CMMC - Cloud Provider Addendum
AWS GOVCLOUD (US) SERVICES

In addition to any other terms and conditions of Customer's Agreement with Rackspace, this Cloud Provider Addendum ("**Addendum**") shall apply when Customer purchases AWS GovCloud (US) Services ("**AWS GovGloud**" or, as used herein, the "**Services**").

1. ADDITIONAL DEFINED TERMS.

"**Add-On Service**" means an additional product or service purchased by Customer from Rackspace to enhance, add to, or modify specific, identifiable Services or deliverables.

"**Applicable Data Protection Law**" means all applicable laws, rules, regulations, orders, ordinances, regulatory guidance, and industry self-regulations in relation to data privacy, including but not limited to the EU General Data Protection Regulation ((EU) 2016/679).

"**Authorized Territory**" means the geographic territory within which Customer may purchase and use the AWS Services pursuant to these Services.

"**AWS**" means the contracting Amazon Web Services affiliate entity identified in Customer's AWS Customer Agreement.

"**AWS AUP**" means the policy currently available at http://aws.amazon.com/aup (and any successor or related locations designated by AWS), as it may be updated by AWS from time to time.

"**AWS Account**" means Customer's member account(s) joined via AWS Organizations to Rackspace's designated AWS management account.

"**AWS Content**" means content that AWS or any of its Affiliates makes available in connection with the AWS Services or on the AWS Site to allow access to and use of the Services, including APIs; WSDLs; sample code; software libraries; command line tools; proofs of concept, templates, and other related technology (including but not limited to any of the foregoing that are provided by any AWS personnel). AWS Content does not include the Services or Third-Party Content.

"**AWS Privacy Policy**" means the privacy policy currently referenced at http://aws.amazon.com/privacy (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

"**AWS Services**" means the web services made available by AWS for Rackspace to resell.

"**AWS Service Terms**" means the rights and restrictions for particular AWS Services located at http://aws.amazon.com/serviceterms (and any successor or related locations designated by AWS), as may be 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.

"**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 Terms of Use**" means the rights and restrictions for particular services located at http://aws.amazon.com/terms/ (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

© 2025 Rackspace US, Inc. – Global Product Terms – 18 July 2025 Revision – OT# 60291

"**AWS Trademark Use Guidelines**" means the guidelines and trademark license located at http://aws.amazon.com/trademark-guidelines/ (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

"**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 Customer's Service Order(s). This excludes Customer Appliances.

"**Controller", "Processor**", "**Data Subject**", "**Personal Data",** and "**Process**" or "**Processing**" shall all have the meanings set out in Applicable Data Protection Law.

"**Covered Environment**" means the Customer servers, per the IP addresses identified in the Services Order.

"**Customer Content**" means content that Customer transfers to AWS for processing, storage, or hosting by the AWS Services in connection with Customer's AWS Account, and any computational results that Customer derive from the foregoing through its use of the AWS Services.

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

"**Customer Submissions"** means content that Customer posts or otherwise submits to developer forums, sample code repositories, public data repositories, community-focused areas of the AWS Site, or any other part of the AWS site that allows third parties to make available software, products, or data.

"**Disaster Declaration"** means the submission by the authorized Customer representative of a ticket via the Customer 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 Customer 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, infrastructure, and/or the network.

"**PII**" means personally identifiable information as defined by the Applicable Data Protection Law.

"**Policies**" means the AWS AUP, AWS Privacy Policy, AWS Terms of Use, AWS Service Terms, AWS Trademark Use Guidelines, all restrictions described in the AWS Content and on the AWS Site, and any other policy or terms referenced in or incorporated into the Agreement, but does not include whitepapers or other marketing materials referenced on the AWS Site.

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

"**Public Sector Access Policy**" means the policy currently available at https://s3-us-west-2.amazonaws.com/solution-provider-program-legal-documents/AWS+Public+Sector+Access+Policy.pdf (and any successor or related locations designated by AWS), as it may be updated by AWS from time to time.

