CARAHSOFT RIDER

Please review and approve the Carahsoft Rider ("Rider").

The Carahsoft Rider contains mandatory terms for all public sector contracts (i.e. GSA, SEWP, NASPO, Open Market orders, etc.). By signing this document, you agree to the incorporation of these terms into all purchase orders placed by Carahsoft on behalf of Public Sector Entities who buy through Carahsoft and/or Carahsoft's prime contractors.

These terms will take precedence over any conflicting terms in your Commercial Supplier Agreement (i.e. End User License Agreement, EULA, Master Service Agreement, or similar document) with Public Sector Entities. These terms will also take precedence over any conflicting terms contained within the Manufacturer Agreement (i.e. Channel Agreement, Distributor Agreement, Aggregator Agreement, Reseller Agreement, VAD Agreement, VAR agreement, or similar document) you may have in place with Carahsoft Technology Corp., if applicable. Lastly, these terms will take precedence over any conflicting terms in any Statement of Work (or similar document) you may have in place with Carahsoft Technology Corp.

A Public Sector Entity ("Licensee") is defined as one of the following:

- A member of the U.S. government's legislative, judicial or executive branches. This includes the department of defense, civilian agencies, intelligence agencies, independent agencies, special inspector general offices, and quasi-official agencies (i.e. National Gallery of Art, National Park Foundation, etc.).
- U.S. state or local government entity. This includes all applicable state agencies, counties, cities, municipalities, and similar entities within a state, the District of Columbia, or one of the territories of the United States.
- An Academic Institution is defined as an accredited institution, and must be organized and operated for educational purposes. The institution must receive funding (partial or full) from a federal, state, or local agency, and must meet one of the following criteria:
    - Public or private elementary, secondary, vocational school, correspondence school, junior college, university, post-graduate school such as a medical college, law school, or business school, management school board, school for disabled, scientific, research, or technical institutions accredited by U.S. Department of Education and State Board of Education, or, by associations recognized by U.S. Department of Education, including the district, regional, and State Administrative offices.
    - Administrative Offices or Board of Education for academic institutions as defined as:
        - A district, regional or state administrative office of public educational institution
        - Administrative entities organized and operated exclusively for private academic institutions
        - Other state or local government entities whose activities consist of administrative support or services for the advancement of public academic institutions.
    - Full-time or part-time faculty, staff, or, matriculated students in good academic standing at an accredited academic institution. Libraries associated with an accredited academic institution
    - Hospitals and teaching hospitals that are wholly owned and operated by an academic institution.
    - Higher Education Research laboratories that are associated with an academic institution, recognized by the U.S. Department of Education, and teach students as part of their research mission.

Manufacturer Name: Rackspace

Signature: R. Rosenburg

Print Name: Rick Rosenburg

Title: Vice President and General Manager

Date: April 29, 2020

By signing above, I have read and agreed with all info regarding the RIDER.

Carahsoft Rider for Public Sector Agencies

1. Applicability. To the extent the terms and conditions in the Manufacturer's Agreements or Commercial Supplier Agreement are inconsistent with applicable public sector law (i.e. *See* FAR 12.212(a), which provides that Public Sector Entities shall accept commercial computer software subject to the supplier's established commercial license and other terms, except to the extent such terms are contrary to federal law), they shall be deemed deleted and unenforceable under any resultant orders or contracts with Carahsoft.

2. Termination. If a Public Sector Entity cancels or terminates its corresponding order with Carahsoft, Carahsoft's reseller partner or a higher tier prime or subcontractor, as applicable, then Carahsoft will have the right to cancel the related order with Manufacturer in the same manner as the cancellation or termination is presented by the Public Sector Entity. In such a cancellation event, Carahsoft will notify Manufacturer as soon as reasonably possible on the specific details of the order cancellation.

- Carahsoft may request cancellation or termination of the Commercial Supplier Agreement and applicable Public Sector Entity purchase order on behalf of the Manufacturer if such remedy is granted to it after conclusion of the Contracts Disputes Act dispute resolutions (or applicable dispute resolutions process) or if such remedy is otherwise ordered by applicable jurisdictional court.

3. Customer Indemnities. All Commercial Supplier Agreement clauses referencing Customer Indemnities are hereby deemed to be deleted to the extent they are contrary to federal law.

4. Contractor Indemnities. All Commercial Supplier Agreement clauses that (1) violate applicable judicial department's right (i.e. 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.

5. Travel and Expenses. Out-of-pocket expenses identified in a quote, statement of work, professional services agreement (or similar agreement) must be submitted for payment no more than sixty (60) days after completion of Services or such payment may be denied. Manufacturer shall ensure that travel expenses are incurred in accordance with the limitations set forth in FAR 31.205-46. Manufacturer will provide budgetary estimates for all travel and expense fees on its quotes (or Statement of Works/Professional Service Agreements) to Carahsoft.

6. Limitation of Liability: Subject to the following:

- Public Sector Entity shall not be liable for any indirect, incidental, special, or consequential damages, or any loss of profits, revenue, data, or data use. Further, Public Sector Entity shall not be liable for punitive damages except to the extent this limitation is prohibited by applicable law. This clause shall not impair the Public Sector Entity's right to recover for fraud or crimes under applicable fraud statute, such as the False Claims Act, 31 U.S.C. §§ 3729-3733.

7. 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.

MASTER SERVICES AGREEMENT

This Master Services Agreement ("**MSA**" or "**GSA**") is between Rackspace, and the customer ordering the Services ("**Customer**", "**Client**", or "**you**") each a "**party**" and together the "**parties**".

1. DEFINED TERMS. The defined terms in Schedule 1 shall be applicable to the Agreement.

2. SERVICES.

2.1. Rackspace shall provide the Services in accordance with the Agreement and all laws applicable to Rackspace. Rackspace's obligation to provide Services is contingent on verification that Customer at all times satisfies Rackspace's credit approval criteria. Rackspace shall have no obligation to provide Services for Customer Configurations which do not meet the Rackspace Configuration Requirements. Rackspace shall provide support only to those individuals designated by Customer in the customer portal and is not required to provide any support directly to Customer's end users. Customer remains liable for the acts and omissions of Customer's end users.

2.2. Customer may use the Services for commercial purposes only and may not use the Services in any situation where failure or fault of the Services or the Customer Configuration could lead to death or serious bodily injury of any person or physical or environmental damage.

3. CUSTOMER OBLIGATIONS.

3.1. For Services where Rackspace's access to the Customer Configuration is necessary to perform the Services and/or to calculate any utility Fees based on usage of the Customer Configuration (other than in respect of Hosted Systems), Customer shall grant Rackspace a reasonable method to access the Customer Configuration. Customer shall cooperate with Rackspace's reasonable investigation of outages, security problems, and any suspected breach of the Agreement. Customer is responsible for keeping its account permissions, billing, and other account information up to date. Customer agrees that its use of any Hosted System shall comply with the AUP. Customer is responsible for determining the suitability of the Services and Customer's compliance with any applicable laws, including export laws and data privacy laws.

3.2. Customer is responsible for ensuring the integrity and security of Customer Data, and for regularly backing up and validating the integrity of backups of Customer Data on an environment separate from the Customer Configuration. Rackspace shall only back up data to the extent stated on a Service Order.

4. SECURITY. Rackspace shall provide the Services in accordance with the Security and Privacy Practices and any additional security specifications identified in the Service Order or Product Terms. Customer shall use reasonable security measures and precautions in connection with its use of the Services, including appropriately securing and encrypting in transit and at rest Sensitive Data stored on or transmitted using the Customer Configuration; and shall take appropriate measures to otherwise prevent access to Sensitive Data by Rackspace where Rackspace's access to the premises, systems or networks managed or operated by Customer may result in its exposure. Customer Data is, and at all times shall remain, Customer's exclusive property. Rackspace shall not use or disclose Customer Data except as materially required to perform the Services or as required by law.

5. INTELLECTUAL PROPERTY.

5.1. Pre-Existing. Each party shall retain exclusive ownership of Intellectual Property created, authored, or invented by it prior to the commencement of the Services. If Customer provides Rackspace with its Customer IP, Customer hereby grants to Rackspace, during the term of the applicable Service Order, a limited, worldwide, non-exclusive, non-transferable, royalty-free, right and license (with right of sub-license where required to

perform the Services) to use the Customer IP solely for the purpose of providing the Services. Customer represents and warrants that Customer has all rights in the Customer IP necessary to grant this license, and that Rackspace's use of Customer IP shall not infringe on the Intellectual Property rights of any third party.

5.2. Proprietary Rights; Deliverables. Unless otherwise specifically stated in the applicable Service Order, and excluding any Customer IP, as between the parties, Rackspace shall own all Intellectual Property created in providing the Services or contained in the Deliverables. Subject to Customer's compliance with the terms of the Agreement, Rackspace grants to Customer a limited, worldwide, non-exclusive, non-transferable, royalty-free right and license (without the right to sublicense) to use:

(A) any Intellectual Property provided by Rackspace to Customer as part of the Services (excluding Third Party Software, Open Source Software, and Deliverables) solely for Customer's internal use and as necessary for Customer to enjoy the benefit of the Services during the term of the applicable Service Order; and

(B) any Intellectual Property provided by Rackspace to Customer as part of the Deliverables (excluding Third Party Software and Open Source Software) solely for Customer's internal use in perpetuity.

5.3. Open Source. In the event Rackspace distributes or otherwise provides for Customer use any Open Source Software to Customer as part of the Services and/or Deliverables then such Open Source Software is subject to the terms of the applicable open source license. To the extent there is a conflict between this MSA and the terms of the applicable open source license, the open source license shall control.

5.4. Third Party Software. Rackspace may provide Third Party Software for Customer's use as part of the Services and/or Deliverables or to assist the delivery of the Services. Unless otherwise permitted by the terms of the applicable license, Customer may not: (i) assign, grant, or transfer any interest in Third Party Services or Third Party Software to another individual or entity; (ii) reverse engineer, decompile, copy, or modify the Third Party Software; (iii) modify or obscure any copyright, trademark or other proprietary rights notices that are contained in or on the Third Party Software; or (iv) exercise any of the reserved Intellectual Property rights provided under the laws governing the Agreement. Customer may only use Third Party Services and Third Party Software provided for its use as part of the Services (identified on the Service Order) on that portion of the Customer Configuration for which it was originally provided, subject to any additional restrictions identified in the Product Terms or Service Order. Customer shall not be permitted to access any Third Party Software which Rackspace installs solely to assist Rackspace's delivery of the Services. Upon termination of the Service Order, Customer shall permit removal of any Third Party Software installed by Rackspace or its Representatives on the Customer Configuration. Rackspace makes no representation or warranty regarding Third Party Services or Third Party Software except that Rackspace has the right to use or provide the Third Party Services or Third Party Software.

5.5. Customer Provided Licenses. If Customer uses any non-Rackspace provided software on the Customer Configuration, Customer represents and warrants to Rackspace that Customer has the legal right to use the software. If Rackspace has agreed to install, patch, or otherwise manage software in reliance on Customer's license with a vendor then Customer represents and warrants that it has a written license agreement with the vendor that permits Rackspace to perform these activities. Rackspace's obligation to install, patch, or otherwise manage Customer provided software is strictly contingent on Customer maintaining original software vendor support or similar authorized support that provides a services request escalation path, access to patching, and software upgrades, as applicable. On Rackspace's request, Customer shall certify in writing that Customer is in compliance with the requirements of this section and any other software license restrictions that are part of the Agreement, and shall provide evidence of Customer's compliance as Rackspace may reasonably request. If Customer fails to provide the required evidence of licensing to Rackspace, and continues to use the software, Rackspace may: (i) charge Customer its standard fee for the use of the software in reliance on Rackspace's licensing agreement with the vendor until such time as the required evidence is provided, or (ii) suspend or terminate the applicable Services.

5.6. Infringement. If the delivery of the Services or provision of Deliverables infringes the Intellectual Property of a third party and Rackspace determines that it is not reasonably or commercially practicable to obtain the

right to use the infringing element, or modify the Services or Deliverables such that they do not infringe, then Rackspace may terminate the infringing Services and/or Deliverables on 90 days' notice and shall not have any liability on account of such termination except to refund amounts paid for unused Services (prorated as to portions of the Services and/or Deliverables deemed infringing).

