Rackspace Government Services (RGS)

Cybersecurity Maturity Model Certification (CMMC) PRODUCT TERMS

In addition to any other terms and conditions of Customer's Agreement with Rackspace, these Product Terms (and the applicable Cloud Provider Addendum), shall apply when Customer purchases the Cybersecurity Maturity Model Certification (CMMC) Computing Services, at each of the respective tiers, CMMC Launchpad, CMMC Ignition and CMMC Liftoff, as described herein (collectively, "**CMMC Services**" or, as used herein, the "**Services**"). In the event of conflict, the applicable Cloud Provider Addendum shall prevail over these Product Terms.

1. ADDITIONAL DEFINED TERMS.

"Audit Services Hours" Hours allocated for Audit Support Services per calendar year, subject to twelve (12) month order commitment, as indicated in the Service Order.

"**Audit Support Services**" or "**Audit Services**" means the security and compliance, advisory and consulting services provided and reports generated at either a quarterly (i.e., four quarterly scans and reports) or monthly basis (i.e., twelve scans and reports), as indicated in the Service Order within scope of this agreement.

"**Authenticated Scans**" means vulnerability scans performed using valid credentials (usernames, passwords, or other authentication methods) to log into the systems being tested.

"AWS" means Amazon Web Services, Inc. or its affiliates.

"AWS GovCloud (US)" or **"AWS GovCloud"** means the isolated AWS Regions, physically and logically administered exclusively by U.S. citizens to support compliance frameworks such as FedRAMP High, and DoD SRG Impact Levels 4 and 5.

"AWS Solutions" means the third-party cloud computing infrastructure and the related product and services provided by AWS.

"Azure Services" or "Azure Solutions" means the third-party cloud computing infrastructure and the related products and services provided by Microsoft.

"Azure Government" means the dedicated cloud service offering physically isolated datacenters and networks within the U.S. and designed to meet stringent security and compliance requirements for U.S. government agencies (and partners) including FedRAMP High and DoD Impact Level 5.

"Business Hours US" means 8:00 AM to 5:00 PM Central Time, Monday through Friday, excluding federal holidays.

"C3PAO" means a Certified Third-Party Assessor Organization.

"**Cloud Infrastructure"** refers to the (physical or virtual) hardware and software resources within the Cloud Provider Solution, including host servers, switches, firewalls, hypervisor, and Operating System Instances (OSIs).

"Cloud Provider" or "**Third Party Cloud Provider**" means AWS, Microsoft, and/or Google (as defined herein).

"**Cloud Provider Addendum**" means the applicable terms and conditions that govern Customer's access to and use of the Cloud Provider Solution in connection with these CMMC Services as identified in the Service Order.

© 2025 Rackspace US, Inc. – Global Product Terms – 18 September 2025 Revision – OT# 60290

"Cloud Provider Console" means the web-based management interface provided by the Third Party Cloud provider (e.g., AWS Management Console, Azure Portal, or Google Cloud Console) that enables authorized users to access, configure, and manage cloud resources, view logs, monitor services, and perform administrative functions within their cloud environment.

"Cloud Provider Solution" means individually, or collectively, AWS Solutions, Azure Solutions, and/or Google Solutions (as defined herein), as applicable to the Customer's CMMC Services.

"CMMC Ignition" or **"Ignition"** means the Services tier and audit acceleration solution designed to assist Customer with CMMC Level 2 compliance by providing in-scope monitoring, logging reports, and compliance Advisory Services, as further described in section 4.

"CMMC Launchpad" or **"Launchpad"** means the Services tier and compliance-focused and Secure Perimeter cloud solution, designed for operations within AWS Solutions, Azure Solutions and Google Solutions environments while complying with Cybersecurity Maturity Model Certification (CMMC) Level 2 controls, as further described in section 3.

"CMMC Liftoff" or **"Liftoff"** means the Services tier and advanced security and compliance solution, integrating CMMC Launchpad and CMMC Ignition with Identity and Host Management, Patch Management, and Advanced Security Controls, as further described in section 5.

"Covered Environment" means a single Customer Configuration (exclusive of applications), in the Customer's Cloud Provider account which may include AWS Solutions, Azure Solutions, and/or Google Solutions, and supported by the CMMC Services, as set out in the Service Order or otherwise documented by Rackspace during the onboarding phase of the CMMC Services.