"**Public Sector Customer**" means a Customer 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 Customers (e.g., higher tier prime government contractors) do not constitute Public Sector Customers for purposes of this Agreement.

"**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.

"**Account Management Guidelines**" and "**AMG**" means the Customer 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 AMG.

2. AWS SERVICES.

2.1. Generally. Pursuant to Customer's duly executed Service Order, Rackspace grants Customer a limited, revokable, non-sublicensable, non-transferrable licenses to access and use the AWS Services that Customer has purchased from Rackspace. Rackspace shall provision Customer's AWS account(s) and apply default settings upon provisioning, unless otherwise contracted. The Services will be designed with multi-tenant server, storage, and networking provided by AWS.

2.2. Public Sector Access. If Customer is a Public Sector Customer then it acknowledges that its use of AWS Services is subject to the AWS Public Sector Access Policy. Rackspace is Customer's "Solution Provider" as defined in the Public Sector Access Policy, and Customer is the "Customer" as defined in the Public Sector Access Policy.

2.3. 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), Customer hereby authorizes Rackspace to accept such terms on Customer's behalf, agrees to be bound by and adhere to such terms, and acknowledges that Customer, and not Rackspace are bound by such terms. Customer may request third-party terms via ticket when Rackspace accepts such terms on Customer's behalf.

3. GOVCLOUD (US) SERVICES.

3.1. AWS Services for GovCloud (US). Rackspace will support, for Customer's use, all US-based AWS Services within scope of AWS GovCloud (US) authorization, which may be updated by AWS from time to time. Not all services are available in all AWS regions. Rackspace may further limit the included offerings due to compliance and/or functional requirements.

3.2. Provisioning & Management. Rackspace shall provision Customer's AWS GovCloud (US) account(s) in accordance with AWS GovCloud (US) requirements. Rackspace is responsible for implementing and managing the Customer's AWS environment, up through and including the AWS Services for Customer appliances and the OSI layer for all other Customer instances.

3.3. 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 Customer's Production Environment; and provides the maintenance, repair or replacement of all Cloud Infrastructure components of Customer's environment. Customer 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 Customer. Notice of Scheduled Maintenance shall be provided through the Customer Portal.

(B) Capacity Planning. Customer may request alerts when pre-defined thresholds (documented in the AMG) have been reached. These alerts shall proactively notify Customer that additional resources may be required to support their workloads. All requests for additional resources shall be made in writing, either via the Customer 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.

(D) 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.

(E) Hardening. Rackspace hardens OSIs (Red Hat Enterprise Linux and Microsoft Windows Server only) and network devices to its configuration baseline. Prior to Customer environment deployment and configuration, Rackspace shall communicate the benchmark version to be implemented and managed. Any Customer-defined hardening requirements in addition to, or in lieu of, the Rackspace 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.

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

(G) 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.

(H) Backups. Rackspace configures AWS-native image-based backups of Production Environment OSIs and Customer Appliances once per day. If file-level, database-level, or otherwise application-aware backups are required, Customer 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 Customer 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. Customer 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. Customer may choose to replace the existing disk or mount as an additional disk; but all file-level, application or database recovery efforts are Customer's responsibility.

3.4. Managed Security Services.

(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.

(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) 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 Customer 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. Customer 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. Customer may purchase additional Services to store their logs. Customer retains all responsibility for configuration and management of these additional log sources.

(D) Configuration Management (CM). Rackspace follows change and configuration management procedures. As part of Rackspace's configuration management process, all proposed changes are recorded and analyzed for impact, and any Customer-impacting changes are coordinated with Customer. 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 Customer-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.

(E) Disaster Recovery. Rackspace provides replication of Customer Production Environment OSIs and Customer Appliances to a Disaster Recovery Site to enable the ability to meet a Recovery Point Objective and Recovery Time Objective. 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 AMG. 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 Customer 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 Customer Production Environment are the responsibility of Customer. Alternatively, Customer 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 Customer responsibility, outside of the scope of the base Services configuration, and would typically require application-level support.

