This Managed Cloud for AWS Services Schedule ("**Managed Cloud for AWS Services Schedule**") provides additional terms and conditions under which Client has elected to purchase Managed Cloud for AWS Services from Datapipe as more particularly defined 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 for AWS Services is set forth as Exhibit "A" to this Managed Cloud for AWS Services Schedule.

ADDITIONAL TERMS AND CONDITIONS:

1. DEFINITIONS.

"**AWS**" means Amazon Web Services™

"**AWS Billing Portal**" means the AWS billing portal found at aws.amazon.com or such other URL as AWS may designate in the future.

"**AWS Policies**" means the AWS legal terms and conditions found at http://aws.amazon.com/legal or such other URL as AWS may designate in the future. AWS Policies include the AWS Customer Agreement, AWS Service Terms, Privacy Agreement and the AWS Terms of Use. AWS Policies does not include the AWS AUP, which is included in the definition of AUP, or the AWS Service Level Agreements, which is defined as the AWS SLA. Notwithstanding anything to the contrary, with respect to all references to the AWS Policies in this Managed Cloud for AWS Services Schedule, in the event of a conflict between the AWS Policies and any separately negotiated written terms and conditions entered into between Client and AWS governing the AWS Services, the terms of such agreement between Client and AWS will govern and control.

"**AWS Services**" means the then-current list of web services made available from time to time by AWS and found at http://aws.amazon.com/ or such other URL as AWS may designate in the future.

"**AWS SLA**" means those certain AWS Service Level Agreements associated with the AWS Services selected by the Client, as same may be modified by AWS from time to time and are found at http://aws.amazon.com/serviceterms/ or such other URL as AWS may designate in the future.

"AWS Usage Fee" means the fee incurred by Client during the previous calendar month in connection with its utilization of the AWS Services, including, but not limited to Reserved Instances or other similar services which may be offered by AWS from time to time.

"Managed Cloud for AWS Services Fee" means the fee determined and invoiced monthly in arrears in accordance with the pricing table, and shall be calculated based on the total monthly AWS Usage Fee and Vendor Fees for Managed Cloud for AWS Services, including, but not limited to, any fees in connection with Reserved Instances or other similar services which may be offered by AWS from time to time.

"**Minimum Managed Cloud for AWS Services Fee**" means the minimum Monthly Recurring Fee for Managed Cloud for AWS Services in any given month as set forth in the Order Form, regardless of the actual Managed Cloud for AWS Services usage by Client.

"**Reserved Instances**" means instance capacity reserved by Client as described by AWS at http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts-on-demand-reserved-instances.html, as may be modified by AWS from time to time.

"Vendor Fees for Managed Cloud for AWS Services" means those then-prevailing rates for any independent software vendor service fees related to Client's utilization of those services in conjunction with the AWS Services, which fees shall be borne by Client.

2. SUSPENSION.

Datapipe, in addition to its suspension rights described in the Framework Agreement also reserves the right to immediately suspend the provision of the Services without liability, if (a) Datapipe receives notice from AWS of a violation of the AWS Policies by virtue of Client's use of the AWS Services; (b) AWS terminates the AWS Services for Client or Datapipe; or (c) a payment for AWS Services is overdue by more than 5 days and not being properly disputed pursuant to the payment terms of the Framework Agreement. Client acknowledges that the AWS Policies are legal obligations of both Datapipe and Client, that the AWS Policies are subject to change without

notice, and that violations of the AWS Policies may result in Client's access to the AWS Services being suspended as a result of the actions of Client or Third Parties. Datapipe will make commercially reasonable efforts, circumstances permitting, to provide Client with written notice of any such suspension or termination. Datapipe shall have no liability for any damage, liabilities, losses (including any loss of data or profits) or any other consequences that Client may incur as a result of any such suspension, provided the basis of such suspension is not solely as a result of the actions or inactions of Datapipe.

3. PAYMENT AND PAYMENT TERMS – FEES.

In addition to the terms provided in the Framework Agreement, all fees for AWS Services, including but not limited to, the Minimum Managed Cloud for AWS Services Fee and Vendor Fees for Managed Cloud for AWS Services, shall be billed to Client via invoice in arrears for the previous calendar month and shall be due as of the due date specified on the invoice.

4. DISCLAIMER OF ACTIONS CAUSED BY AND/OR UNDER THE CONTROL OF THIRD PARTIES.

In addition to the terms provided in the Framework Agreement, Datapipe does not guarantee the integrity of data stored or transmitted via the AWS Services. Datapipe shall not be liable for the inadvertent disclosure of, or corruption or erasure of data transmitted or received or stored via the AWS Services.

5. LIMITATION OF LIABILITY.

NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, INCIDENTAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL DAMAGES 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.