"Critical Events" means security incidents that pose an immediate and significant threat to the confidentiality, integrity, or availability of the Covered Environment, including but not limited to active breaches, data exfiltration attempts, or system compromises.

"Customer Portal" means Rackspace's Customer ticketing and/or notification system, used for managing service requests.

"DIBCAC" means a Defense Industrial Base Cybersecurity Assessment Center.

"DISA" means the Defense Information Systems Agency.

"**DoD**" means the United States Department of Defense.

"FCI/CUI" means Federal Contract Information and Controlled Unclassified Information as defined by the Department of Defense.

"Google" means Google, Inc.

"Google Services" or "**Google Solutions**" means the web services provided by Google, including Google Cloud Platform ("**GCP**"), Google Support, and those services identified at: https://cloud.google.com/terms/services.

"Host Management" means the administration and maintenance of physical or virtual servers (hosts), to maintain security, and optimal operation and workload availability, and may include performance and health monitoring, application of updates, and the management of configurations.

"IAM" means Identity and Access Management.

"Identity and Host Management" refers to user and system identity controls, privileged access management, and enforced security configurations for cloud environments.

"Landing Zone Baseline Configuration" means the pre-configured cloud environment deployed by Rackspace comprising network segmentation, IAM policies, security group rules, logging configurations, encryption settings, and foundational security services that collectively establish the minimum security posture required to support CMMC Level 2 or Level 3 workloads within the Customer's Cloud Provider account.

"Microsoft" means Microsoft Corporation.

"Patch Management" means the process of identifying, prioritizing, acquiring, installing, and verifying patches, updates, and upgrades for software and systems for purposes of security, performance, and reliability.

"POA&Ms" means Plans of Action and Milestones as defined by CMMC requirements.

"Secure Perimeter" refers to the set of security controls, policies, and technologies designed to protect cloud-based assets, applications, and data from unauthorized access, cyber threats, and data breaches established by CMMC Launchpad, restricting administrative access while enforcing security and compliance measures.

"Security Benchmark" means the DISA STIGs configuration guidelines. "**DISA STIGs"** means the Defense Information Systems Agency Security Technical Implementation Guides, published by the Department of Defense, as presently located at: https://public.cyber.mil/stigs/ (subject to change to official governmental agency).

"Support Services" means technical assistance provided through Rackspace's ticketing system and phone support channels.

"Support Services Hours" Hours allocated for Support Services per calendar month, subject to twelve (12) month order.

"Supported Operating Systems" means the operating systems identified in the Service Order or as otherwise agreed between the parties in writing.

2. OVERVIEW. Rackspace CMMC Services provide a tiered approach to Cybersecurity Maturity Model Certification readiness through three progressive service levels: (1) Launchpad (secure cloud foundation with managed controls), (2) Ignition (compliance monitoring and audit preparation), and (3) Liftoff (comprehensive security management including identity, patch, and vulnerability services). The Services are delivered across AWS Solutions, Azure Solutions, and/or Google Solutions to support Customer CMMC compliance efforts for the environment covered by this agreement.

3. CMMC LAUNCHPAD. CMMC Launchpad establishes a foundational cloud security solution that provides a CMMC Level 2 compliant Landing Zone by deploying essential security controls, infrastructure configurations, and baseline monitoring capabilities, as further described in this section 3.

3.1. Cloud Security & Compliance Services.

(A) Firewall Management. Rackspace shall deploy and configure firewall services within the Covered Environment according to CMMC Level 2 requirements. Customer may submit configuration requests, within scope of the Services, via the Customer Portal.

(B) Logging and Monitoring Configuration. Rackspace implements initial logging and monitoring of security events, access activities, and system health metrics as required for the initial CMMC Landing Zone Baseline Configuration (which does not include applications).

(C) CMMC Configuration. Rackspace shall deploy and configure services within the Covered Environment according to CMMC Level 2 requirements including intrusion detection, intrusion protection and network segmentation.

(D) Multi-Factor Authentication (MFA). Rackspace shall configure MFA authentication for all administrative access to the Covered Environment, the Customer Portal, and all privileged user accounts within the landing zone.

(E) Identity Access Management (IAM). Rackspace will configure prebuilt IAM roles for Customer to utilize the cloud console functionality.