(F) Identification and Authentication (IA). Rackspace provides a Customer-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.

(G) 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 Customer of Scheduled Maintenance at least five Business Days before maintenance is scheduled to occur; notification shall be via Customer 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 Customer requires changes to the maintenance schedule, Customer shall coordinate such change within 24 hours of Rackspace notification. On occasion, Emergency Maintenance

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

(H) 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) Customer's Production Environment. Customer 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 Customer's application enter through Customer-managed, application-defined mechanisms. Rackspace provides each Customer environment with a network intrusion detection sensor that monitors all network traffic to and from the Customer'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).

(J) System Integrity (SI).

(i) Endpoint Security Management. Rackspace provides a centrally managed endpoint security software platform for all Customer 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 Customer to determine the appropriate actions.

(ii) File Integrity Monitoring. Rackspace provides a centrally managed File Integrity Monitoring (FIM) solution that monitors all Customer 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 Customer data and/or application files installed by Customer 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 Customer and shall collaborate with Customer to determine the appropriate actions.

3.5. Disaster Recovery Testing. If optionally purchased by Customer, Rackspace shall provide one Disaster Recovery Test per year, upon Customer 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.

4. AUTHORIZED TERRITORY. Customer may purchase and use the Services in the Authorized Territory that corresponds to the Rackspace entity with which Customer contracts, identified in the table below:

Rackspace Entity	Authorized Territory for Public Sector Resell
Rackspace US, Inc.	United States
Rackspace Government Solutions, Inc.	United States

Rackspace International GmbH	Australia, European Economic Area, and United Kingdom

5. CUSTOMER RESTRICTIONS, WARRANTIES & OBLIGATIONS.

5.1. AWS GovCloud (US) Region Representations & Warranties. If Customer purchases AWS GovCloud (US), Customer represents and warrants the following: (1) Customer acknowledges that AWS Services may not be used to process, or store classified data, (2) Customer shall verify that all its end users accessing Customer Content in the AWS GovCloud (US) Region are eligible to gain access to such Customer Content, (3) each Customer end user provided access credentials to the AWS GovCloud (US) Region is a U.S. Person, as defined by 22 CFR part 120.15 ("U.S. Person"); (4) Customer will only assign a U.S. Person as an account owner for the AWS GovCloud (US) Region; (5) if required by the International Traffic In Arms Regulations ("ITAR"), Customer will have and will maintain a valid Directorate of Defense Trade Controls registration; (6) No Customer entity is subject to export restrictions under U.S. export control laws and regulations (e.g., neither any Customer entity nor any end user with access to the AWS Services are denied or debarred party or otherwise subject to sanctions); and (7) Customer shall maintain an effective compliance program to ensure compliance with applicable U.S. export control laws and regulations, including the ITAR. If requested, Customer agrees to provide additional documentation and cooperation to the extent deemed necessary by Rackspace and/or AWS or by any legal, governmental, or regulatory authority to verify the accuracy of the foregoing representations and warranties.

5.2. Multi-Factor Authentication. Customer must enable multi-factor authentication for all AWS Account root users prior to Rackspace providing support to Customer pursuant to this Addendum.

5.3. Services Resale. Customer is prohibited from reselling the AWS Services. Customer is prohibited from selling, transferring, providing, or sublicensing Customer's Rackspace or AWS Account credentials and/or private keys to any other party (except for providing access to agents and subcontractors performing work on Customer's behalf).

5.4. Default Configurations. Rackspace's obligation to provide these Services, including any Add-on Services, is contingent on Customer retaining the default account settings applied by Rackspace, and meeting any Rackspace Configuration Requirements provided to Customer from time to time in the Service Order, product documentation, or otherwise communicated to Customer in writing.

5.5. Customer Content. Customer will ensure that Customer Content and Customer Submissions, and Customer's use of the AWS Services, will not violate any of the Policies or applicable law. Customer is solely responsible for the development, content, operation, maintenance, and use of Customer Content and Customer Submissions.