UNLESS OTHERWISE SPECIFIED IN THE CALL OFF AGREEMENT, THE MAXIMUM CUMULATIVE LIABILITY OF EITHER PARTY OR ITS SUPPLIERS, CONTRACTORS AND SUBCONTRACTORS ARISING OUT OF OR RELATING TO THE SERVICES 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 THE CALL OFF AGREEMENT DURING THE TWELVE MONTH PERIOD PRIOR TO THE EVENT GIVING RISE TO SUCH CLAIM.

THE ABOVE 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 ABOVE LIMITATION OF LIABILITY SHALL NOT APPLY TO EITHER PARTY'S CONFIDENTIALITY AND INDEMNIFICATION OBLIGATIONS UNDER THE CALL OFF AGREEMENT. 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 TOTAL AMOUNT PAID OR TO BE PAID BY CLIENT TO DATAPIPE UNDER THE CALL OFF AGREEMENT DURING THE THREE (3) YEAR PERIOD PRIOR TO THE EVENT GIVING RISE TO SUCH CLAIM;

DESPITE ANY LIMITATIONS SET FORTH IN THIS SECTION, CLIENT SHALL BE LIABLE FOR ALL SUMS DUE OR PAYABLE UNDER THE CALL OFF AGREEMENT FOR THE SERVICSE PROVIDED, REGARDLESS OF AMOUNT, TOGETHER WITH ANY ADDITIONAL FEES, ATTORNEY FEES AND/OR COSTS THAT MAY BE INCURRED BY DATAPIPE.

6. AWS MASTER CREDENTIALS.

6.1. CLIENT-PROVISIONED AWS ACCOUNTS.

If Client has an existing AWS account to be used in connection with the Services ("**Existing Account**"), the Existing Account shall remain in the sole custody of Client during the Term, however Client shall grant Datapipe cross-account access with an administrative role ("**Delegated Access**") promptly upon execution of this Managed Cloud for AWS Services Schedule. Furthermore, Client shall promptly accept a Datapipe-initiated consolidated billing request to ensure AWS usage charges are received under Datapipe's AWS master account ("**Consolidated Billing**") and subsequently invoiced to Client together with any additional charges detailed under the Framework Agreement.

6.2. DATAPIPE-PROVISIONED AWS ACCOUNTS.

If an AWS account is provisioned by Datapipe for Client use in connection with the Services ("**New Account**"), Datapipe shall issue root credentials to Client promptly following account creation, such New Account shall remain in the sole custody of Client during the Term, and Datapipe shall be granted Delegated Access. Encrypted root credentials are emailed to Client via the Client Portal, and thereafter unencrypted by Client by utilizing the Client Portal. Upon receipt of the New Account root credentials, Client must modify the New Account email address and password and agrees to not share this information with Datapipe. Under Datapipe's Delegated Access model, Client maintains its root credentials at all times. Accordingly, Datapipe shall not be responsible for the security of the New Account root credentials once initially distributed to Client. Each New Account shall be configured to allow for Consolidated Billing, and all usage charges shall be invoiced to Client together with any additional charges detailed under the Framework Agreement.

Client at all times maintains ownership of Client Content stored on AWS systems. Upon termination of the Managed Cloud for AWS Services, Client may unconsolidate AWS billing to the extent applicable.

6.3. LEGACY AWS ACCOUNTS.

For AWS accounts managed by Datapipe prior to its implementation of Delegated Access ("**Legacy Accounts**"), Datapipe shall upon termination of this Managed Cloud for AWS Services Schedule: (1) promptly update any Client root credentials to a Client-supplied email address; (2) securely disseminate the root credential password to Client via a mutually agreed method, such as a telephone call; and (3) promptly remove any Datapipe-controlled AWS Identity and Access Management ("**IAM**") accounts, groups, and roles.

6.4. ACCOUNT GOVERNANCE.

Client is advised to enable Multi-Factor Authentication ("**MFA**") on its AWS root account, create an IAM account for management, and leverage root credentials solely for emergency access. Client acknowledges that it has read and understands the AWS security processes outlined at:

http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf.

Delegated Access and Consolidated Billing shall not be modified by either Party during the Term. In the event Client does not provide Datapipe with or removes Delegated Access, Datapipe shall not be responsible for delivering any Services which require Datapipe access in order to provide those Services. Any usage rates visible via the AWS Billing Portal do not apply to Client, as this pricing does not represent generally available retail AWS pricing, but rather specially negotiated Datapipe rates. As such, Datapipe will not provide support for any billing issues, nor will Datapipe address any disputes related to billing rates reflected in Client's AWS Billing Portal. For the avoidance of doubt, Client shall always remit payment in accordance with Datapipe's billing rates described in this Managed Cloud for AWS Services Schedule.

7. AMAZON TERMS.

In addition to its obligations under the Framework Agreement, Client agrees to comply with the AWS Policies as though Client was a direct customer of AWS. No free trials or other pricing promotions that may be offered from time to time by AWS shall apply to any fees specified under the Framework Agreement and this Managed Cloud for AWS Services Schedule unless same is confirmed in writing by Datapipe.