6. FEES.

6.1. Fees. Customer shall pay the Fees due within 30 days from the invoice date. If Customer has arranged for payment by credit card or automated clearing house, Rackspace may charge Customer's card or account on or after the invoice date. If Customer's undisputed payment is overdue by 15 days or more, Rackspace may immediately suspend the associated Services and any other services Customer receives from Rackspace on written notice. Rackspace shall undertake collection efforts prior to suspension. Invoices that are not disputed within 120 days of the invoice date are conclusively deemed to be accepted as accurate by Customer. Customer shall pay the Fees in the currency identified on the Service Order, and, except as expressly permitted in section 6.3, without setoff, counterclaim, deduction, or withholding. Rackspace may charge interest on overdue amounts at the greater of 1.5% per month or the maximum legal rate, and may charge Customer for any cost or expense arising out of Rackspace's collection efforts.

6.2. Fee Increases.

(A) Rackspace Fee Increases. Unless stated to the contrary in the Agreement and subject to sections 6.2(B) and 6.2(C), there will be no Fee increases during the Initial Term or any Renewal Term. However, Rackspace may increase Fees following expiration of the Initial Term, any Renewal Term, or during any Auto-Renewal Term on giving at least 90 days advance written notice.

(B) Third Party Fee Increases. In the event of a Third Party Fee Increase, Rackspace may increase Customer's Fees by the same percentage amount on giving at least 90 days advance written notice.

(C) Holdover Rates. If Customer continues to use any Services following termination of the Agreement or applicable Service Order, Customer shall be responsible for payment of such Services at Rackspace's then-current market rates.

6.3. Taxes. All amounts due to Rackspace under the Agreement are exclusive of Tax. Customer shall pay Rackspace any Tax that is due or provide Rackspace with satisfactory evidence of Customer's exemption from the Tax in advance of invoicing. Customer shall provide Rackspace with accurate and adequate documentation sufficient to permit Rackspace to determine if any Tax is due. All payments to Rackspace shall be made without any withholding or deduction for any taxes except for Local Withholding Taxes. Customer agrees to timely provide Rackspace with accurate factual information and documentation of Customer's payment of any such Local Withholding Taxes. Rackspace shall remit such cost to Customer in the form of a credit on Customer's outstanding account balance following receipt of sufficient evidence of payment of any such Local Withholding Taxes.

6.4. Reimbursement for Expenses. Unless otherwise agreed in the Service Order, if any of the Services are performed at Customer's premises, Customer agrees to reimburse Rackspace for the actual substantiated out-of-pocket expenses of its Representatives.

7. DISCLAIMERS.

7.1. Rackspace makes no commitment to provide any services other than the Services stated in the Service Order. Rackspace is not responsible to Customer or any third party for unauthorized access to Customer Data or for unauthorized use of the Services that is not solely caused by Rackspace's failure to meet its security obligations in section 4. To the maximum extent permitted by law, Rackspace disclaims all responsibility for any situation where the security, availability, or stability of the Services is compromised by: (i) actions of Customer or any end user; (ii) software provided by Customer, or (iii) any actions taken by Rackspace which are requested by Customer and not based on the advice or recommendation of Rackspace. Rackspace shall not be liable for

any failure to comply with its obligations in the Agreement to the extent that such failure arises from a failure of Customer to comply with its obligations under the Agreement.

7.2. Rackspace may designate certain Services as Unsupported Services. Rackspace makes no representation or warranty with respect to Unsupported Services except that it shall use reasonable efforts as may be expected of technicians having generalized knowledge and training in information technology systems. Rackspace shall not be liable to Customer for any loss or damage arising from the provision of Unsupported Services and SLA(s) shall not apply to Unsupported Services, or any other aspect of the Customer Configuration that is adversely affected by Unsupported Services. If Customer uses any Test Services, then Customer's use of those Test Services is subject to the Test Terms. At Customer's request, Rackspace may provide services that are not required by the Agreement. Any such services shall be provided AS-IS with no warranty whatsoever.

7.3. Rackspace and its Representatives disclaim any and all warranties not expressly stated in the Agreement to the maximum extent permitted by law including implied warranties such as merchantability, satisfactory quality, fitness for a particular purpose, and non-infringement.

7.4. Except as expressly provided herein, Rackspace makes no representation or warranty whatsoever regarding Open Source Software or with regard to any third party products or services which Rackspace may recommend for Customer's consideration. TPS Agreements are independent and separate from the Agreement, and Rackspace is not a party to and is not responsible for the performance of any TPS Agreements.

8. TERM AND TERMINATION.

8.1. Term. This MSA shall continue until terminated in accordance with its terms. Service Orders for Recurring Services shall be subject to the Auto Renewal Term unless: (i) otherwise stated in the Agreement, (ii) the parties enter into an agreement for a Renewal Term, or (iii) either party provides the other with written notice of termination at least 90 days prior to the expiration of the then current term.

8.2. Termination for Convenience. For Recurring Services, unless otherwise stated in the Agreement, Customer may terminate all or part of any Service Order for convenience at any time by giving Rackspace at least 90 days advance written notice; subject to an early termination fee equal to the monthly recurring Fee times the number of months remaining in the then current term of the Service Order for the Services that have been terminated.

8.3. Termination for Cause.

(A) Either party may immediately terminate the MSA and/or the affected Service Order(s) for cause on written notice if the other party materially breaches the Agreement and, where the breach is remediable, does not remedy the breach within 30 days of the non-breaching party's written notice describing the breach.

(B) Rackspace may immediately terminate the Agreement and/or the applicable Service Order(s) for breach on written notice if, following suspension of Customer's Services for non-payment, payment of any invoiced undisputed amount remains overdue for a further ten days.

(C) Subject to applicable law, either party may immediately terminate the MSA and any Service Order(s) on written notice if the other party enters into compulsory or voluntary liquidation, or ceases for any reason to carry on business, or takes or suffers any similar action which the other party reasonably believes means that it may be unable to pay its debts.

(D) Notwithstanding anything to the contrary in the Agreement, the Fees for the Services through the conclusion of all Service Orders shall become due immediately in the event Rackspace terminates the MSA in accordance with this section 8.3.

8.4. Delayed Termination. If, following Customer's notice of termination, Rackspace permits Customer to cancel or delay the scheduled termination date, Customer is obligated to re-notify Rackspace in writing at least 90 days prior to any rescheduled termination date.

9. CONFIDENTIAL INFORMATION. Each party agrees not to use the other's Confidential Information except in connection with the performance or use of the Services, the exercise of its legal rights under the Agreement, or as required by law; and shall use reasonable care to protect Confidential Information from unauthorized disclosure. Each party agrees not to disclose the other's Confidential Information to any third party except: (i) to its Representatives, provided that such Representatives agree to confidentiality measures that are at least as stringent as those stated in this MSA; (ii) as required by law; (iii) in response to a subpoena or court order or other compulsory legal process, provided that the party subject to such process shall give the other written notice of at least seven days prior to disclosing Confidential Information unless the law forbids such notice; or (iv) with the other party's consent.

10. LIMITATIONS ON DAMAGES.

10.1. Notwithstanding anything in the Agreement to the contrary:

(A) Rackspace's liability arising from: (i) death or personal injury caused by negligence; (ii) fraudulent misrepresentation; or (iii) any other loss or damages for which such limitation is expressly prohibited by applicable law, shall be unlimited.

(B) Subject to section 10.1(A), the maximum aggregate monetary liability of Rackspace and any of its Representatives in connection with the Services or the Agreement under any theory of law shall not exceed the actual damages incurred up to the greater of: (i) an amount equal to six times the Fees payable by Customer for the Services that are the subject of the claim in the first month in which Fees are charged under the Agreement, or (ii) the total amount paid by Customer to Rackspace for the Services that are the subject of the claim in the 12 months immediately preceding the event(s) that first gave rise to the claim.

10.2. Neither party (nor any of its Representatives) is liable to the other party for any indirect, special, incidental, exemplary, or consequential loss or damages of any kind. Neither party is liable for any loss that could have been avoided by the damaged party's use of reasonable diligence, even if the party responsible for the damages has been advised or should be aware of the possibility of such damages. In no event shall either party be liable to the other for any punitive damages; or for any loss of profits, data, revenue, business opportunities, customers, contracts, goodwill, or reputation.

10.3. As an essential part of the Agreement, the liquidated damages payable under the SLA(s) shall be the credits stated in any applicable SLA(s) which are Customer's sole and exclusive remedy for Rackspace's failure to meet those guarantees for which credits are provided; and the parties agree that the credits are not a penalty, are fair and reasonable and represent a reasonable estimate of loss that may reasonably be anticipated from any breach. The maximum credit(s) for failures to meet any applicable SLA(s) for any calendar month shall not exceed 100% of the then current monthly recurring Fee for the Services. Customer is not entitled to a credit if Customer is in breach of the Agreement at the time of the occurrence of the event giving rise to the credit, until such time as Customer has remedied the breach. No credit shall be due if the credit would not have accrued but for Customer's action or omission.

11. INDEMNIFICATION.

11.1. If Rackspace, its Affiliates, or any of its or their respective Representatives (collectively, the "**Indemnitees**" or "**Indemnified Parties**") are faced with a claim by a third party arising out of: Customer's breach of TPS Agreement, end user agreement, AUP, security obligation or section 5.5, then Customer shall hold Rackspace harmless and pay the cost of defending the claim (including reasonable legal and professional fees and expenses) and any damages, losses, fine, or other penalty that is imposed on or incurred by the Indemnitees

as a result of the claim. Customer's obligations under this section include claims arising out of the acts or omissions of Customer's employees, agents, end users, any other person to whom Customer has given access to the Customer Configuration, and any person who gains access to the Customer Configuration as a result of Customer's failure to use reasonable security precautions, even if the acts or omissions of such persons were not authorized by Customer.

11.2. If Rackspace receives notice of a claim that is covered by this section 11, Rackspace shall give Customer prompt written notice thereof. Rackspace shall be allowed to conduct the defense of the matter, including choosing legal counsel to defend the claim, provided that the choice is reasonable and is communicated to Customer. Customer shall comply with Rackspace's reasonable requests for assistance and cooperation in the defense of the claim. Rackspace may not settle the claim without Customer's consent, which may not be unreasonably withheld, delayed or conditioned. Customer shall pay costs and expenses due under this section 11 as Rackspace incurs them.

12. NOTICES. Customer routine communications to Rackspace regarding the Services should be sent to Customer's account team using the customer portal. To give a notice regarding termination of the Agreement for breach, indemnification, or other legal matter, Customer shall send it by electronic mail and overnight postal service to:

legalnotice@rackspace.com
General Counsel
Rackspace US, Inc.
One Fanatical Place, City of Windcrest
San Antonio, Texas 78218

Rackspace's routine communications regarding the Services and legal notices shall be posted on the customer portal or sent by email or post to the individual(s) Customer designates as contact(s) on Customer's account. Notices are deemed received as of the time posted or delivered, or if that time does not fall within a Business Day, as of the beginning of the first Business Day following the time posted or delivered. For purposes of counting days for notice periods, the Business Day on which the notice is deemed received counts as the first day. Notices shall be given in the English language.

13. PUBLICITY, USE OF MARKS. Customer agrees that Rackspace may publicly disclose that it is providing Services to Customer and may use Customer's name and logo to identify Customer in promotional materials, including press releases. Customer may not issue any press release or publicity regarding the Agreement, use the Rackspace name or logo or other identifying indicia, or publicly disclose that it is using the Services without Rackspace's prior written consent.

14. ASSIGNMENT/SUBCONTRACTORS. Neither party may assign the Agreement or any Service Orders without the prior written consent of the other party, except to an Affiliate or successor as part of a corporate reorganization or a sale of some or all of its business, provided the assigning party notifies the other party of such change of control. Rackspace may use its Affiliates or subcontractors to perform all or any part of the Services, but Rackspace remains responsible under the Agreement for work performed by its Affiliates and subcontractors to the same extent as if Rackspace performed the Services itself.

15. FORCE MAJEURE. Neither party shall be liable or be in breach of the Agreement (excluding in relation to the Customer's payment obligations) if the failure to perform the obligation is due to an event beyond its control, including significant failure of a part of the power grid, failure of the Internet, natural disaster or weather event, fire, acts or orders of government, war, riot, insurrection, epidemic, strikes or labor action, or terrorism.