(F) Configuration Change Management. Customer may request changes to the Covered Environment via the Customer Portal, within scope of the Services. Customer is responsible for ensuring that all requested changes maintain compliance with CMMC Level 2 requirements. Customer may submit configuration requests, within scope of the Services, via the Customer Portal.

(G) Self Service Security Reporting. Customer shall have access to cloud native security and audit logs through the Cloud Infrastructure console provided by Customer's Cloud Provider.

3.2. Deliverables.

(A) Platform Logs. Customer shall have access to platform logs for the Covered Environment through the Cloud Provider console and/or APIs (subject to authorized user permissions).

(B) Customer Portal Access for Support. Customer shall have access to the Rackspace Customer Portal for submitting support requests and viewing ticket status.

(C) Enhanced Cloud Tooling. Customer shall receive access to cloud-native security and compliance tooling access via the cloud console and based off their user roles.

(D) Cloud Console Access. Customer receives full administrative console access, and IAM Roles to the Covered Environment, with permissions specified in the Service Order and subject to Rackspace security policies.

3.3. Customer Enclave Obligations: Following Rackspace's deployment of the initial CMMC Landing Zone, (including network architecture, security groups, and baseline configurations), Customer shall be responsible for all ongoing operational activities, security maintenance, and compliance management within the Covered Environment. Support can be provided for Configuration Change Management per section 3.1(F) with Support Services Hours included in the Service Order. Customer must make available administrative credentials for any Rackspace support.

4. CMMC IGNITION. CMMC Ignition provides an audit accelerator solution that extends CMMC Launchpad by providing Customer with compliance scanning, monitoring, and advisory capabilities to support Customer's management of the Customer Environment in accordance with CMMC Level 2 requirements. As further described in this section 4, these Services consist of: (i) automated compliance scanning and reporting at the Customer-selected schedule (monthly, quarterly, or on-demand) identifying specific areas needing adjustment for compliance with CMMC Level 2 practices; and (ii) Audit Support up to the purchased number of Audit Services Hours.

4.1. Compliance & Security Services.

(A) CMMC Control Reports. Rackspace shall provide detailed documentation mapping implemented technical controls to CMMC Level 2 requirements, including periodic control implementation status reports and evidence packages suitable for CMMC assessment.

(B) CMMC Level 2 Monitoring & Logging. Rackspace shall implement tooling to support compliance-specific CMMC Level 2 requirements, including event correlation for security incidents, and maintain audit trails suitable for assessment evidence.

(C) Audit Support Services. Rackspace shall provide Audit Support Services for CMMC requirements interpretation, gap analysis, remediation recommendations, audit preparation, and control implementation recommendations, scheduled in minimum 30-minute increments.

(D) Security Posture & Compliance Configuration Management. Rackspace, shall, at the request of Customer implement configuration changes agreed to in section 4.1(C) in support of Customer's CMMC Level 2 compliance. These changes will be delivered via Support Services Hours.

4.2. Deliverables.

(A) Vulnerability and Security Scanning. Automated cloud native vulnerability scans shall be performed at the frequency specified in the Service Order (monthly, or quarterly), using Authenticated Scans of the Covered Environment with detailed findings and remediation guidance to be delivered to Customer via the Customer Portal.

(B) Enhanced Audit Reports. Security reports to support auditing shall consist of summaries, vulnerability findings, user access audits, configuration change tracking, and compliance metrics, delivered via the Customer Portal quarterly (i.e., four quarterly scans and reports) or monthly basis (i.e., twelve scans and reports), as indicated in the Service Order within scope of this agreement.

(C) Annual Allocation of Audit Support Services. 30 hours will be available to Customer as described in this agreement. These hours are reset on the first day of the annual renewal date and any unused hours are not carried over.

(D) Inclusive of Launchpad. All Services and Deliverables from section 3.1 and section 3.2 are included in CMMC Ignition.

5. CMMC LIFTOFF. CMMC Liftoff extends beyond Ignition by providing identity management, automated patch management, and enhanced security monitoring capabilities aligned with CMMC Level 2 requirements, as further described in this section 5.

5.1. Security & Compliance Services.

(A) Identity and Host Management. Rackspace shall: (i) deploy and manage centralized identity management systems with role-based access control aligned to CMMC Level 2 requirements; (ii) implement privileged access management with user log tracking enabled; (iii) support Customer's access reviews (as reasonably requested); and (iv) support management of identity lifecycle for system accounts. For identity and host management systems deployed under liftoff, only Rackspace shall retain administrative access. Customer will not have administrative access; Customer will have only IAM-defined role-based access to the Covered Environment.