5.6. Security & Backup. Unless otherwise provided elsewhere in the Agreement, Customer is solely responsible for (a) properly configuring and using the AWS Services in a manner that will provide appropriate security and protection of its AWS Accounts, and (b) providing appropriate security, protection, and backup of the Customer Content.

6. CHANGES.

6.1. To Service Offerings. AWS may change or discontinue any of the AWS Services or change or remove any functionality of any or all of the AWS Services from time to time. Rackspace will endeavor to provide Customer with notice prior to any such changes, provided Rackspace has been notified by AWS of such changes or discontinuations. Notwithstanding the foregoing, AWS is not obligated to provide notice, and Rackspace will have no obligation to provide notice if the discontinuation is necessary to address an emergency or threat to the security or integrity of AWS, respond to claims, litigation, or loss of license rights related to third-party intellectual property rights, or comply with the law or request of a government entity.

6.2. To APIs. AWS may change or discontinue any APIs for the AWS Services from time to time. Rackspace will endeavor to provide Customer with notice prior to any such changes, provided Rackspace has been notified by AWS of such changes or discontinuations. AWS may continue supporting the previous version of such API for 12 months after the change or discontinuation, except if doing so would pose a security or intellectual property issue, is technically infeasible, or would prevent AWS from complying with the law or requests of government entities.

7. PRIVACY & SECURITY.

7.1. Information About Customer. To provide to Customer a license for the AWS Services and help Customer to provision its AWS Account(s), Rackspace may provide AWS the following information on a monthly basis: (i) Customer name and contact information (including customer name, telephone number, email address, city, state/region, country and zip/postal code), and (ii) Customer's AWS account ID associated with Rackspace's reseller account. Customer consents to Rackspace's collection, use, and disclosure of this information associated with the AWS GovCloud (US) Services in accordance with Rackspace's Privacy Statement (available at http://www.rackspace.com/information/legal/privacycenter/, as such may be updated by Rackspace from time to time). If the AWS Services include one or more third party solutions, AWS may disclose, among other things, Customer's name, city, state/region, country and zip/postal code and information associated with Customer's use of the Services. Information obtained by AWS is subject to the applicable AWS Privacy Policy.

7.2. AWS Security Standards. AWS maintains certain security standards, detailed in Exhibit A to this Addendum, which may change from time to time. The information provided in Exhibit A is provided for informational purposes only and does not constitute a condition, representation, or warranty on behalf of AWS.

7.3. Customer Data. When using the AWS Services, Customer agrees that Customer is the Controller and primary Processor of Customer Data. Customer consents to the processing of Customer Data in, and the transfer of Customer Data into, the AWS regions selected by Customer. Customer may specify the AWS regions in which Customer Data will be stored and accessible by Customer and its end users. Rackspace will not move Customer Data from Customer's selected AWS regions without Customer's explicit instruction and without notifying Customer, unless required to comply with the law or a binding order of a governmental body. Processing of Customer Data is subject to the Agreement.

8. DISCLAIMERS.

8.1. Warranty Disclaimer. Notwithstanding anything to the contrary, Rackspace makes no express or implied warranty, condition, or representation on behalf of its Representatives under the Agreement (including this Addendum), and to the extent any language may be construed as a warranty, condition, or representation, it is hereby disclaimed.

8.2. Rackspace Customer. Customer is a customer of Rackspace and has no direct relationship AWS pursuant to this Addendum. AWS does not provide any support or service directly to Customer pursuant to this Addendum, unless Customer has a separate agreement with AWS obligating AWS to provide support or services.

8.3. AWS Services. Customer releases Rackspace from any and all liability whatsoever arising out of or in connection with the AWS Services, AWS's provision, management, or operation of the AWS Services. Notwithstanding anything to the contrary, for the purpose of calculating Rackspace's liability under the Agreement, AWS Services are excluded from the definition of "Services," and Fees for AWS Services are excluded from any limitation on damages calculation.