16. GOVERNING LAW.

16.1. The Agreement shall be governed by the applicable governing law determined as set out below by reference to the Rackspace contracting entity (and, where applicable, Customer's primary address as stated in the Service Order), exclusive of any choice of law principle that would require the application of the law

of a different jurisdiction; and each party unconditionally and irrevocably submits to (i) the exclusive jurisdiction of the courts of the applicable jurisdiction, or (ii) binding arbitration, as set out below:

CONTRACTING ENTITY	GOVERNING LAW	ARBITRATION OR JURISDICTION
Rackspace Limited	England and Wales	Courts of England
Datapipe Europe Limited		
Rackspace International GmbH, unless stated otherwise in this table		
Rackspace Asia Limited	Hong Kong Special Administrative Region of the People's Republic of China	Courts of Hong Kong Special Administrative Region of the People's Republic of China
Datapipe Asia Limited		
Rackspace International GmbH, only if Customer's primary address is in Hong Kong		
Rackspace Hosting Australia PTY LTD	New South Wales, Australia	Courts of New South Wales, Australia
Rackspace International GmbH, only if Customer's primary address is in Australia		
Datapipe Singapore Pte. Ltd.	Singapore	Courts of Singapore
Rackspace US, Inc.	State of Texas, USA and the federal laws of the USA	Arbitration
Datapipe, Inc.		
Rackspace Government Solutions, Inc.		
Rackspace International GmbH, only if the Customer's primary address is in the United States, Latin America (including the Caribbean) or Canada		
RelationEdge, LLC		
TriCore Solutions, LLC		
Onica Group, LLC		
Onica Technologies Canada Inc.		

Where stated to be subject to arbitration in the table above, any dispute or claim relating to or arising out of the Agreement shall be submitted to binding arbitration. The arbitration shall be conducted in the state and county (or equivalent geographic location) of the non-asserting party's principal business offices in accordance with the Commercial Rules of the AAA in effect at the time the dispute or claim arose. The arbitration shall be conducted by one arbitrator from AAA or a comparable arbitration service. The arbitrator shall issue a reasoned award with findings of fact and conclusions of law. Either party may bring an action in any court of competent

jurisdiction to compel arbitration under the Agreement, or to enforce an arbitration award. Neither party nor an arbitrator may disclose the existence, content, or results of any arbitration under the Agreement without the prior written consent of both parties. Either party shall be permitted to appeal the final award under the AAA's Optional Appellate Arbitration Rules in effect at the time the dispute or claim arose. Grounds for vacating the award shall include, in addition to those enumerated under the Federal Arbitration Act, 9 U.S.C. §1, et seq, that the arbitrator committed errors of law that are material and prejudicial. The appeal shall be determined upon the written documents submitted by the parties, with no oral argument. After the appellate rights described in this section 16.1 have been exercised or waived, the parties shall have no further right to challenge the award.

16.2. Notwithstanding any exclusive jurisdiction provision above, Customer agrees that Rackspace may seek to enforce any judgment anywhere in the world where Customer may have assets. No claim may be brought as a class or collective action, nor may Customer assert such a claim as a member of a class or collective action that is brought by another claimant. Each party agrees that it shall not bring a claim under the Agreement more than two years after the time that the claim accrued. The Agreement shall not be governed by the United Nations Convention on the International Sale of Goods.

16.3. The prevailing party in any action or proceeding relating to the Agreement shall be entitled to recover reasonable legal fees and costs, including attorney's fees.

17. MISCELLANEOUS.

17.1. Some terms are incorporated into the Agreement by reference to pages on the Rackspace website and Rackspace may revise those terms from time to time (including the MSA). Such revisions shall only be effective and supersede and form part of the Agreement as of the time: (i) Customer enters into a new Service Order referencing the revised terms, or (ii) a Service Order automatically renews pursuant to the Agreement or the parties enter into an agreement for a Renewal Term in which case Customer acknowledges that Customer has reviewed and accepted the then-current version of the terms as of the date of the renewal. If there is a conflict between the terms of the Agreement, the documents shall govern in the following order: the Service Order, the Product Terms, and the MSA. The headings or captions in the Agreement are for convenience only. If over time Customer enters into multiple agreements for a given Customer Configuration (for example to add additional components or services) then the most recent terms referenced in the Service Order(s) shall govern the entirety of the Services for the given Customer Configuration.

17.2. Unless otherwise expressly permitted in the Agreement, the terms of the Agreement may be varied only by a written agreement signed by both parties that expressly refers to the Agreement. A Service Order may be amended to modify, add, or remove Services by a formal written agreement signed by both parties, or by an exchange of correspondence (including via the Rackspace ticketing system) that includes the express consent of an authorized individual for both parties. The pre-printed terms of Customer's purchase order or other business form or terms that Customer provides shall be void and of no effect.

17.3. If any part of the Agreement is found unenforceable, the rest of the Agreement shall continue in effect, and the unenforceable part shall be reformed to the extent possible to make it enforceable and give business efficacy to the Agreement. The parties acknowledge and agree that the pricing and other terms in the Agreement reflect and are based upon the intended allocation of risk between the parties and form an essential part of the Agreement. Each party may enforce its respective rights under the Agreement even if it has waived the right or failed to enforce the same or other rights in the past. The relationship between the parties is that of independent contractors and not business partners. Neither party is the agent for the other and neither party has the right to bind the other on any agreement with a third party. Other than Representatives for the purposes of sections 7, 10, and 11, or as otherwise specifically designated a "Third Party Beneficiary", there are no third party beneficiaries to the Agreement. The use of the word "including" means "including without limitation".

17.4. The following provisions shall survive expiration or termination of this MSA: Intellectual Property, Confidential Information, Limitation on Damages, Indemnification, Notices, Governing Law, Miscellaneous, all terms of the Agreement requiring Customer to pay any Fees for Services provided prior to the time of expiration or termination or requiring Customer to pay an early termination Fee, and any other provisions that by their nature are intended to survive expiration or termination of the Agreement.

17.5. The Agreement constitutes the complete and exclusive understanding between the parties regarding its subject matter and supersedes and replaces any prior or contemporaneous representation(s), agreement(s) or understanding(s), written or oral.

SCHEDULE 1
DEFINED TERMS

"**AAA**" means the American Arbitration Association.

"**Affiliate**" as to Customer means any entity that directly or indirectly controls, is controlled by, or is under common control with the entity referred to, but only for so long as such control exists; and as to Rackspace means Rackspace Hosting, Inc. and any entity that is directly or indirectly controlled by Rackspace Hosting, Inc. As used in this definition "**control**" means control of more than a 50% interest in an entity.

"**Agreement**" means, collectively, the MSA and any applicable Service Order, Product Terms, or other addenda which govern the provision of Services.

"**AUP**" means Rackspace's Acceptable Use Policy found at www.rackspace.com/information/legal/aup.

"**Auto Renewal Term**" means the automatic renewal period following expiry of the Initial Term, for consecutive rolling 90 day terms.

"**Business Day**" means Monday through Friday, excluding public holidays, in the country whose laws govern the Agreement.

"**Confidential Information**" means non-public information disclosed by one party to the other in any form that: (i) is designated as "Confidential"; (ii) a reasonable person knows or reasonably should understand to be confidential; or (iii) includes either party's products, customers, marketing and promotions, know-how, or the negotiated terms of the Agreement; and which is not independently developed by the other party without reference to the other's Confidential Information or otherwise known to the other party on a non-confidential basis prior to disclosure.

"**Customer Configuration**" means an information technology system (hardware, software and/or other information technology components) which is the subject of the Services or to which the Services relate.

"**Customer Data**" or "**Client Content**" means all data which Customer receives, stores, or transmits on or using the Customer Configuration.

"**Customer IP**" means Customer's pre-existing Intellectual Property.

"**Deliverables**" means the tangible or intangible materials which are prepared for Customer's use in the course of performing the Services and that are specifically identified and described in a Service Order as Deliverables.

"**Fees**" means the fees payable under the applicable Service Order.

"**Hosted System**" means a Customer Configuration provided by Rackspace for Customer's use at a Rackspace data center.

"**Initial Term**" means the initial term of the applicable Service Order.

"**Intellectual Property**" means patents, copyrights, trademarks, trade secrets, and any other proprietary intellectual property rights.

"**Local Withholding Taxes**" means withholding (or similar) taxes imposed on income that may be attributable to Rackspace in connection with its provision of the Services that Customer is legally required to withhold and remit to the applicable governmental or taxing authority.

"**One Time Services**" means Services which are provided on a one-off basis.

"**Open Source Software**" means open source software including Linux, OpenStack, and software licensed under the Apache, GPL, MIT, or other open source licenses.

"**Product Terms**" or "**Service Schedule(s)**" means additional terms and conditions incorporated in a Service Order which contain product-specific obligations.

"**Rackspace**" or "**we**" means the Rackspace Affiliate identified in the Service Order, or if none is identified: (i) Rackspace US, Inc. if Customer's primary billing address is located in the United States, or (ii) Rackspace International GmbH if Customer's primary billing address is located outside of the United States.

"**Rackspace Configuration Requirements**" means those specifications identified by Rackspace as required to perform the Services, such as a required reference architecture or software version, as described in Customer's Service Order or Product Terms.

"**Recurring Services**" means Services which are provided on an on-going basis.

"**Renewal Term**" means a fixed term extension of the Service Order term.

"**Representatives**" means a party's respective service providers, officers, directors, employees, contractors, Affiliates, suppliers, and agents.

"**Security and Privacy Practices**" means Rackspace's Global Security and Privacy Practices found at www.rackspace.com/information/legal/securitypractices.

"**Sensitive Data**" means any: (i) personally identifiable information or information that is referred to as personal data (including sensitive personal data); PII (or other like term) under applicable data protection or privacy law and includes information that by itself or combined with other information can be used to identify a person; (ii) financial records; and (iii) other sensitive or regulated information.

"**Services**" means the Rackspace services identified in a specific Service Order.

"**Service Order**" or "**Order Form**" means the document describing the Services Customer is purchasing, including any online order, process, API, statement of work, or tool through which Customer requests or provisions Services.

"**SLA**" means any provision providing a specified credit remedy for an identified failure to deliver or provide the Services to the identified standard.

"**Tax**" means any value added, goods and services, sales, use, property, excise, and like taxes, import duties and/or applicable levies arising out of the provision of the Services.

"**Test Services**" means those Services designed by Rackspace as "Test", "Beta", "early access", or with like designation in a Service Order.

"Test Terms" means the Test Terms found at www.rackspace.com/information/legal/testterms.

"**Third Party Fee Increase**" means the direct or indirect increase of fees by a third party vendor charged to Rackspace for Customer's use of Third Party Services, Third Party Software, or both, which may occur at any time.

"**Third Party Services**" means services provided by a third party and used in connection with the Services.

“**Third Party Software**” means software applications provided by a third party and used in connection with the Services.

“**TPS Agreements**” means agreements for products and services provided by third parties, which are entered into directly between Customer and such third party.

“**Unsupported Services**” means Services designated by Rackspace as “best efforts”, “non-standard”, “reasonable endeavors”, “unsupported”, or with like designation in a Service Order.

US PUBLIC SECTOR TERMS

In addition to any other terms and conditions of Customer's Agreement with Rackspace, these US Public Sector Terms shall apply only to Services where the Customer's end user of those Services is any agency or instrumentality of the United States ("**Government End User**"). In the event of a conflict, these US Public Sector Terms shall take precedence over the any other term or condition of the Agreement.

1. GOVERNMENT CUSTOMERS.

1.1. Commercial Items Representation. The parties acknowledge that Services constitute "commercial items" as defined in the Federal Acquisition Regulation ("FAR") at 48 U.S.C. 2.101.

1.2. Termination for Government Customer's Convenience. In the event that a Government End User terminates Customer's prime contract or order for the Services for convenience, Customer may terminate only the Services directly affected by the Government End User's termination on at least 30 days written notice to Rackspace. In the event of termination for convenience under this Section 1.2, Customer shall be liable to Rackspace for the value of all Services provided through to the effective date of termination, and for Rackspace's costs associated with the termination.

