RACKSPACE PRIVATE CLOUD
GUEST OS / VM MANAGEMENT SERVICES

In addition to any other terms and conditions of Customer's Agreement with Rackspace, these Product Terms shall apply when Customer purchases the Guest OS / VM Management Services, or the Host Protection Services (individually, the "**VM Management Services**" or the "**Host Management Services**" or collectively, as used herein, the "**Services**")

1. ADDITIONAL DEFINED TERMS.

"**Advanced Host Protection**" means the enhanced security services tier for the Supported VMs as further described in section 3.2.

"**Documentation**" means the "Rackspace VM Management for Private Cloud" documentation which identifies the supported platforms and which describes the Services, as may be updated by Rackspace, and as presently found at the following URL: https://docs.rackspace.com/docs/rackspace-vm-management-for-private-cloud#getting-started.

"**Host Protection**" means the basic security services tier for the Supported VMs as further described in section 3.1.

"**Host Protection Services**" means individual and collectively, Hosting Protection and Advanced Host Protection.

"**Service Commencement Date**" means the date Rackspace is provided logical access to the Supported VMs.

"**Sophos Limited**" or "**Sophos**" means the Rackspace supplier and Representative with an office at 1 Bartholomew Lane, London, England, EC2N 2AX.

"**Sophos Terms**" means the Sophos End User Terms of Use available at https://www.sophos.com/en-us/legal/sophos-end-user-terms-of-use (or successor URL as notified by Rackspace).

"**Supported VMs**" means those Virtual Machines which are enrolled in the VM Management Services (including one or more of Managed OS Administration, Managed OS Patching, Managed OS Monitoring, and Anti-Virus License), as may be further described in the Documentation.

2. VM MANAGEMENT SERVICES. As further described in the Documentation, Rackspace provides the following VM Management Services.

2.1. Managed OS Administration. If Customer purchases Managed OS Administration, Rackspace shall assist Customer with routine administrative OS tasks on the Supported VM's.

2.2. Managed OS Patching. If Customer purchases Managed OS Patching, Rackspace shall patch the Supported VM Operating System in accordance with the procedures described in section 5.3, as applicable. While Customer's virtual servers are in an "inactive" status Rackspace shall not install any software updates that Rackspace may have otherwise agreed to install. Rackspace shall update Customer's virtual servers when Customer returns them to "active" status, but there may be a delay of up to 24 hours before the updates initiate. Some OS patches are untested prior to release and installation. Rackspace disclaims all liability to the extent an OS patch causes loss of data or function in the Customer Configuration, or any system connected to or reliant on the Customer Configuration.

2.3. Managed OS Monitoring. If Customer purchases Managed OS Monitoring, Rackspace shall monitor key performance metrics for the operating system (i.e. CPU, RAM, and Disk), and select applications (i.e. process statistics, users, throughput) and databases (i.e. caching, performance, transaction success) on the Supported

© 2025 Rackspace US, Inc. – Global Product Terms – July 14, 2025 Revision – OT# 50181

VM's and shall notify Customer of monitoring alerts within the timeframes described in Section 5.1 (Response Time SLA).

3. HOST PROTECTION SERVICES. If Customer purchases Rackspace Host Protection Services, Rackspace shall provide either Host Protection or Advanced Host Protection based on Customer's selection as follows:

3.1. Host Protection (Basic Tier). Rackspace shall install anti-virus software on the Supported VM and provide automated malware scanning, threat detection, and real-time protection services (as may be further described in the Documentation).

3.2. Advanced Host Protection (Enhanced Tier). In addition to all Host Protection features, Rackspace shall provide the following (as may be further described in the Documentation).

(A) File Integrity Monitoring. File Integrity Monitoring to detect unauthorized changes to files, folders, and registry keys;

(B) Application Control Application. Control for audit trails and application blocking based on Customer-defined policies;

(C) Data Loss Prevention ("DLP"). Data Loss Prevention to monitor and restrict transfer of files containing sensitive data based on Customer-selected templates; and

(D) Threat Alert Dashboard. Access to a Threat Alert Dashboard for security event visibility.

3.3. Service Availability. These Services are available on supported platforms as described in the Documentation. Rackspace reserves the right to allow applications required for routine management tasks, even if such applications would otherwise be blocked by Customer-configured policies.