8. THIRD PARTY PARTNERS

Datapipe leverages certain Third Party partners to provide value added services in connection with reporting on AWS performance, cost, security status and optimization ("**Datapipe AWS Partners**"). In order to extend these services, Datapipe provides read-only IAM access keys to the Datapipe AWS Partners. Data collected from the AWS platform by such keys shall be used exclusively to deliver the Managed Cloud for AWS Services. While Datapipe AWS Partners do not have any direct access to data stored within the AWS platform, they will have access to certain meta-data including, but not limited to tagging information, security groups, and instance names ("**Partner Metadata**"). Datapipe and the Datapipe AWS Partners shall protect Partner Metadata from unauthorized disclosure. Client consents to granting Datapipe AWS Partners read-only access to all managed AWS accounts and agrees that (i) such access shall not constitute a transfer of PII; (ii) Partner Metadata shall not constitute Confidential Information; and (iii) Datapipe AWS Partners shall not be considered Datapipe subcontractors.

[THE BALANCE OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

1. AWS BEST PRACTICES.

Client agrees to adopt the following best practices in connection with its use of AWS Services:

- Client shall enable AWS CloudTrail services (may be subject to a fee).
- Client shall allow for and maintain a Datapipe AWS IAM role for administration.

2. INCIDENT MANAGEMENT.

2.1. MANAGED CLOUD FOR AWS SEVERITY LEVEL DEFINITIONS

"**Severity Level 1**" means the total lack of availability of the AWS Services such that Client cannot continue its business due to the severity of the outage.

"**Severity Level 2**" means a material degradation of availability of the AWS Services such that Client can continue operating its business, but in a negatively impacted and degraded mode or any other support request not meeting the definition of Severity Level 1 or Immediate Support Request.

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

2.2. 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 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

2.3. OPENING/REPORTING AN INCIDENT.

Datapipe will send Client a notification in accordance with the Client's Solution Escalation Action Plan (SEAP), advising that the AWS Services are unavailable. Regardless of whether Datapipe or Client reported the incident, Client cooperation and responsiveness is often required in order for Datapipe to effectively resolve incidents. As such, Client agrees that both Parties will be responsible for tracking the ticket for the incident, and Client shall assist Datapipe as may be reasonably requested until such time as the incident is resolved.

2.4. WORKING THE INCIDENT.

Once an incident has been reported (either by Client or Datapipe) and a 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

2.4.1. 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 3, "Datapipe Performance Standards."

2.4.2. Status Updates.

Update intervals will vary depending on the incident severity as indicated in Section 3. While an Immediate Support Request, Severity Level 1 Event, or Severity Level 2 Event is being resolved, Datapipe will send periodic resolution updates.

3. DATAPIPE PERFORMANCE STANDARDS.

Datapipe shall provide responses and updates to Support Requests as follows (the "**Incident Management Service Level**"):

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	10 minutes
	Status update	Every 60 minutes
Severity Level 2 Event	Initial response to event reported by the monitoring system or Client	10 minutes
	Datapipe will start to work on the resolution	30 minutes
	Status update	Every 2 hours
Immediate Support Request	Initial response	5 minutes
	Datapipe will start to work on the resolution	5 minutes
	Status update	Every 60 minutes
AWS-initiated scheduled maintenance or outage	Notification via e-mail	No more than 24 hours from AWS notification to Datapipe
AWS unplanned outage	Incident report via e-mail	Within 48 hours of incident

3.1. CREDITS.

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

Monthly Cumulative Incident Management Failures	Service Credits (% of Monthly Managed Cloud for AWS Services Fee)
3-5	5%
6-10	15%
11+	50%

**Based on a 30-day billing cycle.*

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 3.1.

4. AWS SLA

Client's sole and exclusive remedy in connection with its use of and/or any failure of the AWS Services under this Managed Cloud for AWS Services Schedule shall be pursuant to and as limited by the AWS SLA. Upon written request, Datapipe will assist Client as may be reasonably required in asserting an SLA credit claim with AWS.

5. EXCEPTIONS TO THE CREDIT PROCESS:

A credit will not be issued due to:

- The acts or omissions of Client, its employees, agents, third-party contractors or vendors, or anyone gaining access to the Services at the request of Client;
- A Force Majeure Event; or
- Any suspension of Services pursuant to the Framework Agreement.

6. LIMITED REMEDY AND MAXIMUM CREDITS AVAILABLE.

The sole and exclusive remedy for an Incident Management Failure shall be the receipt of service credits as provided in Section 3.1 above. In addition, the total aggregate credit available to Client in any calendar month for an Incident Management Failure shall not exceed the Managed Cloud for AWS Services Fee for such calendar month.

[END OF EXHIBIT A]