1.3. Government License Rights. The rights to use, modify, reproduce, release, perform, display, sublicense, or disclose technical data and software related to Services include only those rights customarily provided to the public as set out in Rackspace's Agreement. Rackspace's Agreement is its customary commercial license provided in accordance with FAR 12.211 (Technical Data) and FAR 12.212 (Software) for Government End Users. This Section 1.3, consistent with 48 C.F.R. 12.211, 48 C.F.R. 27.212 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses US Government rights in computer software, computer software documentation or technical data related to the Rackspace software or third party services and software products licensed under the Agreement.

2. US GOVERNMENT FLOWDOWNS. The following FAR clauses shall apply to the Services only if included in Customer's prime contract with the Government End User for the end use of those Services. No other FAR, DFARS, or other clauses shall apply unless agreed to by the parties in writing.

2.1. FAR 52.203-13. Contractor Code of Business Ethics and Conduct (Apr. 2010), applies only to Service Orders with a value of more than US$5,000,000 and for Services with a performance period of more than 120 days.

2.2. FAR 52.203-14. Display of Hotline Poster(s) (Oct. 2015), applies only to Service Orders with a value of more than US$5,500,000.

2.3. FAR 52.203-15. Whistleblower Protection Under the American Recovery and Reinvestment Act of 2009, applies only if the Customer notifies Rackspace that the Service Order is funded under the Recovery Act.

2.4. FAR 52.222-21. Prohibition of Segregated Facilities (Apr. 2015), applies only when the clause at FAR 52.222-26 applies.

2.5. FAR 52.222-25. Affirmative Action Compliance (Apr. 1984).

2.6. FAR 52.222-26. Equal Employment Opportunity (Mar. 2007).

2.7. FAR 52.222-35. Equal Employment Opportunity for Veterans (Oct. 2015), applies only to Service Orders with a value equal to, or more than, US$150,000.00.

2.8. FAR 52.222-36. Affirmative Action for Workers with Disabilities (Oct. 2010).

2.9. FAR 52.222-37. Employment Reports on Veterans, applies only when the clause at FAR 52.222-35 applies.

2.10. FAR 52.222-38. Compliance With Veterans' Employment Reporting Requirement, applies only when the clause at FAR 52.222-37 applies.

2.11. FAR 52.222-40. Notification of Employee Rights Under the National Labor Relations Act (Dec. 2010).

2.12. FAR 52.222-50. Combating Trafficking in Persons (Jan. 2019).

2.13. FAR 52.222-54. Employment Eligibility Verification (Oct. 2015), applies only to Service Orders with a value of more than US$3,500.

3. NON-SOLICITATION. Customer shall not knowingly and directly solicit or attempt to solicit for employment or as a consultant any persons employed by Rackspace during the term or within one calendar year of termination or expiration of the Agreement. The foregoing restriction does not apply, however, to any employee or former employee of Rackspace who responds to a general advertisement, online job posting, or other form of broad solicitation that does not directly or indirectly target employees of Rackspace or who has been separated from employment with Rackspace for at least six consecutive calendar months before the date when the person is first recruited, solicited for hire, or offered employment.

RACKSPACE GOVERNMENT CLOUD ON VMWARE PRODUCT TERMS

In addition to any other terms and conditions of Client's Agreement with Rackspace, these Product Terms apply where Client purchases Rackspace Government Cloud on VMware Services.

1. ADDITIONAL DEFINED TERMS.

"**A&A Package**" means the Assessment and Authorization set of documents, consisting of the System Security Plan, supporting security plans, test results, plan of action, and milestones.

"**Available Hours**" means the total number of hours in an applicable month less the number of Cloud Infrastructure downtime hours attributable to Scheduled Maintenance and Emergency Maintenance in the same month.

"**Actual Uptime**" means applicable monthly Available Hours less Client Cloud Infrastructure downtime hours attributable to causes other than Scheduled Maintenance and Emergency Maintenance in the same month.

"**Border Routers**" means any routers that connect Rackspace's internal network to a transit or peering provider via Border Gateway Protocol (BGP). The external WAN interface uplinking the router to a third-party fiber or cross-connect provider is not included in this definition.

"**Business Hours**" means, for the sake of these Product Terms, 9:00 AM to 5:00 PM Eastern Standard Time, on Business Days.

"**Compliance Baseline**" means the defined set of security controls to which the Services are managed, as specified in the Service Order.

"**Contingency Plan**" means the artifact of the Compliance Baseline A&A Package required by all Cloud Service Providers. It denotes interim measures to recover information system services following an unprecedented emergency or system disruption. The Rackspace Contingency Plan is internal to Rackspace.

"**Client Access Switch**" means the Rackspace-managed access switch uplinked to the Production Environment.

"Client Appliance" means any Client-owned and managed virtual machine (VM).

"**Client Portal**" means Rackspace's Client ticketing and notification portal.

"**Cloud Infrastructure**" means the hardware and software resources, which are located in enterprise-grade data centers, used to deploy the Services, including the host servers, switches, firewalls, hypervisor, and Operating System Instances (OSIs) provided by Rackspace, as set forth in Client's Service Order(s). This excludes Client Appliances.

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

"**Disaster Recovery Site**" means the secondary site where Client production data will be replicated.

"**Disaster Recovery Testing**" means verifying the processes and services in place through simulated recovery of a mutually agreed-upon portion of the Production Environment in the Disaster Recovery Site.

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

"**Minimum Level Resources**" means the committed minimum capacities for each resource used to provide the Services specified in the Service Order(s).

"**Monthly Services Fee**" means those monthly fees incurred by Client that are related to the Services provided by Rackspace under these Product Terms.

"**Operating System Instance (OSI)**" means an independent, functional virtual or bare metal server running an operating system that is both supported by the operating system manufacturer and offered by Rackspace. This excludes Client Appliances.

"**Parties**" means Rackspace and Client collectively.

"**Party**" means Rackspace or Client individually.

"**Production Environment**" means the total Client environment, encompassing the entirety of contracted Services being delivered to Client in support of Client's production cloud solution, but explicitly excludes any resources designated "non-production" and/or "dev/test". This is inclusive of Cloud Infrastructure, Client Appliances, OSIs, Compliance Baseline, and any optional Services as provided by Rackspace and set forth in Service Order(s).

"**Privileged User**" means any user of the Client environment with access authority greater than users of the environment's applications. Privileged Users include application, database, network, system, and security administrators.

"**Recovery Point Objective**" or **"RPO"** means the maximum period of permitted data loss upon Restoration Success, measured in hours preceding the time of failure.

"**Recovery Time Objective**" or "**RTO**" means the duration of time, measured in hours, between Rackspace confirmation of a Disaster Declaration and Restoration Success.

"**Restoration Success**" means that the Operating System Instances at the Disaster Recovery Site are online and available for Client to use.

"**Rackspace Equipment**" means the Rackspace hardware used to provide the Services as set forth in these Product Terms.

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

"**Rackspace Support**" means the support available via the Client Portal, or by phone at (201) 792-4847, or such other phone number as Rackspace may designate in the future, which is available 24 hours a day, seven days a week, year-round.

"**Scheduled Maintenance**" means any planned maintenance or upgrades (including tech refreshes) needed for the security, redundancy, or performance of the Production Environment, Rackspace infrastructure, and/or the Rackspace Network.

"**Solution Escalation Action Plan (SEAP)**" means the jointly-prepared Client management plan that shall define the steps to be taken by Rackspace personnel when responding to incidents, tickets, and alerts. Specific monitoring thresholds are also documented in the SEAP.

"**System Security Plan**" means the main document of the A&A Package detailing how a Cloud Service Provider manages the security controls throughout the lifecycle of the Services, in accordance with the Compliance Baseline. In addition to the narrative of the security control implementation, it also includes a system description of the components and services inventory, and depictions of the system's data flows and authorization boundary.

"**vCore**" means a unit of server compute resources.

2. EXPORT MATTERS. Client may not provide access to the Services to any person (including any natural person, government, or private entity) that is located in, or is a national of, any country that is embargoed or highly restricted under US export laws and regulations.

3. SERVICE INFORMATION. Rackspace provides a fully managed cloud platform designed to support government cloud workloads. The Services are designed with single-tenant server, storage, and networking hardware managed 24x7 by Rackspace's operations teams. Rackspace is responsible for implementing and managing the Production Environment, up through and including the hypervisor for Client-provided Appliances and the OSI layer for all other Client VMs. Rackspace shall upgrade the Cloud Infrastructure as reasonably necessary to comply with the terms of the Agreement. The Services include implementation and ongoing management of the Compliance Baseline. At a minimum, the Compliance Baseline implements a subset of the NIST SP 800-53 Revision 4 Moderate impact security controls but may include additional overlays and/or Client-defined controls. Any controls in addition to, or in lieu of, provisionally authorized controls may be mutually agreed upon and included, provided there is no conflict of applicable laws, Executive Orders, directives, policies, regulations, or other mandated compliance requirements. Any additional, mutually agreed-upon controls shall be identified and set forth in the applicable Service Order, inclusive of any additional implementation and management fees, prior to being implemented and provided as part of the Services.

3.1. Managed Cloud Infrastructure Services.

(A) System Administration & Maintenance Services. Rackspace provides system administration and maintenance services for all elements of the Services. Compute, storage, network, and OSIs are configured, hardened, and managed per pre-defined configuration management controls. Rackspace installs and implements Client's Production Environment; and provides the maintenance, repair or replacement of all Cloud Infrastructure components of Client's environment. Client is solely responsible for all administration, maintenance, security, and compliance management services required for any software or program installed on the Rackspace-provided and -managed OSIs. Rackspace shall attempt to schedule maintenance for a time that minimizes impact on Client. Notice of Scheduled Maintenance shall be provided through the Client Portal.

(B) Cloud Server Compute Resources. Rackspace provides the use of dedicated computing resources as vCores to support Client's applications. Each increment of vCore includes computing resources of up to 4GB of memory and one virtual CPU Core that can be combined to create virtual machines to match Client's requirements (e.g., combining multiple vCore resources to create a dual core virtual CPU, 8GB RAM virtual machine).

(C) Cloud Storage Services. Rackspace provides a fully managed storage environment for OSIs, Client Appliances, backups, and disaster recovery, separated at the Client tenant level. Storage options are tiered for price and performance optimization, and provisioned and billed in 100GB increments, as defined in the Service Order.

(D) Capacity Planning. Client may request alerts when pre-defined thresholds (documented in the SEAP) have been reached. These alerts shall proactively notify Client that additional resources may be required to support their workloads. All requests for additional resources shall be made in writing, either via the Client Portal or executed Service Order.

(E) Network Services. Rackspace provides highly available LAN configurations as well as redundant WAN connectivity through multiple Tier I internet service providers, including Rackspace Network links between

data centers. Rackspace shall provide availability monitoring of all Rackspace Network components. Rackspace also implements denial-of-service (DoS) protection mechanisms at the network ingress and egress points.

(i) Network Capacity. Rackspace provides a maximum of 5 Mbps of public internet bandwidth per OSI, at no additional charge.

(F) Infrastructure Services Specifications.

SERVICE AREA	RACKSPACE STANDARD OFFERING
Bandwidth	Rackspace provides: • 10 Gbps connectivity at the primary and secondary data centers. • 10 Gbps Rackspace Network connection for replication between the primary and secondary data centers. • Firewall at ingress/egress

(G) OSI Management. Rackspace shall provide provisioning, hardening, encryption, administration, backups, monitoring, and alerting of the Production Environment OSIs deployed, as set forth in this Section 3.1(G) and in the applicable Service Order.

(i) Provisioning. The Rackspace Cloud Server Management Implementation Service provides the implementation and initial testing of the monitoring, alerting, and O/S administration tools for the cloud servers deployed.

(ii) Hardening. Rackspace hardens OSIs (Red Hat Enterprise Linux and Microsoft Windows Server only) and network devices to its configuration baseline based on Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) benchmarks. Prior to Client environment deployment and configuration, Rackspace shall communicate the STIG benchmark version to be implemented and managed. Any Client-defined hardening requirements in addition to, or in lieu of, the Rackspace DISA STIG configuration baseline shall be identified and set forth in Services Order(s), inclusive of any additional implementation and management fees, prior to being implemented and provided as part of the Services.

(iii) Encryption. Rackspace manages transparent FIPS 140-2 validated encryption at the storage layer. Compliance Baseline encryption requirements for any software or program installed on top of the Rackspace-provided and -managed OSIs are the sole responsibility of Client.

(iv) Administration. Rackspace provides administration of OSIs, including routine preventative maintenance, monthly patching, and troubleshooting, and may include additional services, as defined in the Service Order.