8.4. Safe Harbor. Notwithstanding anything in the Agreement to the contrary, Rackspace may change the terms of this Agreement at any time, effective immediately, as required to comply with the reseller agreement between AWS and Rackspace or in response to changes made by AWS to the reseller agreement between AWS and Rackspace. Additionally, Rackspace may immediately terminate any applicable Service Order, the

Agreement (if necessary), and/or Customer's AWS Accounts if Rackspace or AWS determine such termination is necessary to comply with the law or if AWS no longer permits resale of one or more of the AWS Service to Customer. If Rackspace terminates Customer's Services in accordance with this section, then both Rackspace and Customer shall reasonably cooperate to develop a transition plan, and Rackspace shall, without undue delay, provide Customer's name, contact information and the AWS Account ID to AWS, to facilitate a smooth transition of Customer's AWS Accounts, if applicable, pursuant to any established transition plan. Rackspace shall use commercially reasonable efforts to provide Customer advance notice of any termination or modification made pursuant to this section.

9. FEES. Rackspace shall charge Customer the current AWS pay-as-you-go rates for Customer's use of the AWS Services purchased from Rackspace, Fees for any AWS Marketplace purchases, and applicable service Fees (collectively, "Monthly Services Fee"). Rackspace shall obtain Customer's AWS usage and billing information directly from Customer's AWS Account, and Customer shall assist Rackspace as reasonably required to gain access to such information. Customer will be responsible for all Fees and charges accrued under Customer's AWS Accounts (including AWS Marketplace purchases), regardless of whether such Fees and/or charges accrued before or after the date of transfer to or from Rackspace. Notwithstanding anything to the contrary in the Master Services Agreement, in the event of a Third Party Fee Increase by AWS, Rackspace may also increase Customer's Fees by the same percentage amount on 30 days advance written notice.

10. TERM. The Initial Term of the Services will be as defined in, and commence upon Customer's signature of, the applicable Service Order. Upon expiration of the Initial Term, the Services will renew for consecutive, rolling 30-day terms 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 30 days prior to the expiration of the then current term.

11. SUSPENSION.

11.1. Generally. Rackspace may suspend Customer's or its end user's right to access or use any portion of or all of these Services immediately, upon notice to Customer, if it reasonably believes:

(A) Customer or its end user's use of the AWS Services (i) pose a security risk to the Services or any third party, (ii) risk adversely impacting Rackspace's or AWS's systems, the Services, or the systems or content of any other Rackspace or AWS customer, or (iii) risk subjecting Rackspace, its Affiliates, or Representatives to liability; or

(B) Customer or any End User is not in compliance with the AWS AUP or is in violation of the proprietary rights of Rackspace, its Affiliates, or Representatives.

11.2. Limitations. In the event a suspension is initiated, Rackspace will work with AWS to ensure AWS will, to the extent practicable, (i) only suspend Customer's right to access or use those instances, data, or portions of the AWS Services that caused the suspension and (ii) limit suspension to those AWS Accounts that caused the suspension.

11.3. Customer Responsibilities. Customer remains responsible for all Fees and charges incurred for these Services during the period of suspension. Customer is not entitled to any service credits under any SLAs for any period of suspension.

12. TERMINATION.

12.1. Notice Requirements. Upon termination of these Services, Rackspace will no longer be the reseller of Customer's AWS Services and, provided Customer is still permitted to consume AWS Services, Customer must elect to either: (i) transfer ownership of its AWS Accounts to AWS, or (ii) close Customer's AWS Accounts. Such election shall be made at the time Customer provides notice of termination. If Customer failure to make such election as herein required, then Rackspace may close Customer's account on the effective date of

termination without liability (e.g., for any lost Customer Data or account credentials). Customer's notice of termination must be in compliance with the terms of the Agreement and must include the effective date of termination for these Services.