(B) Patch Management. Rackspace shall implement a patch management schedule covering Supported Operating Systems and provide patch compliance reporting within thirty (30) days of patch release by the vendor.

(C) Compliance Posture Management. Rackspace shall perform configuration management on behalf of and in coordination with Customer to maintain the baseline configurations related to CMMC Level 2 compliance posture.

(D) Access Logging and Security Monitoring. Systems deployed by Rackspace shall support logging of all privileged access. Systems shall support security event monitoring.

(E) Critical Event Remediation. Rackspace shall undertake reasonable remediation efforts for Critical Events within the Covered Environment within the scope of the exclusions in section 14. If Customer's Services do not include a disaster recovery environment (or if Customer has not elected disaster recovery

services), remediation options may be limited and regardless of services options, Rackspace does not warrant that remediation can be achieved.

(F) Active Account Hardening. Rackspace shall perform monthly authenticated vulnerability scans within the Covered Environment, implement security hardening based on industry standards, and provide vulnerability reports with remediation recommendations. Rackspace will coordinate the scheduling with Customer for the implementation of the recommendations described in 5.1(C).

5.2. Deliverables.

(A) Enhanced Reporting. Monthly reports including vulnerability scan results with malware detection summaries, patch compliance status, configuration assessments, and security metrics aligned to CMMC Level 2 requirements.

(B) Monthly Allocation of Support Services Hours. Eight monthly hours will be available to Customer as described with these Product Terms. Support Services hours and allocated and consumed as described in section 10.5.

(C) Inclusive of Launchpad & Ignitions. All Services and Deliverables from section 4.1 and section 4.2 (inclusive of the Launchpad services) are included in CMMC Liftoff.

6. ADDITIONAL SUPPORT SERVICES. Any additional Support Services required by Customer above the monthly Support Services Hours included in their Services tier shall be available during Business Hours US for Two Hundred Fifty Dollars ($250.00) per person, per hour, if booked one or more weeks in advance. For less than one week of advance notice, additional services shall be available during Business Hours US for Three Hundred Fifty Dollars ($350.00) per person, per hour. Additional services requested outside of Business Hours US are available for Four Hundred Fifty Dollars ($450.00) per person, per hour. Purchased Support Services Hours may be used at any time and do not expire during the term of the Service Order. All additional Support Services Hours are subject to Service Order or statement of work ordering requirements and minimum one (1) hour billing increments.

7. ADDITIONAL AUDIT SUPPORT SERVICES. Any additional Audit Support Services required by Customer above the monthly Support Services Hours included in their Services tier shall be available during Business Hours US for Two Hundred Fifty Dollars ($250.00) per person, per hour, if booked one or more weeks in advance. For less than one week of advance notice, additional services shall be available during Business Hours US for Three Hundred Fifty Dollars ($350.00) per person, per hour. Additional services requested outside of Business Hours US are available for Four Hundred Fifty Dollars ($450.00) per person, per hour. Purchased Audit Support Services Hours may be used at any time and do not expire during the term of the Service Order. All additional Audit Support Services Hours are subject to Service Order or statement of work ordering requirements and minimum one (1) hour billing increments.

8. RACKSPACE CONFIGURATION REQUIREMENTS. CMMC Services can be purchased to support existing or new Cloud Provider Solutions. Customer shall ensure that any Cloud Provider Solution forming part of the Covered Environment meet the Rackspace Configuration Requirements before CMMC Service commencement. Customers requesting CMMC Services may be required to purchase additional Support Services or Professional Services to conform the Covered Environment to the Rackspace Configuration Requirements.

9. CLOUD PROVIDER TERMS; SUPPORT OBLIGATIONS. Customer use of the Cloud Provider Solution (i.e., AWS Solutions, Azure Solutions, and/or Google Solutions) is subject to and governed by the applicable Cloud Provider Addendum. Customer shall maintain a subscription to Cloud Provider Support, pursuant to the service level or support options required by Rackspace to support the CMMC Services, for the duration of the CMMC Services. (For example: for AWS, the Customer shall maintain Enterprise Support with Rackspace (PLES) or shall independently procure the Developer support tier or higher from AWS).

