INCIDENT MANAGEMENT.

Communication is a key element in reporting and resolving service incidents. Unless otherwise noted, Datapipe and Client will communicate via the Client Portal or other identified means during the incident management process.

All communications shall include:

- Support ticket reference number
- Time and date of transaction in question
- Description of incident
- List of actions taken to verify and isolate the problem

4.4. OPENING/REPORTING AN INCIDENT.

Regardless of whether Datapipe or Client reported the incident, Client will be responsible for diligently cooperating with Datapipe in tracking and assisting in addressing the ticket until the incident is resolved.

4.5. WORKING THE INCIDENT.

Once an incident has been reported and a Client support ticket created, Datapipe and Client will work together to address the incident. This process involves:

- An initial response to the incident report
- Status updates
- Escalation
- Communication and resolution times for working the incident

4.5.1. Initial Response.

Upon receiving the notification for an opened incident, Datapipe will respond to Client via the Client Portal. Response intervals vary depending on incident severity, as indicated in Section 4, "Datapipe Performance Standards."

4.5.2. Status Updates.

Update intervals will vary depending on the incident severity as indicated in Section 4. While an Immediate Support Request, Severity Level 1 or Severity Level 2 event is being resolved, Datapipe will send periodic resolution updates.

5. DATAPIPE PERFORMANCE STANDARDS.

Event Type	Description	Datapipe Performance Standard
Severity Level 1 Event	Initial response to event reported by Datapipe's monitoring system or Client	10 minutes
	Datapipe will start to work on the resolution	15 minutes
	Status update	Every 60 minutes
Severity Level 2 Event	Initial response to event reported by the monitoring system or Client	15 minutes
	Datapipe will start to work on the resolution	30 minutes
	Status update	Every 2 hours
Immediate Support Request	Initial response	10 minutes
	Datapipe will start to work on the resolution	10 minutes
	Status update	Every 60 minutes
Scheduled Maintenance	Notification via e-mail	At least 48 hours before maintenance
Datapipe Network Unavailability or Power Unavailability Post Mortem Report	Incident report via e-mail	Within 48 hours of incident
User Adds, Deletes, Modifications	Following the submission of a ticket into the Datapipe ticketing system, and any requested clarifications, Datapipe will complete a user addition, deletion, modification.	Within 48 hours
Taking snapshots	Following the submission of a ticket into the Datapipe ticketing system, and any requested clarifications, Datapipe will complete the snapshot.	Within 48 hours
Audit/Artifact Resolution	Datapipe will provide Client with a proposed schedule of completion of the audit/artifact request. Due to the nature of the audit/artifact request can vary significantly, Datapipe cannot put an exact timeframe to resolution. Datapipe will provide Client with a proposed schedule to complete the request within the specified Performance Standard.	Within 3 business days
Critical Vulnerability (as defined in section 4.2)	Datapipe will remediate any Critical vulnerability as discovered on the monthly vulnerability scans to be performed in	Within 14 calendar days

	accordance with Datapipe's FedRAMP documentation.	
High Vulnerability (as defined in section 4.2)	Datapipe will remediate any High vulnerability as discovered on the monthly vulnerability scans to be performed in accordance with Datapipe's FedRAMP documentation.	Within 30 calendar days
Medium Vulnerability (as defined in section 4.2)	Datapipe will remediate any Medium vulnerability as discovered on the monthly vulnerability scans to be performed in accordance with Datapipe's FedRAMP documentation.	Within 60 calendar days
Low Vulnerability (as defined in section 4.2)	Datapipe will remediate any Low vulnerability as discovered on the monthly vulnerability scans to be performed in accordance with Datapipe's FedRAMP documentation.	Within 90 calendar days

5.1. SERVICE LEVEL CREDITS

If Datapipe fails to meet the service levels described in this Section 4 (the "**Incident Management Service Level**") in any given calendar month, Datapipe will credit Client in accordance with the following schedule (the "**Standard Service Credit for Incident Management**"):

Monthly Cumulative Incident Management Failures	**Service Credit (% of Monthly Recurring Fee for Managed Hosting Services*)**
3-5	3.3%
6-10	6.6%
11-20	10%
More than 20	33.33%

In no event shall any single ticket result in more than one Incident Management Failure, for purposes of calculating Client credits pursuant to this Section 4.1. The Standard Service Credit for Incident Management is Datapipe's sole and exclusive liability and Client's sole and exclusive remedy for any failure of Datapipe to meet the Incident Management Service Level. The total credit available to Client for an Incident Management Failure in any particular calendar month shall in no event exceed the Managed Cloud Hosting Services Monthly Service Fee for the prior month.

5.2. CHANGE CONTROL PROCESSES CREDITS

If Datapipe fails to meet the documented change control processes (the "**Change Control Processes**"), as stated in Datapipe's FedRAMP documentation, in any given calendar month (a "**Change Control Failure**"), Datapipe will credit Client in accordance with the following schedule (the "**Standard Service Credit for Change Control Failure**"):

Monthly Cumulative Change Control Failures	Service Credit (% of Monthly Recurring Fee for Managed Hosting Services*)
1-2	2%
3-5	5%
6-10	15%
11+	30%

*Based on a 30-day billing cycle

6. EXCEPTIONS TO THE CREDIT PROCESS.

Credit shall not be issued due to failures that are, as determined by Datapipe, in its good faith reasonable judgment, the result of:

- Scheduled Maintenance or Emergency Maintenance;
- For vulnerability remediation, no credit shall be issued if Datapipe does not receive sufficient maintenance windows for remediation activities as well as sufficient cooperation from Client due to remediation activities impacting Client's application, as stated in writing from Datapipe to Client during the time period from when the vulnerability was identified to the time when the remediation is due per the defined Performance Standard.
- Written agreement between Datapipe and Client that a change may be implemented without following the Change Control Processes;
- Client-initiated work independently generated by Client or Service interruptions requested by Client;
- Violations of Datapipe's Acceptable Use Policy as may be updated from time to time at http://www.datapipe.com/about-us-legal-acceptable-use-policy.htm;
- Client-required operating system software revisions and hardware/software configurations that are not DGS tested/approved
- Events of Force Majeure;
- DNS issues outside the direct control of DGS
- Patches or Antivirus updates which contain code faults, flaws or other errors attributable to the Third Party vendors that created such code;
- Any suspension of the Managed Cloud Hosting Services pursuant to the terms of the MSA;
- A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack), wherein one or more compromised systems attack a single target, designed to make resources unavailable to its intended users;
- Any actions or inactions of Client, an End User or any Third Party;
- Client's equipment, software or other technology and/or Third Party equipment, software or other technology (other than Third Party equipment within Datapipe's direct control); or
- Manufacturer or safety code-related shutdowns required for safety compliance;
- Failures of individual virtual server instances not attributable to a Covered Cloud Outage.

7. CREDITS.

The total credit available to Client in any particular calendar month shall in no event exceed the fee for one month of Managed Cloud Hosting Services as calculated based on the prior month's usage. Any credits available to Client under this Managed Cloud Hosting Services Schedule will be applied to fees due from Client for the Managed

Cloud Hosting Services, and will not be paid to Client as a refund unless such credit pertains to the last month of service in the Term.

8. SUPPORT.

Client or an End User must report any outages or other issues associated with the Managed Cloud Hosting Services covered under this SLA via the Datapipe ticketing system or by contacting Datapipe Support.