(v) Backups. Rackspace performs image-based Changed Block Tracking backups of Production Environment OSIs and Client Appliances once per day. If file-level, database-level, or otherwise application-aware backups are required, Client is responsible for providing a compatible backup solution – e.g., database-native backup to a local disk included in the daily image backup. The backups for Production Environment OSIs and Client Appliances shall be available onsite for 14 calendar days, and the Production Environment backups shall be replicated from the primary backup location to the archival backup location available in the Disaster Recovery Site for the same 14-day period. Client may request additional Services for longer retention periods, as defined in the Service Order. Any required restores shall only be created from Rackspace-provided disk images and presented to the OSI as a full disk. Client may choose to replace the existing disk or mount as an additional disk; but all file-level, application or database recovery efforts are Client's responsibility.

(H) Managed Security and Compliance Services. Rackspace performs the following functions, in accordance with the Compliance Baseline, to secure the Rackspace Network and Cloud Infrastructure. Compliance Baseline requirements for any software or program installed on top of the Rackspace-provided and -managed OSIs are the sole responsibility of Client.

(i) 24x7 Monitoring and Alerting. Rackspace monitors the performance, availability, and network connectivity of supported cloud servers 24x7. By default, all alerts are configured to go to Rackspace, but the SEAP can be updated to define Client notification and escalation criteria.

(ii) Access Control (AC). Rackspace's architecture and processes maintain controlled Privileged User access to the Cloud Infrastructure. Privileged Users shall access the Cloud Infrastructure with an encrypted VPN connection established using multi-factor authentication. This connection from outside the environment can only be made to an approved jump host server. While the connection is in place, all other internet communication from the Privileged User's source device is disabled. From the jump host, privileged users can access other devices within the Cloud Infrastructure via Remote Desktop Services or SSH based on role privileges set up by Rackspace.

All privileged user sessions on jump hosts are recorded to provide a detailed activity log to support potential security incident analysis and response.

Rackspace shall be responsible for and have administrator control over the domain, forest, and/or organizational units that comprise the computer, user, and service accounts that pertain to, and provide access to, the Production Environment.

(iii) Awareness and Training (AT). All Rackspace engineering staff supporting the Cloud Infrastructure receive annual privacy and information security awareness training.

(iv) Audit and Accountability (AU). Rackspace configures all elements of the Cloud Infrastructure to feed audit information into a centralized logging platform that provides near-real-time log collection, indexing, and management separated at the Client tenant level for: (i) System Security logs, (ii) IDS logs and (iii) Firewall logs.

Rackspace's centralized logging platform allows Rackspace security engineers and analysts to use a suite of automated and manual tools to extract audit information. In the event of a security incident or suspected incident, logs assist in determining: (i) if there was an incident, (ii) who was involved in the incident, (iii) when the incident took place, (iv) what type of incident took place and (v) how the incident occurred.

Logs are collected and retained online for 90 days through replication to the online log server and further preserved offline for one year.

Client is responsible for retaining application and database audit records online, in order to provide support for after-the-fact investigations of security incidents and to meet their respective regulatory and organizational information retention requirements. Client may purchase additional Services to store their logs. Client retains all responsibility for configuration and management of these additional log sources.

(v) Configuration Management (CM). Rackspace uses a baseline configuration based on DISA STIGs. Rackspace follows change and configuration management procedures detailed in the Configuration Management Plan as part of the A&A Package. As part of Rackspace's configuration management process, all proposed changes are recorded and analyzed for impact, and any Client-impacting changes are coordinated with Client. In addition, configuration tools automatically develop baselines when initially configured, and maintain those baselines by comparing any changes to the baseline, at least once per quarter, as the system is being used.

Any Client-defined hardening other than the Rackspace-defined configuration baseline shall be stated in any applicable Service Order(s), which shall include additional implementation and management fees.

(vi) Quarterly Configuration Compliance Scanning and Reporting. Rackspace scans the managed OSIs for compliance with the Rackspace-defined hardening configuration standard. The raw, unmodified compliance scan results shall be provided quarterly to Client for each environment.

Any Client-defined hardening configurations, other than the Rackspace-defined configuration baseline, shall be stated in any applicable Service Order(s), which shall include additional implementation and management fees.

Any custom-configuration compliance scanning and associated reporting shall be stated in any applicable Service Order(s), which shall include additional implementation and management fees.

(vii) Contingency Planning (CP). Rackspace maintains a Contingency Plan for the Rackspace Cloud Infrastructure as required by Compliance Baseline requirements. Rackspace shall support Client Contingency Planning efforts by meeting the Recovery Point Objective and Recovery Time Objective in the event of a major disruption to the Production Environment. The SEAP shall be used to define the tools, processes, and procedures within the areas of responsibility of Rackspace and Client. Rackspace shall provide one Disaster Recovery Test per year, upon Client request with written notice 30 days prior. This can include turning on virtual machines at a secondary facility; running specific workloads at a secondary facility in a temporary, non-impactful way; verifying data backup integrity; or testing for hardware outages.

(viii) Disaster Recovery. Rackspace provides replication of Client Production Environment OSIs and Client Appliances to a Disaster Recovery Site. Rackspace manages the Disaster Recovery Site and provides disaster recovery support services in accordance with the SEAP. Upon a Disaster Declaration, replicated VMs are activated by Rackspace in the Disaster Recovery Site to seek to restore Services to support Restoration Success within the RPO and RTO. RTO does not include any third-party dependencies outside of Rackspace's control, including Client application coming back online and time required for external third-party components and network protocols to be migrated by third-party providers. Any other application-level activities to recover and reconstitute the Client Production Environment are the responsibility of Client.

Rackspace makes no warranty as to the quality, contents or formatting of Client data. Client accepts and acknowledges the limitations of data replication, specifically that data corruption and deletion within the Production Environment, both intentional and unintentional, will be replicated to the Disaster Recovery Site. As such, Disaster Recovery shall NOT be used as a replacement for application state and database backups, which remain the sole responsibility of Client. Additionally, the rate at which the data in the Production Environment can be transferred to the Disaster Recovery Site shall vary depending on the rate of change, amount and type of data, constraints inherent in the Services, and fluctuations in bandwidth availability. Therefore, at any given time, the Disaster Recovery Site may not be completely up to date. In the event of a failover to the Disaster Recovery Site, data that has not yet completed transfer from the Production Environment shall be lost commensurate with the Recovery Point Objective. Client also accepts and acknowledges that this same risk of data loss exists during execution of Disaster Recovery Testing. Rackspace is not liable for any data loss as a result of performing Client initiated Disaster Recovery Testing, nor by executing Client's instructions in the event of a legitimate Disaster Declaration.

The Disaster Recovery Services provided are not a full business continuity solution. It is intended to be a component in a Client managed and executed business continuity plan. As such, Rackspace takes no responsibility for, and does not guarantee, any business continuity capabilities as a result of Client's use of the Disaster Recovery Services.

Where Client has not purchased VM Replication Enhanced Edition for Government Services the services shall enable the ability to meet a RPO and RTO commensurate with the Compliance Baseline; and unless otherwise specified in a Service Order the default RPO and RTO are both 24 hours.

Solely where Client purchases VM Replication Enhanced Edition for Government Services, and both the Client Production Environment and Disaster Recovery Site are located in the United States, then RPOs and RTOs shall not be set commensurate with the Compliance Baseline, and instead shall enable the ability to meet a RPO and RTO commensurate with commensurate with the Disaster Recovery Tier identified in the Service Order(s), as set out below:

Disaster Recovery Tier	RPO & RTO
Bronze	24 Hours
Silver	12 Hours
Gold	4 Hours
Platinum	1 Hour

Alternatively, Client can opt to deploy their Production Environments in an active-active manner, in which the Production Environment can always be running in the Disaster Recovery Site as well. Active-active configuration is a Client responsibility, outside of the scope of the base Services configuration, and would typically require application-level support.

(ix) Identification and Authentication (IA). Rackspace provides a Client-specific identity store implemented via Active Directory domain. This Active Directory domain resides on a pair of highly available domain controllers within the Production Environment. All resources within the Production Environment are domain-joined, including the VPN concentrator, which requires multi-factor authentication to establish a tunnel. This tunnel only exposes a single jump host, which is also domain-joined.

(x) Maintenance (MA). Rackspace shall coordinate maintenance windows to perform Scheduled Maintenance activities as required for the Cloud Infrastructure components that Rackspace supports. Rackspace shall notify Client of Scheduled Maintenance at least five Business Days before maintenance is scheduled to occur; notification shall be via Client Portal. Scheduled Maintenance may be adjusted by Rackspace up to 24 hours in either direction (before or after the then-current maintenance schedule); however, to the extent Client requires changes to the maintenance schedule, Client shall coordinate such change within 24 hours of Rackspace notification.

On occasion, Emergency Maintenance may be required to maintain a security posture commensurate with the Compliance Baseline. Rackspace is authorized to perform all reasonable actions to meet or exceed requirements in connection with the delivery of the Services against the Compliance Baseline. Rackspace shall make every effort to provide advanced notification to Clients whenever possible, but specific circumstances may dictate immediate action without prior notification.

(xi) Media Protection (MP). Rackspace utilizes validated cryptographic mechanisms to encrypt removable storage media within Rackspace data centers. All physical media transport outside of the data center is strictly controlled. Unless set forth in a separate agreement, Rackspace shall not accept any Client-furnished storage devices, and Rackspace shall not provide to Client any Rackspace storage

devices. All decommissioned disk drives and digital media are sanitized before physical destruction, in accordance with the Compliance Baseline.

(xii) Personnel Security (PS). All Rackspace personnel with physical or logical access to the Cloud Infrastructure shall be U.S. Citizens and undergo pre-employment background checks as part of the on-boarding and application process. An employee's hiring is contingent upon internal investigations, such as background, credit, and reference checks.

If Client requires personnel security approvals or clearances outside of Rackspace's standard background investigation, then Rackspace reserves the right to submit for approval and/or clearance its entire operations and security teams associated with the Services to enable adequate support. Client shall bear the costs and expenses incurred by Rackspace in connection with obtaining approvals or clearances required to allow Rackspace to perform its obligations hereunder.

(xiii) Physical Environment (PE). Rackspace data centers implement security safeguards to control access to areas within the facility that are officially designated as publicly accessible. Rackspace uses badges for all personnel with access privileges. Rackspace maintains a current list of personnel with authorized access to the areas where the Cloud Infrastructure resides, in addition to maintaining a separate list of personnel with authorized access to the government-only enclave area. The data center floor incorporates badge and biometric access controls, alarmed dual-factor authenticated locked doors, CCTV, and 24x7 guards to enforce physical access authorizations at all access points. Separate controlled access is required to access a U.S. government-only enclave area of the data center.

(xiv) Risk Assessment (RA).

(a) Monthly Vulnerability Scanning. Rackspace performs monthly vulnerability scanning for each Client's managed OSIs within their environment(s). The scans are performed by Rackspace and the raw, unmodified vulnerability scan results shall be provided to Client. Rackspace and Client shall mutually agree on a monthly scanning schedule for the duration of the services agreement.

Any custom vulnerability scanning activities and associated reporting requested by Clients shall be stated in any applicable Service Order(s), which shall include additional implementation and management fees.

(xv) System and Communication Protection (SC). Rackspace separates user functionality from management functionality through physical and logical network segmentation and associated access management policies. The Cloud Infrastructure is separated into at least two security environments: 1) a management environment containing Rackspace's support tools, and 2) Client's Production Environment. Client may implement "non-production" environments. Access to each environment is controlled by a logical firewall. Access to the management environment is limited to only Rackspace personnel. Privileged Users access the Production Environment using multi-factor authentication into a jump host via an encrypted VPN connection. End users of Client's application enter through Client-managed, application-defined mechanisms.

Rackspace provides each Client environment with a network intrusion detection sensor that monitors all network traffic to and from the Client's Production Environment. The sensor monitors all unencrypted traffic for indicators of known potential attacks and potentially malicious traffic, excluding network traffic that is encrypted using transport-layer encryption methods (e.g. HTTPS, SSL, TLS, SSH) which the sensor is unable to decrypt.

(a) System Availability. Appliance availability and failover is accomplished via component resiliency at several levels.