12.2. Transitions Assistance. Rackspace will provide reasonable assistance, subject to Rackspace's then current availability and rates, in transferring Customer's AWS Account credentials and/or Customer Data stored in the AWS Services. Rackspace will make reasonable efforts to perform such additional services within 90 days of Customer's notice of termination. If Customer and Rackspace do not agree on a transition plan within a reasonable time period of time following Customer's notice of termination, then Rackspace may immediately close Customer's account on the effective date of termination without liability (e.g., for any lost Customer Data or account credentials). Customer remains responsible for all Fees and charges incurred by Customer through the date of termination.

13. INCIDENT RESPONSE.

13.1. Communication during Incident Management. Customer shall reasonably cooperate as requested, to develop the AMG that shall define the steps to be taken by Rackspace personnel when responding to incidents, tickets, and alerts.

(A) During the incident management process, Rackspace and Customer shall communicate via means designated in the AMG. Initial communication shall be made based on the timelines defined in the SLAs listed in section X(14).

(B) If incident resolution requires Customer cooperation, such cooperation shall not be unreasonably withheld.

(C) Upon incident receipt notification by phone call or Customer Portal, Rackspace shall respond to Customer via the Customer Portal.

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

(E) Customer 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 Customer tickets and requests.

13.2. Support Requests. Customer 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 X(14). The Customer 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.

13.3. Security Incident Response. In the event of a security incident in the Customer 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 Customer Appliances and OSIs), until completion of remediation.

14. SERVICE LEVEL AGREEMENTS (SLAs). All support requests shall be made directly to Rackspace, and Rackspace shall escalate to AWS directly, if needed. This section does not apply to requests made to AWS.

14.1. Initial Incident Response Time SLAs Table.

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	15 minutes

	that Customer cannot continue to operate its business due to the severity of the outage.	
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 Customer 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

14.2. Credit Remedy. Customer is eligible for a credit of $250 per incident for Rackspace's failure to meet the Initial Response Time SLAs listed in section 14.1. The Initial Response Time begins upon Rackspace's receipt of Customer's support request resulting from a ticket being submitted by either Customer or Rackspace support through the Customer Portal.

14.3. Exceptions to the Credit Process. Credit shall not be issued due to failures that are, as determined by Rackspace, in its reasonable judgment, the result of: (A) Scheduled Maintenance or Emergency Maintenance; (B) Written agreement between Rackspace and Customer confirming implementation of a change or modification; (C) Customer independent actions; (D) Customer support requests not submitted through the Customer Portal; (E) Service interruptions initiated by Customer; (F) Violations of Rackspace's AUP; (G) Customer-required OSI revisions and hardware/software configurations that are not Rackspace tested/approved; (H) Customer-created rules, objects, functional configuration errors, third-party software configuration, or other failure of Customer Appliances, software, or hardware, or third-party software or hardware; (I) Force majeure events; (J) 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 Customer, an end user, or any third-party; (O) Customer'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) Customer'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.

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

EXHIBIT A

AWS SECURITY STANDARDS

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the applicable AWS Enterprise Customer Agreement. AWS represents the following AWS Security Standards to Rackspace, and they are provided here for Customer's awareness. Nothing in this Exhibit A shall be construed as a representation, warranty, or condition made on behalf of AWS.

"**AWS Network**" means AWS's data center facilities, servers, networking equipment, and host software systems (e.g., virtual firewalls) that are within AWS's control and are used to provide the AWS Services.

1. Information Security Program. AWS will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) satisfy the Security Objectives, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the AWS Network, and (c) minimize security risks, including through risk assessment and regular testing. AWS will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

1.1. Network Security. The AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incident response plans to respond to potential security threats.

1.2. Physical Security.

(A) Physical Access Controls. Physical components of the AWS Network are housed in nondescript facilities (the "Facilities"). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.

(B) Limited Employee and Contractor Access. AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its affiliates.

(C) Physical Security Protections. All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

2. Continued Evaluation. AWS will conduct periodic reviews of the security of its AWS Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. AWS will continually evaluate the security of its AWS Network and associated Services to determine whether

additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.