4. CUSTOMER OBLIGATIONS.

4.1. General Assistance. Customer shall: (i) provide Rackspace in a timely manner, with all required cooperation, and with complete and accurate information, as reasonably requested or required to set up, maintain and manage the Services; (ii) as reasonably required or requested, designate primary or additional and adequately qualified points of contact, identify authorized personnel and access requirements, and provide escalation procedures for support; (iii) coordinate maintenance windows for affected systems with end customers and users, stakeholders and/or third parties; (iv) be responsible for its own data and applications and the support of its end customers and users, stakeholders, or other third parties (except as otherwise expressly stated herein as within scope of the Services); (v) affirmatively and promptly provide (and not unreasonably withhold, delay or condition), agreement, consent, feedback, or similar action to facilitate Services delivery; and (vi) comply with all applicable data privacy laws and regulations and use only secure methods, according to the applicable data privacy laws and regulations, when transferring or otherwise making personal identifiable information available to Rackspace.

4.2. Supported Operating Systems. All Services described herein are limited to operating systems that are currently supported by Rackspace. Operating systems currently supported by Rackspace are those currently listed on the Rackspace Extended Lifecycle Support web-page (presently found at the following URL: https://www.rackspace.com/information/legal/eolterms), as that web-page may be updated from time to time, which have not reached their end of support date.

4.3. Services Management Agent. Customer agrees that Rackspace may install the required tools and service management agents on Customer's Hosted System for purposes of providing the Services and identifying security vulnerabilities. Except as otherwise necessary for the provision of the Services such agents will use only a minimal amount of computing resources and Rackspace shall not use the agents to view or capture Customer Data. The Services will become Unsupported Services if Customer disables or interferes with Rackspace's services management agent(s).

4.4. Advanced Host Protection. Additional Customer obligations are applicable to Advanced Host Protection as follows:

(A) For Application Control. Customer shall review application logs and provide lists of applications to be blocked according to Customer's organizational policies. Rackspace will apply base policies in logging mode, but Customer must request and confirm any application blocking.

(B) For Data Loss Prevention: Customer shall select appropriate DLP templates and regions during the enrollment process. Customer acknowledges that Rackspace will not configure DLP without Customer's explicit template selection, which must exclude any regulated data categories per section X.

(C) All Features. Customer shall monitor the Threat Alert Dashboard regularly and Customer is responsible for any VM performance impacts resulting from the Services.

5. SERVICE LEVEL AGREEMENTS.

5.1. Response Time SLA. Upon receiving a support request related to the Supported VM's, Rackspace shall designate each request according to one the following severity categories:

Severity Level	Example	Initial Response Time
Emergency: Server, or site down	Customer cannot access the server or site from the public Internet.	Within 15 minutes
Urgent: Server or site functioning improperly or at less than optimal performance	Customer's server or site is accessible but in a reduced state (timeouts or slow response)	Within 1 hour
Standard: Non-critical; server or site is functioning normally, but Customer requires information or assistance, wish to schedule maintenance, or any other non-immediate tasks	Customer's site is functioning with acceptable parameters, but Customer requires assistance in loading software or have a help desk-type question	Within 4 hours

5.2. Response Time Remedy. If Rackspace fails to meet an initial response time stated in this section 5.1, Customer is entitled to a credit of US$250 per event, up to 100% of Customer's monthly fee for the affected VM Management Services. The initial response times stated in section 5.1 apply only to requests Customer makes via ticket or telephone. The times in section 5.1 are response times, not resolution times, Rackspace makes no guarantee regarding the time to resolve a request.

5.3. Managed OS Patching. This section 5.3, and the applicable SLA shall apply if Customer purchases Managed OS Patching Services.

(A) Supported Software. The performances and obligations described in this section 5.3 only to vendor supplied and supported OS and application software patches, excluding: (i) software that Rackspace did not provide to Customer as part of Customer's Services, and (ii) Oracle database software (even if provided as part of Customer's Services).

(B) Release. When operating system software vulnerabilities are addressed by a vendor patch, Rackspace shall categorize the patch as either "critical" or "non-critical" in Rackspace's reasonable discretion.