10. PRICING & PAYMENTS. CMMC Services are offered through a tiered service model with progressive capabilities, services and features that are cumulative across the CMMC offerings (e.g., Customers ordering Liftoff

will receive all the Services of Launchpad and Ignition). Notwithstanding the foregoing, CMMC Ignition can also be purchased as a one-time report (i.e., in addition to the subscription option that can run monthly, quarterly or annually). For the sake of clarity, and notwithstanding the terms in this section 10, Customer acknowledges that its selected Cloud Provider may have different pricing terms, ordering terms and commitments; thus, in the event of conflict, the Cloud Provider Cloud Provider Addendum shall prevail over the terms contained herein.

10.1. Consumption-Based Pricing Model. Each Services tier is based on Customer's infrastructure size, consumption levels, and selected service options as specified in the Service Order. For Customers with infrastructure spend below the threshold specified in the Service Order, Services are provided at a fixed monthly rate. Once Customer's monthly infrastructure consumption exceeds the baseline threshold indicated in the Service Order, pricing transitions to a percentage-based model where fees are calculated as a proportion of total infrastructure spend. The applicable percentage decreases as infrastructure spend increases, with specific tiers and rates as defined in the Service Order. Pricing for all Service components will be in accordance with the then-current rates applicable to CMMC Services, as indicated in Customer's Service Order. Except for pricing changes permissible under the Agreement, Customer pricing shall remain in effect throughout the term, until expiration of the applicable Service Order. Upon renewal, pricing may be increased automatically to the then-current Services rates.

10.2. Services Fees; Base Fees. Customer shall pay a monthly base fee for each subscribed CMMC Services tier, which includes: (i) Configuration and management services for the Covered Environment; (ii) A baseline allocation of Support Services Hours per month; (iii) Security tooling and monitoring capabilities appropriate to the Services tier; and (iv) Access to compliance documentation and reporting features.

10.3. Onboarding and Setup. An onboarding fee may apply based on the complexity of the Covered Environment and implementation requirements, as determined during pre-sales scoping and specified in the Service Order.

10.4. Host Management Fees. For CMMC Liftoff services, Customer shall pay an additional per-host management fee for each virtual machine under active management, as specified in the Service Order.

10.5. Hourly Allocations. For Services that include a monthly allocation of hours (i.e., Support Services Hours and Audit Services Hours), such hours are consumed based on the type and complexity of services requested. Each month’s hourly allocation must be consumed during the applicable month; unused monthly hours do not carry forward and are forfeited.

10.6. Additional CMMC Support Services. Services required beyond the monthly Support Services Hours allocation are available at hourly rates specified in section 6 above, subject to advance notice requirements. Premium services rates and/or Rackspace pre-approval may apply for: (i) expedited services with short notice; and/or (ii) after-hours and emergency support. Except for Services identified and priced within the Service Order pricing schedule, additional Support Services Hours shall be charged at Rackspace's then-current rates.

10.7. Invoicing. Customer's onboarding fees (or other one-time Fees), if applicable, will be invoiced upon execution of the Services Order. For Services fees based on infrastructure, the monthly Services Fee will be invoiced on a monthly recurring basis in arrears, starting from the close of the first month of Services (unless specified otherwise in the Service Order). Fees for CMMC Support Services Hours (or any other ad-hoc services or add-ons) will be invoiced as incurred, or in arrears following the close of the month, when applicable. All Fees are non-refundable and are payable in accordance with the terms of the Agreement.

10.8. Service Scaling. Subject to advance notice of thirty (30) days, Customer may migrate to a higher Services tier effective upon the following billing cycle (subject to reasonable resource availability as notified by Rackspace). Except for Service Orders with a term commitment, subject to advance notice of ninety (90) days, Customer may migrate to a lower Services tier, effective upon the following billing cycle. Rackspace shall co-term the upgraded or downgraded Services to Customer's existing term.

11. TERM & TERMINATION. The Initial Term for CMMC Services shall commence upon execution of the Service Order (or as otherwise expressly stated in the Service Order) and shall continue for the term indicated in the Service Order. Upon expiration of the Initial Term (except as otherwise indicated in the Service Order or Cloud Provider Addendum), CMMC Services will automatically renew for the Auto Renewal Term pursuant to the Agreement.