At the network level, WAN internet connectivity is delivered through Tier 1 internet service providers. The connectivity is available via Border Gateway Protocol (BGP), whereby Rackspace announces paths for public IPs amongst all carriers. In the event of a carrier, link, or device failure, traffic is automatically re-routed.

From the edge WAN routers through to the host servers, all network devices and paths are redundantly meshed to prevent perceptible downtime in the event of the failure of any single device. Each host server has redundant path connections to both storage and production networks.

Unless otherwise specified in a Service Order, the host servers powering the Production Environment are configured in an N+1 configuration featuring VMware's high availability (HA) capability which shall restart any VM(s) from a failed host server on the remaining server nodes in the cluster.

(xvi) System Integrity (SI).

(a) Endpoint Security Management. Rackspace provides a centrally managed endpoint security software platform for all Client OSIs within their environment. The endpoint security management solution provides centralized anti-virus, malware defense**,** and host-based intrusion prevention services. Rackspace provides ongoing management of the management servers**;** agents installed on OSIs**;** and associated configurations, updates**,** and policy management. In the event a security event is detected, Rackspace shall notify and collaborate with Client to determine the appropriate actions.

(b) File Integrity Monitoring. Rackspace provides a centrally managed File Integrity Monitoring (FIM) solution that monitors all Client OSIs for file changes. The FIM solution monitors core OSI operating system files and identifies and reports on changes made to these files. Monitoring the integrity of Client data and/or application files installed by Client on OSIs is excluded from the Rackspace FIM solution monitoring scope of services. Rackspace provides ongoing management of the FIM management servers; agents installed on OSIs; and associated configurations, updates, and policy management. In the event a FIM event is detected, Rackspace shall notify Client and shall collaborate with Client to determine the appropriate actions.

4. AUDIT SUPPORT SERVICES. Upon at least 30 days of advance written notice, Rackspace provides up to 60 hours of security audit services for one security audit, per each 12-month period for each separate engagement following the Commencement Date of the applicable Service Order. Any additional security audit services required by Client for each Project above this time cap, shall be available during Business Hours for $250.00 USD per person, per hour, if booked two or more weeks in advance. For less than two weeks of advance notice, additional security audit services shall be available during Business Hours for $350.00 USD per person, per hour. Additional security audit services requested outside of Business Hours are available for $450 USD per person, per hour. If the security audit is performed on behalf of an end client of Client, Client shall give Rackspace direct access to the end client and its auditors.

5. INCIDENT RESPONSE.

5.1. Communication During Incident Management. Client shall assist Rackspace in developing a SEAP that shall define the steps to be taken by Rackspace personnel when responding to incidents, tickets, and alerts.

During the incident management process, Rackspace and Client shall communicate via means designated in the SEAP. Communications shall be made based on the timelines defined in the SLAs listed in Section 6.

In the event that incident resolution requires Client cooperation, such cooperation shall not be unreasonably withheld.

Upon incident receipt notification by phone call or Client Portal, Rackspace shall respond to Client via the Client Portal.

Rackspace shall use commercially reasonable efforts to provide the post-incident Client incident report within two Business Days via email.

Client shall designate a primary point of contact to communicate with Rackspace regarding all technical issues that may arise during the term of any Service Orders in the agreement, including highlighting the priority and urgency of Client tickets and requests.

5.2. Support Requests. Client shall create tickets within the Rackspace Portal for all support requests, change requests, or incidents. Following the submission of the ticket, Rackspace's response time shall match the agreed-upon severity of the ticket, as described in Section 6.1.

The Client Portal shall send an email notification to the requestor/creator of the ticket as well as the approver when a ticket is closed by Rackspace Support personnel.

5.3. Security Incident Response. In the event of a security incident in the Client Infrastructure, such as a denial of service attack, Rackspace reserves the right to suspend Services without notice as necessary (e.g., powering off or network-isolating Client Appliances and OSIs), until completion of remediation.

6. SERVICE LEVEL AGREEMENTS (SLA).

6.1. Initial Incident Response Time SLAs.

Ticket Severity	Severity Definition	Initial Response Time
Sev1	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.	15 minutes
Sev2	Either of the following: (i) 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; or (ii) Any other support request not meeting the definition of Severity Level 1.	60 minutes

Client is entitled to a credit of $250 for the failure of Rackspace to meet the Section 6.1 Initial Response Time SLAs. The Initial Response Time begins upon the Client Portal system timestamp for submission of a ticket, resulting from a ticket being submitted by either (i) Client or (ii) Rackspace Support through the Rackspace Support phone number.

6.2. Availability SLAs. Rackspace guarantees 99.95% availability for Cloud Infrastructure. Client shall be entitled to prorated monthly Fees for each full or partial hour of downtime in excess of the Availability SLA.

6.3. Disaster Recovery SLA. Solely where Client purchases VM Replication Enhanced Edition for Government Services, Rackspace guarantees that it shall meet the applicable RTO for the Disaster Recovery Tier.). Rackspace makes no guarantee the RTO shall be achieved where the Client does not purchase VM Replication Enhanced Edition for Government Services; and in all circumstances Rackspace makes no guarantee that the RPO shall be achieved. Client is entitled to a credit of $250 for the failure of Rackspace to meet the Section 6.3 Enhanced Disaster Recovery Time SLA.

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

(A) Scheduled Maintenance or Emergency Maintenance

(B) Written agreement between Rackspace and Client confirming a change may be implemented without following the Change Control Processes

(C) Client-initiated work independently generated by Client

(D) Client support requests not submitted through the Client Portal nor Rackspace Support phoneline

(E) Service interruptions requested by Client

(F) Violations of Rackspace's Acceptable Use Policy as may be updated from time to time at www.rackspace.com/information/legal/aup.php

(G) Client-required OSI revisions and hardware/software configurations that are not Rackspace tested/approved

(H) Client-created rules, objects, functional configuration errors, third-party software configuration, or other failure of Client Appliances, software, or hardware, or third-party software or hardware

(I) Events of Force Majeure

(J) DNS issues outside the direct control of Rackspace

(K) Patches or antivirus updates which contain code faults, flaws, or other errors attributable to the third-party vendors that created such code

(L) Any suspension of the Services pursuant to the terms of the Agreement

(M) A DoS attack or distributed denial-of-service attack (DDoS attack)

(N) Any actions or inactions of Client, an end user, or any third party

(O) Client's equipment, software, or other technology and/or third-party equipment, software, or other technology (other than third-party equipment within Rackspace's direct control)

(P) Client's failure to request SLA credits within 30 days of the applicable month for which Services are invoiced

(Q) Manufacturer or safety code-related shutdowns required for safety compliance

6.5. Service Level Credit Limitations. The SLA credit remedies contained in this Section are Rackspace's sole and exclusive liability and Client's sole and exclusive remedy for any failure of Rackspace to meet an SLA. Client must request SLA credits within 30 days of the applicable month for which Services are invoiced. The total credit available to Client for all SLA failures in any particular calendar month shall in no event exceed the Monthly Service Fee for the environment in which the SLA failure occurred during that invoiced month. Any credits available to Client shall be applied to Fees due from Client for the Monthly Services Fee and shall not be paid to Client as a refund, unless such credit pertains to the last month of Client's service.

RACKSPACE GOVERNMENT CLOUD ON AWS PRODUCT TERMS

In addition to any other terms and conditions of Client's Agreement with Rackspace, these Product Terms apply where Client purchases Rackspace Government Cloud on AWS Services.

1. ADDITIONAL DEFINED TERMS.

"**A&A Package**" means the Assessment and Authorization set of documents, consisting of the System Security Plan, supporting security plans, test results, plan of action, and milestones.

"**Available Hours**" means the total number of hours in an applicable month less the number of Cloud Infrastructure downtime hours attributable to Scheduled Maintenance and Emergency Maintenance in the same month.

"**Actual Uptime**" means applicable monthly Available Hours less Client Cloud Infrastructure downtime hours attributable to causes other than Scheduled Maintenance and Emergency Maintenance in the same month.

"**Business Hours**" means, for the sake of these Product Terms, 9:00 AM to 5:00 PM Eastern Standard Time, on Business Days.

"**Compliance Baseline**" means the defined set of security controls to which the Services are managed, as specified in the Service Order.

"**Contingency Plan**" means the artifact of the Compliance Baseline A&A Package required by all Cloud Service Providers. It denotes interim measures to recover information system services following an unprecedented emergency or system disruption. The Rackspace Contingency Plan is internal to Rackspace.

"**Client Portal**" means Rackspace's Client ticketing and notification portal.

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

"**Disaster Recovery Site**" means the secondary site where Client production data shall be replicated.

"**Disaster Recovery Testing**" means verifying the processes and services in place through simulated recovery of a mutually agreed-upon portion of the Production Environment in the Disaster Recovery Site.

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

"**Monthly Services Fee**" means those monthly fees incurred by Client that are related to the Services provided by Rackspace under these Product Terms.

"**Parties**" means Rackspace and Client collectively.

"**Party**" means Rackspace or Client individually.

"**Privileged User**" means any user of the Client environment with access authority greater than users of the environment's applications. Privileged Users include application, database, network, system, and security administrators.

"**Recovery Point Objective**" means the maximum period of permitted data loss upon Restoration Success, measured in hours preceding the time of failure.

"**Recovery Time Objective**" means the duration of time, measured in hours, between Rackspace confirmation of a Disaster Declaration and Restoration Success.

"**Restoration Success**" means that the Operating System Instances at the Disaster Recovery Site are online and available for Client to use.

"**Rackspace Equipment**" means the Rackspace hardware used to provide the Services as set forth in these Product Terms.

"**Rackspace Network**" means the TCP/IP stack of all Rackspace-owned and -managed networking hardware and software.

"**Rackspace Support**" means the support available via the Client Portal, or by phone (as Rackspace may designate), which is available 24 hours a day, seven days a week, year-round.

"**Scheduled Maintenance**" means any planned maintenance or upgrades (including tech refreshes) needed for the security, redundancy, or performance of the Production Environment, Rackspace infrastructure, and/or the Rackspace Network.

"**Solution Escalation Action Plan (SEAP)**" means the jointly-prepared Client management plan that shall define the steps to be taken by Rackspace personnel when responding to incidents, tickets, and alerts. Specific monitoring thresholds are also documented in the SEAP.

"**System Security Plan**" means the main document of the A&A Package detailing how a Cloud Service Provider manages the security controls throughout the lifecycle of the Services, in accordance with the Compliance Baseline. In addition to the narrative of the security control implementation, it also includes a system description of the components and services inventory, and depictions of the system's data flows and authorization boundary.

1.1. Rackspace Government Cloud on AWS Definitions.

"**AWS**" means Amazon Web Services, Inc.

"**AWS Client License Terms**" means the separate agreement between Client and AWS governing Client's use of the AWS Services, which may be updated by AWS from time to time and are located at https://s3.amazonaws.com/Reseller-Program-Legal-Documents/AWS+Reseller+Customer+License+Terms.pdf or such other URL as AWS may designate in the future.

"**AWS Public Sector Policy**" means the access policy between Client and AWS governing Client's use of the AWS Service if Client is a Public Sector Client, which may be updated by AWS from time to time and are located at https://s3.amazonaws.com/Reseller-Program-Legal-Documents/AWS+Access+Policy.pdf or such other URL as AWS may designate in the future.

"**AWS Services**" means the web services made available by AWS.

"**AWS Service Level Agreement**" means all service level agreements that AWS offers for the AWS Services and posted on the AWS Site, as updated by AWS from time to time.

"**AWS Site**" means http://aws.amazon.com (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

"**Client Appliance**" means any Client-owned and managed EC2 instance.

"**Cloud Infrastructure**" means the hardware and software resources, used to deploy the Services, including the AWS Services, and Operating System Instances (OSIs) provided by Rackspace, as set forth in Client's Service Order(s). This excludes Client Appliances.

"**Minimum Level Resources**" means the committed minimum capacities for each resource used to provide the Services specified in the Service Order(s).

"**Operating System Instance (OSI)**" means an independent, functional EC2 instance running an operating system that is both supported by the operating system manufacturer and offered by Rackspace. This excludes Client Appliances.

"**Production Environment**" means the total Client environment, encompassing the entirety of contracted Services being delivered to Client in support of Client's production cloud solution, but explicitly excludes any resources designated as "non-production," "dev/test," or identified with similar language. This is inclusive of Cloud Infrastructure, Client Appliances, OSIs, Compliance Baseline, and any optional Services as provided by Rackspace and set forth in Service Order(s).