(C) Procedure (Opt In, Opt Out). Non-critical patches shall be applied to Customer's environment on a monthly basis, and critical patches shall be applied on an as-needed basis. Unless otherwise agreed,

Rackspace shall notify Customer via the ticketing system prior to the application of patches. Patches shall generally be applied unless Customer opts out of the patch. If Customer does not want a particular patch applied to Customer's environment, Customer shall notify Rackspace via support ticket reasonably in advance of the patching window. For some patches Rackspace may state in the ticket that Customer must opt into the patch before Rackspace shall apply it, in which case Rackspace shall not apply the patch unless Customer notifies Rackspace via ticket that Customer would like the patch applied.

(D) Untested Patches. At Customer's request Rackspace shall apply patches to Supported VMs prior to the completion of Rackspace's testing, but Rackspace makes no guarantee whatsoever about the impact of applying an untested patch. If Customer would like a patch applied to the environment prior to the time that Rackspace would normally apply a patch, Rackspace shall do so within four hours of the time that Customer open a support ticket requesting the application of the patch.

(E) Alternative Procedure. Rackspace shall not patch pursuant to the procedures described in this section 4.2 if Customer has made other arrangements with Rackspace via support ticket or written agreement.

(F) Remedy. If Rackspace materially fails to apply patches in accordance with the procedures set forth in this section 5.3 (or the procedures stated in Customer's alternative patching procedure, if applicable) and such failure adversely affects the Hosted System, Customer is entitled to a credit of $250 per event, up to 100% of Customer's monthly fee for the VM Management Services.

6. SERVICES LIMITATIONS, RESTRICTIONS & DISCLAIMERS.

6.1. Out of Scope. Rackspace will provide only the Services described in section 2 and section 3, per Customer options in the Service Order. All other services are out of scope, are not included within the Services and are specifically excluded from performance obligations of Rackspace and its Representatives. To the extent of any out-of-scope services that Rackspace may provide, at its sole discretion, such services are deemed Unsupported Services and are provided on an as-is basis, without warranty or liability.

6.2. Host Protection: Scope of Support. Support for Host Protection Services is limited to agent deployment, agent health monitoring, and troubleshooting of the anti-virus and protection features. Support does not include incident response, security incident triage, forensic analysis, or remediation of infected systems beyond the automated actions taken by the anti-virus software. Critical alerts will be notified to Customer based on automated scans, but Customer is responsible for any required remediation actions beyond automated malware removal.

6.3. Host Protection Restrictions. Customer acknowledges and agrees that the Host Protection Services (both tiers) may not be used: (i) for or in connection with safety-critical applications including medical systems, transport management systems, vehicle applications, or power generation applications (including nuclear power); or (ii) to store, process, or protect regulated data of any kind, including but not limited to healthcare data subject to HIPAA, payment card data subject to PCI-DSS, or financial data subject to regulatory requirements.

6.4. Customer Compliance Requirements. Rackspace does not provide compliance certification, and Rackspace makes no representation or warranty as to the compliance readiness of any portion of the Services. Customer acknowledge that compliance readiness is a system wide endeavor, and the compliance readiness of the Services can fail if a single aspect of the environment is not compliant. Customer retains ultimate responsibility for all regulatory requirements and compliance standards.

6.5. Warranty Disclaimer. Rackspace makes no guarantees as to the effectiveness of the Host Protection Services in detecting or preventing all threats, malware, or data loss. Rackspace provides no warranty or representation regarding Third Party Services (including all performances, obligations, services or Deliverables provided by Rackspace Suppliers). Rackspace is not liable for any loss or damage arising from Third Party Services, and Rackspace SLAs do not apply to Third Party Services or any aspect of the Customer

Configuration affected thereby. Customer's sole remedy for any Third Party Services failure is, when permitted by applicable third party terms, to terminate the affected Service and be relieved of payment obligations.

7. COMPLIANCE WITH TERMS.

7.1. Compliance with Sophos Terms. Customer access to and use of the Advanced Host Protection is subject to the Sophos Terms (which will be effective without signature). Customer acknowledges that Sophos is a Rackspace Representative and third-party beneficiary under the Agreement as necessary to exercise its rights and enforce Customer compliance with applicable Sophos Terms.

7.2. Changes to Terms. Notwithstanding anything in the Agreement to the contrary, Rackspace may change these Product Terms at any time, effective immediately in response to: (i) changes to applicable law; (ii) changes made to any Vendor Solutions or Supported Vendor Terms; (iii) operational changes to the Services which are generally effective to Customer at large or which are required (in Rackspace's reasonable determination) for the ongoing performance or proper functioning of the Services.