12. CHANGES TO PRODUCT TERMS. Notwithstanding anything in the Agreement to the contrary, Rackspace may change these Product Terms (and the applicable Cloud Provider Addendum) at any time, effective immediately, in response to: (i) CMMC regulatory changes or other changes to applicable law; (ii) changes made to any third party supplier product or services upon which these Services depend; or (iii) security enhancements or operational changes to the Services which are generally applicable to all CMMC Services customers, or which are required (in Rackspace's reasonable determination) for the ongoing performance or proper functioning of the Services. Customer will be notified of significant changes impacting their use of the Services.

13. GLOBAL CUSTOMER OBLIGATIONS.

13.1. General Assistance. Customer shall: (i) provide Rackspace in a timely manner with all required cooperation and complete and accurate information as reasonably requested to set up, maintain and manage the Services; (ii) designate primary and additional points of contact, identify authorized personnel and access requirements, and provide escalation procedures; (iii) ensure designated personnel are adequately qualified and participate in Services meetings; (iv) coordinate maintenance windows for affected systems; (v) remain responsible for its own data and applications and support of its end users (or end customers) and third parties except as expressly stated within Services scope; (vi) promptly provide required approvals, consents, and feedback to facilitate Services delivery; and (vii) comply with all applicable data privacy laws and use secure methods when transferring personally identifiable information to Rackspace.

13.2. Systems and Access. Customer shall provide Rackspace with all access credentials and facilitate access to all accounts, systems, and provide all technical assistance, documentation, and configuration data as required. Additionally, Customer shall ensure that its contact information remains current. If Customer fails to provide required information within three Business Days of written request, Rackspace may suspend Services performance which shall not relieve Customer's payment obligations.

13.3. Information Requirements. Customer shall provide timely, accurate, and pertinent information regarding the Customer Environment, including network diagrams, asset inventories, data flow diagrams identifying Federal Contract Information/Controlled Unclassified Information (FCI/CUI) locations and paths, existing policies, procedures, security configurations, personnel roles, and prior assessment results. Customer shall grant necessary and appropriate access to relevant systems, documentation.

13.4. CMMC-Specific Obligations. Customer is solely responsible for: (i) Dedicating sufficient qualified resources for CMMC preparation, implementation, and maintenance; (ii) All decisions regarding cybersecurity posture, risk tolerance, CMMC requirements interpretation, security controls selection, and compliance strategy; (iii) Designing, implementing, configuring, testing, managing, and maintaining all security controls and practices required for CMMC Requirements, except activities explicitly included in Services scope per section 3 through section 5; (iv) C3PAO or DIBCAC selection, contracting, scheduling, and payment for formal CMMC assessments; (v) Conducting accurate self-assessments and annual affirmations where CMMC permits; (vi) Developing, managing, and closing Plans of Action and Milestones (POA&Ms) per CMMC rules, including meeting one hundred eighty (180) -day deadlines and obtaining required validations; (vii) Maintaining stable operational environments during Rackspace assessment activities; (viii) Ensuring third-party supplier and subcontractor CMMC compliance.

13.5. Performance Dependencies. Customer acknowledges that Rackspace's Services performance is contingent upon Customer meeting these obligations. Rackspace shall not be liable for any failure, delay or substandard performance caused by Customer non-compliance and may invoice Customer for additional costs resulting from Customer's non-performance. Customer agrees that any damages arising from Customer's failure to meet its obligations constitute damages that "could have been avoided by the damaged party's use of reasonable diligence" per the Agreement.

14. LIMITATIONS, EXCLUSIONS & DISCLAIMERS.

14.1. Services Exclusions. The Services expressly EXCLUDE: (i) Remediation Activities. For Launchpad and Ignition Services: performing remediation activities including implementing security controls, configuring systems, installing patches, or modifying policies except as explicitly described in section 3 through section 5 (or as otherwise per Support Services Hours purchased by Customer). Notwithstanding, for Liftoff Services: such activities are included only to the extent explicitly described in section 5; (ii) Management and Monitoring. Managing, monitoring, or operating Customer Environment components beyond the scope explicitly described in section 3 through section 5 for the applicable Services tier; (iii) Certification Guarantee. Guaranteeing Customer will achieve any CMMC Level or Certification or pass any assessment; (iv) Assessment Services. Acting as or performing C3PAO or DIBCAC assessor functions. Rackspace maintains independence from formal assessment processes; (v) Decision Making. Making final decisions regarding risk acceptance, control priorities, policy adoption, resource allocation, or compliance strategy; (vi) Legal Services. Providing legal advice or interpretations. Customer must obtain independent legal counsel; (vii) Supply Chain Compliance. Ensuring third-party vendor CMMC compliance; (viii) Assessment Interface. Direct interface with DoD, CMMC Accreditation Body (Cyber AB), C3PAOs, or DIBCAC during formal assessments except limited observational support if expressly agreed; (ix) Security Services. Continuous monitoring, incident response, or managed security services unless included in selected Services tier or contracted separately; and (x) Platform Certification. Certifying Customer's specific platform use meets CMMC Requirements. Platform compliance depends on Customer's configuration and management.