"**Public Sector Client**" means a Client that is an agency, organization, or other entity that is within (or is substantially owned, funded, managed, or controlled by): (i) the executive, legislative, or judicial branches of any government within the U.S. (federal, state, or local) and its territories; or by any other country's government at any level; (ii) Quasi-governmental entities (such as the World Bank); (iii) international governing/regulatory bodies (such as EU institutions); (iv) publicly funded institutions (such as colleges, universities, and hospitals); or (v) higher-tier prime contractors, consultants, or other entities working in support of the foregoing. Commercial entities which also qualify as Public Sector Clients (e.g. higher tier prime government contractors) do not constitute Public Sector Clients for purposes of this Agreement.

2. EXPORT MATTERS. Client may not provide access to the Services to any person (including any natural person, government, or private entity) that is located in, or is a national of, any country that is embargoed or highly restricted under US export laws and regulations.

3. SERVICE INFORMATION. Rackspace provides a fully managed cloud platform designed to support government cloud workloads. The Services are designed with multi-tenant server, storage, and networking provided by AWS and managed 24x7 by Rackspace operations teams. Rackspace is responsible for implementing and managing the Production Environment, up through and including the AWS Services for Client Appliances and the OSI layer for all other Client instances. Rackspace shall upgrade the Cloud Infrastructure as reasonably necessary to comply with the terms of the Agreement. The Services include implementation and ongoing management of the Compliance Baseline. At a minimum, the Compliance Baseline implements a subset of the NIST SP 800-53 Revision 4 Moderate impact security controls, but may include additional overlays and/or Client-defined controls. Any controls in addition to, or in lieu of, provisionally authorized controls may be mutually agreed upon and included, provided there is no conflict of applicable laws, Executive Orders, directives, policies, regulations, or other mandated compliance requirements. Any additional, mutually agreed-upon controls shall be identified and set forth in the applicable Service Order, inclusive of any additional implementation and management fees, prior to being implemented and provided as part of the Services.

3.1. AWS Services. Unless Client is a Public Sector Client: by entering the Agreement, Client acknowledges that its use of the AWS Services is subject to the AWS Client License Terms, which shall be effective without signature, and the Agreement. If Client is a Public Sector Client: by entering the Agreement, Client acknowledges that its use of AWS Services is subject to the AWS Public Sector Access Policy, which shall be effective without signature, and this Agreement. Rackspace is Client's "Reseller" as defined in the AWS Client License Terms or Public Sector Access Policy, and Client releases Rackspace from any and all liability whatsoever arising out of or in connection with the AWS Services, AWS' provision, management, or operation of the AWS Services, and AWS' exercise of its rights in the AWS Client License Terms or Public Sector Access Policy or Client's breach thereof.

Rackspace provides for Client use all US-based AWS Services within scope of AWS' FedRAMP authorization, which may be updated by AWS from time to time and are located at https://aws.amazon.com/compliance/services-in-scope/. Not all services are available in all AWS regions, and if an ATO is required, only offerings that are part of the various AWS FedRAMP P-ATO's shall be made available. Rackspace may further limit the included offerings due to compliance and/or functional requirements. Rackspace shall provision in-scope services and manage for Client as part of the Production Environment. All support requests shall be made directly to Rackspace, and Rackspace shall escalate to AWS directly, if needed.

(A) AWS Services Resale. Rackspace shall resell to Client a subscription for the AWS Services and provision its AWS account(s) in accordance with the Compliance Baseline. Default settings shall be applied to the AWS account(s) provisioned by Rackspace on Client's behalf. Rackspace shall charge Client the current AWS retail rates for Client's use of the AWS Services (including use of the AWS Services resulting from Rackspace's support), fees for any AWS Marketplace purchases, and a fee for the support Services (collectively, "**Monthly Services Fee**"). Rackspace shall obtain Client's AWS usage and billing information directly from Client's AWS account. Client is prohibited from reselling the AWS Services. Client is prohibited from selling, transferring, or sublicensing Client's Rackspace or AWS account credentials to any other party (except to agents and subcontractors performing work on Client's behalf).

(B) Agent for Third-Party Software. Rackspace may agree to install third-party software (for example, from AWS Marketplace) as part of the Services. Where such activity requires the acceptance of an End User License Agreement (or similar terms), Client hereby authorizes Rackspace to accept such terms on Client's behalf, agrees to be bound by and adhere to such terms, and acknowledges that Client, and not Rackspace are bound by such terms. Client may request third-party terms via ticket when Rackspace accepts such terms on Client's behalf.

(C) GovCloud Specific Terms. When Client purchases GovCloud Services in any Service Order, the AWS Services may not be used to process or store classified data. Client is responsible for verifying that all End Users access Client content in the AWS GovCloud (US) Region are eligible to gain access to Client content. Client represents and warrants that Client: (i) is a U.S. Person, as defined by 22 CFR part 120.15 ("**U.S. Person**"); (ii) shall only assign a U.S. Person as account owner for the AWS GovCloud (US) Region; (iii) if required by the International Traffic in arms Regulations ("**ITAR**"), has and shall maintain a valid Directorate of Defense Trade Controls registration; (iv) is not subject to export restrictions under U.S. export control laws and regulations (e.g., neither Client nor any of its board members, officer, or employees is a denied or debarred party or otherwise subject to sanctions); and (v) maintain an effective compliance program to ensure compliance with applicable U.S. export control laws and regulations, including the ITAR. If requested, Client agrees to provide additional documentation and cooperation to verify the accuracy of the foregoing representations and warranties.

3.2. Managed Cloud Infrastructure Services.

(A) System Administration & Maintenance Services. Rackspace provides system administration and maintenance services for all supported elements of the Services. AWS Services and OSIs are configured, hardened, and managed per pre-defined configuration management controls. Rackspace installs and implements Client's Production Environment; and provides the maintenance, repair or replacement of all Cloud Infrastructure components of Client's environment. Client is solely responsible for all administration, maintenance, security, and compliance management services required for any software or program installed on the Rackspace-provided and -managed OSIs. Rackspace shall attempt to schedule maintenance for a time that minimizes impact on Client. Notice of Scheduled Maintenance shall be provided through the Client Portal.

(B) Capacity Planning. Client may request alerts when pre-defined thresholds (documented in the SEAP) have been reached. These alerts shall proactively notify Client that additional resources may be

required to support their workloads. All requests for additional resources shall be made in writing, either via the Client Portal or executed Service Order.

(C) OSI Management. Rackspace shall provide provisioning, hardening, encryption, administration, backups, monitoring, and alerting of the Production Environment OSIs deployed, as set forth herein and in the applicable Service Order.

(i) Provisioning. The Rackspace Cloud Server Management Implementation Service provides the implementation and initial testing of the monitoring, alerting, and O/S administration tools for the cloud servers deployed.

(ii) Hardening. Rackspace hardens OSIs (Red Hat Enterprise Linux and Microsoft Windows Server only) and network devices to its configuration baseline based on Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) benchmarks. Prior to Client environment deployment and configuration, Rackspace shall communicate the STIG benchmark version to be implemented and managed. Any Client-defined hardening requirements in addition to, or in lieu of, the Rackspace DISA STIG configuration baseline shall be identified and set forth in Services Order(s), inclusive of any additional implementation and management fees, prior to being implemented and provided as part of the Services.

(iii) Encryption. Rackspace enables AWS-native transparent encryption at the storage layer. Compliance Baseline encryption requirements for any software or program installed on top of the Rackspace-provided and -managed OSIs are the sole responsibility of Client.

(iv) Administration. Rackspace provides administration of OSIs, including routine preventative maintenance, monthly patching, and troubleshooting, and may include additional services, as defined in the Service Order.

(v) Backups. Rackspace configures AWS-native image-based backups of Production Environment OSIs and Client Appliances once per day. If file-level, database-level, or otherwise application-aware backups are required, Client is responsible for providing a compatible backup solution – e.g., database-native backup to a local disk included in the daily image backup. The backups for Production Environment OSIs and Client Appliances shall be available onsite for 14 calendar days, and the Production Environment backups shall be replicated from the primary backup location to the archival backup location available in the Disaster Recovery Site for the same 14-day period. Client may request additional Services for longer retention periods, as defined in the Service Order. Any required restores shall only be created from Rackspace-provided disk images and presented to the OSI as a full disk. Client may choose to replace the existing disk or mount as an additional disk; but all file-level, application or database recovery efforts are Client's responsibility.

3.3. Managed Security and Compliance Services. Rackspace performs the following functions, in accordance with the Compliance Baseline, to secure the Rackspace Network and Cloud Infrastructure. Compliance Baseline requirements for any software or program installed on top of the Rackspace-provided and -managed OSIs are the sole responsibility of Client.

(A) 24x7 Monitoring and Alerting. Rackspace monitors the performance, availability, and network connectivity of supported cloud servers 24x7. By default, all alerts are configured to go to Rackspace, but the SEAP can be updated to define Client notification and escalation criteria.

(B) Access Control (AC). Rackspace's architecture and processes maintain controlled Privileged User access to the Cloud Infrastructure. Privileged Users shall access the Cloud Infrastructure with an encrypted VPN connection established using multi-factor authentication. A connection from outside the environment can only be made to an approved jump host server. While the connection is in place, all other internet communication from the Privileged User's source device is disabled. From the jump host, privileged users

can access other devices within the Cloud Infrastructure via Remote Desktop Services or SSH based on role privileges set up by Rackspace.

All privileged user sessions on jump hosts are recorded to provide a detailed activity log to support potential security incident analysis and response.

Rackspace shall be responsible for and have administrator control over the domain, forest, and/or organizational units that comprise the computer, user, and service accounts that pertain to, and provide access to the Production Environment.

(C) Awareness and Training (AT). All Rackspace engineering staff supporting the Cloud Infrastructure receive annual privacy and information security awareness training.

(D) Audit and Accountability (AU). Rackspace configures all elements of the Cloud Infrastructure to feed audit information into a centralized logging platform that provides near-real-time log collection, indexing, and management separated at the Client tenant level for (i) system security logs, (ii) IDS logs, (iii) firewall logs. Rackspace's centralized logging platform allows Rackspace security engineers and analysts to use a suite of automated and manual tools to extract audit information. Logs are collected and retained online for 90 days through replication to the online log server and further preserved offline for one year. Client is responsible for retaining application and database audit records online, in order to provide support for after-the-fact investigations of security incidents and to meet their respective regulatory and organizational information retention requirements. Client may purchase additional Services to store their logs. Client retains all responsibility for configuration and management of these additional log sources. In the event of a security incident or suspected incident, logs assist in determining:

(i) if there was an incident,

(ii) who was involved in the incident,

(iii) when the incident took place,

(iv) what type of incident took place, and

(v) how the incident occurred.

(E) Configuration Management (CM). Rackspace uses a baseline configuration based on DISA STIGs. Rackspace follows change and configuration management procedures detailed in the configuration management plan, which is part of the A&A Package. As part of Rackspace's configuration management process, all proposed changes are recorded and analyzed for impact, and any Client-impacting changes are coordinated with Client. In addition, configuration tools automatically develop baselines when initially configured, and maintain those baselines by comparing any changes to the baseline, at least once per quarter, as the system is being used.

Any Client-defined hardening, other than the Rackspace-defined configuration baseline, shall be stated in any applicable Service Order(s), which shall include additional implementation and management fees.

(F) Quarterly Configuration Compliance Scanning and Reporting. Rackspace scans the managed OSIs for compliance with the Rackspace-defined hardening configuration standard. The raw, unmodified compliance scan results shall be provided quarterly to Client for each environment.

Any Client-defined hardening configurations, other than the Rackspace-defined configuration baseline, shall be stated in any applicable Service Order(s), which shall include additional implementation and management fees.

Any custom-configuration compliance scanning and associated reporting shall be stated in any applicable Service Order(s), which shall include additional implementation and management fees.

(G) Contingency Planning (CP). Rackspace maintains a Contingency Plan for the Rackspace Cloud Infrastructure as required by Compliance Baseline requirements. Rackspace shall support Client Contingency Planning efforts by meeting the Recovery Point Objective and Recovery Time Objective in the event of a major disruption to the Production Environment. The SEAP shall be used to define the tools, processes, and procedures within the areas of responsibility of Rackspace and Client. Rackspace shall provide one Disaster Recovery Test per year, upon Client request with written notice 30 days prior. This can include turning on virtual machines at a secondary facility; running specific workloads at a secondary facility in a temporary, non-impactful way; verifying data backup integrity; or testing for hardware outages.