7.3. SLA Limitations.

(A) Maintenance. Customer is not eligible for a credit remedy if an SLA failure results from Maintenance. "Maintenance" means:

(i) Rackspace Maintenance Windows: modification or repairs to shared infrastructure (such as core routing or switching infrastructure) and fleet management activities (such as firmware updates for Customer's network appliances) that Rackspace has provided notice of at least 72 hours in advance and that occurs during off peak hours in the time zone where the data center is located;

(ii) Scheduled Customer Maintenance: maintenance of the configuration that Customer requests and that Rackspace schedules with Customer in advance (either on a case by case basis, or based on standing instructions), such as hardware or software upgrades, and including periods during which Customer sets or requests an alert suppression on the configuration; and

(iii) Emergency Maintenance: critical unforeseen maintenance needed for the security or performance of the Hosted System or Rackspace's network.

(B) Requests. Customer shall request a credit in writing via a support ticket no later than 14 days following the occurrence of the event giving rise to the credit. Rackspace shall contact Customer within 30 days to approve or reject the claim or to request more information. If the claim is approved, the credits shall be applied to invoices issued after the approval of the credit. Unused credits shall not be refunded. For the purpose of determining the amount of a credit, time periods shall be measured from the time stamp generated by Rackspace's ticket system. Customer may open a support ticket to document the start time for a support request or other incident, or if Customer contacts Rackspace by telephone to request support, Rackspace shall open a ticket for Customer (there may be a delay between the time of the call and the time Rackspace opens a ticket). Credit remedies identified in specific currency amounts are awarded in the amount matching the currency on Customer's invoice.

(C) Exclusions. Customer is not entitled to a credit if Customer is in breach of the Agreement (including Customer's payment obligations to Rackspace) at the time of the occurrence of the event giving rise to the credit. Customer is not entitled to a credit for a failure to meet a SLA which results from denial of service attacks, viruses or malware, hacking attempts, or any other circumstances that are not within Rackspace's control.

8. ORDERING, FEES & VM ENROLLMENT.

8.1. VM Ordering. Customer's quantity of Supported VMs shall be reflected in the Service Order. Customer may increase the quantity of Supported VMs at any time by executing a new Service Order.

8.2. VM Fees. Customer's fees shall be reflected in the Service Order or the Rackspace customer portal (as applicable), and Rackspace may increase the price for the VM Management Services during the Initial Term or any Renewal Term of these Services by up to 3% annually upon written notice to Customer. Such price increase may not occur more than once in any rolling 12 month period. For the sake of clarity, this section provides Rackspace additional rights and does not replace nor supersede those sections regarding Fees contained in Customer's Master Services Agreement.

8.3. VM Enrollment. Customer may enroll or un-enroll Supported VM's in the VM Management Services via the customer portal. The Services shall commence once successfully tagged as enrolled in the Rackspace portal, and Rackspace shall cease providing the Services at Customer's request effective upon Rackspace's processing of Customer's un-enrollment or termination of the Services. Rackspace may cancel VM Management Services for those VMs which do not conform to Rackspace's requirements for the Services, as detailed in the Documentation.

8.4. Host Protection Services: Pricing & Fees. Host Protection Services are priced on a utility basis per Supported VM per month. Fees are calculated based on: (i) the number of Supported VMs enrolled in Host Protection Services during the billing period; and (ii) the tier of Service selected for each VM (Host Protection or Advanced Host Protection) as specified in the Service Order. Billing for Host Protection Services commences on the date of execution of the Service Order for each enrolled Supported VM. Customer may upgrade from Host Protection to Advanced Host Protection, or downgrade from Advanced Host Protection to Host Protection, on a per-VM basis by providing written notice to Rackspace. Such changes will be effective immediately upon Rackspace's processing of the request, and Fees will be adjusted accordingly on a pro-rated basis for the affected VMs. \\

8.5. Host Protection Services: Invoicing & Payment. Fees for Host Protection Services will be invoiced monthly in arrears based on actual usage during the billing period. Usage is calculated by the number of VMs enrolled in each Service tier multiplied by the applicable per-VM rate for the portion of the month such VMs were enrolled. All Fees are non-refundable and are payable in accordance with the terms of the Agreement.