14.2. Liability Limitations. Customer agrees that any claims arising from these Services shall be subject to the liability limitations in the Agreement, and that such matters constitute services for which warranties are disclaimed pursuant to the Agreement.

14.3. General Disclaimer. EXCEPT FOR EXPRESS WARRANTIES HEREIN, SERVICES AND DELIVERABLES PROVIDED "AS IS" AND "AS AVAILABLE." RACKSPACE DISCLAIMS ALL OTHER WARRANTIES (EXPRESS, IMPLIED, STATUTORY) INCLUDING MERCHANTABILITY, FITNESS FOR PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, AND WARRANTIES FROM COURSE OF DEALING.

14.4. No Certification Guarantee. RACKSPACE DOES NOT WARRANT OR GUARANTEE CUSTOMER WILL ACHIEVE OR MAINTAIN CMMC CERTIFICATION OR COMPLIANCE. ACHIEVEMENT DEPENDS ON FACTORS OUTSIDE RACKSPACE'S CONTROL INCLUDING: (I) CUSTOMER INFORMATION TIMELINESS AND ACCURACY; (II) RESOURCE DEDICATION; (III) CUSTOMER'S IMPLEMENTATION EFFECTIVENESS; (IV) ASSESSOR INTERPRETATIONS AND METHODOLOGIES; (V) THIRD-PARTY ACTIONS; (VI) REQUIREMENTS INTERPRETATIONS DURING ASSESSMENT. THE PARTIES ACKNOWLEDGE THAT THE LIMITATIONS OF LIABILITY IN THE AGREEMENT APPLY TO ALL CLAIMS RELATED TO CMMC CERTIFICATION FAILURES, LOST DOD CONTRACTS, REGULATORY PENALTIES, OR SIMILAR COMPLIANCE-RELATED DAMAGES, WHICH SHALL BE DEEMED CONSEQUENTIAL DAMAGES PER THE AGREEMENT.

15. COMPLIANCE.

15.1. Third-Party Software. With respect to Third-Party Software, Customer may not: (i) transfer Third Party Software interests; (ii) reverse engineer, decompile, or modify; (iii) remove proprietary notices; or (iv) exercise reserved IP rights. Customer must permit removal of Rackspace-only tools. Open-Source Software is subject to applicable licenses which control over Agreement terms. Services become Unsupported if Customer disables required components.

15.2. Intellectual Property. IP transfers contrary to the Master Services Agreement are void unless documented in writing, conspicuously identifying specific rights and fees, and properly executed by the parties.

15.3. Legal Compliance. Customer is responsible for overall compliance with applicable laws, regulations, and contractual obligations including DoD requirements. Customer may not provide access to the Services to any

individual or entity located in a sanctioned or embargoed country, as per applicable compliance laws and regulations.

16. INDEMNIFICATION. Customer's indemnification obligations under the Agreement include any claims arising from or related to: (i) Customer's breach of Agreement or these Product Terms (and the applicable Cloud Provider Addendum); (ii) third-party claims related to Customer's Services use; (iii) Customer's implementation of or reliance on Rackspace recommendations; (iv) C3PAO or DIBCAC assessment claims including disputes regarding findings or outcomes; (v) Customer's legal non-compliance; (vi) unauthorized Services access or use.

17. CASE STUDY AUTHORIZATION. Customer authorizes Rackspace to produce and publish case studies outlining work performed under the Service Order. Customer shall have prior review and approval rights, not to be unreasonably withheld. Rackspace may collect, analyze and use Services usage information for whitepapers, test cases, and documentation. Customer agrees to share contact information and participate in reference calls with prospective customers upon reasonable request.