(H) Disaster Recovery. Rackspace provides replication of Client Production Environment OSIs and Client Appliances to a Disaster Recovery Site to enable the ability to meet a Recovery Point Objective and Recovery Time Objective commensurate with the Compliance Baseline. Unless otherwise specified in a Service Order, the default Recovery Point Objective and Recovery Time Objective are both 24 hours. Rackspace manages the Disaster Recovery Site and provides disaster recovery support services in accordance with the SEAP. Upon a Disaster Declaration, replicated instances are activated by Rackspace in the Disaster Recovery Site to restore Services to support Restoration Success within the Recovery Point Objective and Recovery Time Objective. Recovery Time Objective does not include any third-party dependencies outside of Rackspace's control, including Client Appliance coming back online and time required for external third-party components and network protocols to be migrated by third-party providers. Any other application-level activities to recover and reconstitute the Client Production Environment are the responsibility of Client.

Alternatively, Client can opt to deploy their Production Environments in an active-active manner, in which the Production Environment can always be running in the Disaster Recovery Site as well. Active-active configuration is a Client responsibility, outside of the scope of the base Services configuration, and would typically require application-level support.

(I) Identification and Authentication (IA). Rackspace provides a Client-specific identity store implemented via Active Directory domain. This Active Directory domain resides on a pair of highly available domain controllers within the Production Environment. All resources within the Production Environment are domain-joined, including the VPN concentrator, which requires multi-factor authentication to establish a tunnel. This tunnel only exposes a single jump host, which is also domain-joined.

(J) Maintenance (MA). Rackspace shall coordinate maintenance windows to perform Scheduled Maintenance activities as required for the Cloud Infrastructure components that Rackspace supports. Rackspace shall notify Client of Scheduled Maintenance at least five Business Days before maintenance is scheduled to occur; notification shall be via Client Portal. Scheduled Maintenance may be adjusted by Rackspace up to 24 hours in either direction (before or after the then-current maintenance schedule); however, to the extent Client requires changes to the maintenance schedule, Client shall coordinate such change within 24 hours of Rackspace notification.

On occasion, Emergency Maintenance may be required to maintain a security posture commensurate with the Compliance Baseline. Rackspace is authorized to perform all reasonable actions to meet or exceed requirements in connection with the delivery of the Services against the Compliance Baseline. Rackspace shall make every effort to provide advanced notification to Clients whenever possible, but specific circumstances may dictate immediate action without prior notification.

(K) Media Protection (MP). Rackspace utilizes validated cryptographic mechanisms to encrypt removable storage media within our data centers. All physical media transport outside of the data center is strictly controlled. Unless set forth in a separate agreement, Rackspace shall not accept any Client-furnished storage devices, and Rackspace shall not provide to Client any Rackspace storage devices. All

decommissioned disk drives and digital media are sanitized before physical destruction, in accordance with the Compliance Baseline.

(L) Personnel Security (PS). All Rackspace personnel with physical or logical access to the Cloud Infrastructure shall be U.S. Citizens and undergo pre-employment background checks as part of the on-boarding and application process. An employee's hiring is contingent upon internal investigations, such as background, credit, and reference checks.

If Client requires personnel security approvals or clearances outside of Rackspace's standard background investigation, then Rackspace reserves the right to submit for approval and/or clearance its entire operations and security teams associated with the Services to enable adequate support. Client shall bear the costs and expenses incurred by Rackspace in connection with obtaining approvals or clearances required to allow Rackspace to perform its obligations hereunder.

(M) Physical Environment (PE). Rackspace data centers implement security safeguards to control access to areas within the facility that are officially designated as publicly accessible. Rackspace uses badges for all personnel with access privileges. Rackspace maintains a current list of personnel with authorized access to the areas where the Cloud Infrastructure resides, in addition to maintaining a separate list of personnel with authorized access to the government-only enclave area. The data center floor incorporates badge and biometric access controls, locked and alarmed dual-factor authenticated doors, CCTV, and 24x7 guards to enforce physical access authorizations at all access points. Separate controlled access is required to access a U.S. government-only enclave area of the data center.

Rackspace and Client inherit additional PE controls from AWS.

(N) Risk Assessment (RA).

> **(i) Monthly Vulnerability Scanning**. Rackspace performs monthly vulnerability scanning for each Client's managed OSIs within their environment(s). The scans are performed by Rackspace and the raw, unmodified vulnerability scan results shall be provided to Client. Rackspace and Client shall mutually agree on a monthly scanning schedule for the duration of the services agreement.
>
> Any custom vulnerability scanning activities and associated reporting requested by Clients shall be stated in any applicable Service Order(s), which shall include additional implementation and management fees.

(O) System and Communication Protection (SC). Rackspace separates user functionality from management functionality through physical and logical network segmentation and associated access management policies. The Cloud Infrastructure is separated into at least two security environments: 1) a management environment containing Rackspace's support tools, and 2) Client's Production Environment. Client may implement "non-production" environments. Access to each environment is controlled by a logical firewall. Access to the management environment is limited to only Rackspace personnel. Privileged Users access the Production Environment using multi-factor authentication into a jump host via an encrypted VPN connection. End users of Client's application enter through Client-managed, application-defined mechanisms.

Rackspace provides each Client environment with a network intrusion detection sensor that monitors all network traffic to and from the Client's Production Environment. The sensor monitors all unencrypted traffic for indicators of known potential attacks and potentially malicious traffic, excluding network traffic that is encrypted using transport-layer encryption methods (e.g. HTTPS, SSL, TLS, SSH) which the sensor is unable to decrypt.

> **(i) System Availability**. Appliance availability and failover is accomplished transparently via component resiliency at several levels.

Unless otherwise specified in a Service Order, the AWS Services powering the Production Environment are configured in an N+1 configuration featuring use of multiple AWS Availability Zones (AZs).

(P) System Integrity (SI).

(i) Endpoint Security Management. Rackspace provides a centrally managed endpoint security software platform for all Client OSIs within their environment. The endpoint security management solution provides centralized anti-virus, malware defense**,** and host-based intrusion prevention services. Rackspace provides ongoing management of the management servers**;** agents installed on OSIs**;** and associated configurations, updates**,** and policy management. If a security event is detected, Rackspace shall notify and collaborate with Client to determine the appropriate actions.

(ii) File Integrity Monitoring. Rackspace provides a centrally managed File Integrity Monitoring (FIM) solution that monitors all Client OSIs for file changes. The FIM solution monitors core OSI operating system files, and identifies and reports on changes made to these files. Monitoring the integrity of Client data and/or application files installed by Client on OSIs is excluded from the Rackspace FIM solution monitoring scope of services. Rackspace provides ongoing management of the FIM management servers; agents installed on OSIs; and associated configurations, updates, and policy management. If a FIM event is detected, Rackspace shall notify Client and shall collaborate with Client to determine the appropriate actions.

4. AUDIT SUPPORT SERVICES. Upon at least 30 days of advance written notice, Rackspace can provide up to 60 hours of security audit support services per security audit per 12-month period. Any additional security audit support services required by Client shall be available during Business Hours for $250.00 USD per person, per hour, if booked two or more weeks in advance. For less than two weeks of advance notice, additional security audit services shall be available during Business Hours for $350.00 USD per person, per hour. Additional security audit support services requested outside of Business Hours are available for $450 USD per person, per hour. If the security audit support is performed on behalf of an end client of Client, Client shall give Rackspace direct access to the end client and its auditors.

5. INCIDENT RESPONSE.

5.1. Communication during Incident Management. Client shall assist Rackspace in developing a SEAP that shall define the steps to be taken by Rackspace personnel when responding to incidents, tickets, and alerts.

During the incident management process, Rackspace and Client shall communicate via means designated in the SEAP. Initial communication shall be made based on the timelines defined in the SLAs listed in Section 6.

If incident resolution requires Client cooperation, such cooperation shall not be unreasonably withheld.

Upon incident receipt notification by phone call or Client Portal, Rackspace shall respond to Client via the Client Portal.

Rackspace shall use commercially reasonable efforts to provide the post-incident Client incident report within two Business Days via email.

Client shall designate a primary point of contact to communicate with Rackspace regarding all technical issues that may arise during the term of any Service Orders hereunder, including highlighting the priority and urgency of Client tickets and requests.

5.2. Support Requests. Client shall create tickets within the Rackspace Portal for all support requests, change requests, or incidents. Following the submission of the ticket, Rackspace's response time shall match the agreed-upon severity of the ticket, as described in Section 6.1.

The Client Portal will send an email notification to the requestor/creator of the ticket as well as the approver when a ticket is closed by Rackspace Support personnel.

5.3. Security Incident Response. In the event of a security incident in the Client Infrastructure, such as a denial of service attack, Rackspace reserves the right to suspend Services without notice as necessary (e.g., powering off or network-isolating Client Appliances and OSIs), until completion of remediation.

6. SERVICE LEVEL AGREEMENTS (SLA).

6.1. Initial Incident Response Time SLAs.

Ticket Severity	Severity Definition	Initial Response Time
Sev1	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.	15 minutes
Sev2	Either of the following: (a) 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; **OR** (b) Any other support request not meeting the definition of Severity Level 1.	60 minutes

Client is entitled to a credit of $250 for the failure of Rackspace to meet the Initial Response Time SLAs. The Initial Response Time begins upon the Client Portal system timestamp for submission of a ticket, resulting from a ticket being submitted by either (i) Client or (ii) Rackspace Support through the Rackspace Support phone number.

6.2. AWS Service Level Agreements. Rackspace shall provide Client with credits for the AWS Services purchased through Rackspace pursuant to the applicable AWS Service Level Agreements, provided that Client shall notify Rackspace of any service level requests by the end of the next billing cycle after which the service incident occurred. Client may not go directly to AWS with service level inquiries or requests for remedies. Rackspace shall notify Client of any credits owed under the AWS Service Level Agreements within 60 days of request to Rackspace for such credits, and such credits shall be applied only against future purchases of the AWS Services from Rackspace. Client's sole and exclusive remedy for any unavailability, nonperformance, or other failure by AWS to provide the AWS Services is the receipt of a credit pursuant to the terms of the relevant AWS Service Level Agreements.

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

(A) Scheduled Maintenance or Emergency Maintenance;

(B) Written agreement between Rackspace and Client confirming a change may be implemented without following the Change Control Processes;

(C) Client-initiated work independently generated by Client;

(D) Client support requests not submitted through the Client Portal nor Rackspace Support phoneline;

(E) Service interruptions requested by Client;

(F) Violations of Rackspace's Acceptable Use Policy as may be updated from time to time at www.rackspace.com/information/legal/aup.php;

(G) Client-required OSI revisions and hardware/software configurations that are not Rackspace tested/approved;

(H) Client-created rules, objects, functional configuration errors, third-party software configuration, or other failure of Client Appliances, software, or hardware, or third-party software or hardware;

(I) Force majeure events;

(J) DNS issues outside the direct control of Rackspace;

(K) Patches or antivirus updates which contain code faults, flaws, or other errors attributable to the third-party vendors that created such code;

(L) Any suspension of the Services pursuant to the terms of the Agreement;

(M) A DoS attack or distributed denial-of-service attack (DDoS attack);

(N) Any actions or inactions of Client, an end user, or any third-party;

(O) Client's equipment, software, or other technology and/or third-party equipment, software, or other technology (other than third-party equipment within Rackspace's direct control);

(P) Client's failure to request SLA credits within 30 days of the applicable month for which Services are invoiced; or

(Q) Manufacturer or safety code-related shutdowns required for safety compliance.

6.4. Service Level Credit Limitations. The SLA credit remedies contained in this Section 6 are Rackspace's sole and exclusive liability and Client's sole and exclusive remedy for any failure of Rackspace to meet an SLA. The total credit available to Client for all SLA failures in any particular calendar month shall in no event exceed the monthly Fee for the environment in which the SLA failure occurred during that invoiced month. Any credits available to Client shall be applied to Fees due from Client and shall not be paid to Client as a refund, unless such credit pertains to the last month of Client's service.