GLOBAL SECURITY & PRIVACY PRACTICES

1. SECURITY PRACTICES. Rackspace is responsible for the security measures set out in the Agreement and shall maintain and implement the following technical and organizational measures in relation to the security of the Customer Configuration.

1.1. Physical Security – Data Centers. The following physical security controls apply to Customer Data residing in data center or office premises either owned or leased by Rackspace or its Affiliates in connection with the provision of Services to Customer (and expressly excludes third party hosting Services):

(A) Servers and devices dedicated to Customer's use as part of the Customer Configuration provided by Rackspace will be located in a controlled access data center (or portion thereof) either operated by or dedicated to use by Rackspace or its Affiliate.

(B) Rackspace operates or audits the use of an electronic access control system which logs access to physical facilities, managed by a professional security guard force in line with Rackspace's current processes.

(C) Access to the raised production floor of the data halls will be restricted to Rackspace employees or its agents who need access for the purpose of providing the Services. Access within data center facilities is in zones and provisioned based on physical access rights required by a given individual. Access to designated "meet me" rooms will be available to customers, subject to data center escort policies.

(D) The data center will be staffed 24/7/365 and will be monitored by video surveillance, recording to a centralized location, and viewed by the onsite security force.

(E) Rackspace limits access to physical facilities to authorized individuals by proximity-based access cards and biometric hand scanners or other approved security authentication methods.

(F) Except as specifically stated in the Agreement, Rackspace will not relocate the Customer Configuration from a Rackspace data center in one country to a data center in another country without Customer's express written permission.

(G) Following the termination of the Agreement or a Customer Configuration, Rackspace will wipe data from those hard drives and storage devices dedicated to Customer use prior to re-use.

1.2. Security Controls Audits & Reporting. Rackspace shall engage qualified third party auditors to perform examinations of its in scope systems and services in accordance with the best practice recommendations of ISO 27001 for the purpose of auditing Rackspace's compliance with SSAE 18 compliance frameworks and the AT 101 compliance framework (based upon select Trust Services Principles); and/or equivalent industry standards. Rackspace's annual SOC report(s), or suitable equivalent standard(s) as specified by Rackspace, is available to Customer upon Customer's request subject to Rackspace's SOC distribution requirements. Not all Rackspace Services are included in the scope of the SOC report(s) or audits described in this section 1.2 (for details, Customer should contact the Rackspace account manager). Rackspace shall be under no obligation to notify or provide Customer with routine security alerts in respect of the Customer Configuration (including pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing, or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers, or similar incidents), except as otherwise specifically set out as part of the Services or Rackspace's express obligations in the Agreement.

1.3. Administrative Controls. The following security controls apply to access to Rackspace accounts which are provided by Rackspace for Customer use.

© 2021 Rackspace US, Inc. – SPP Terms – April 3, 2023 - Revision – OT# 45789

(A) Screening. Rackspace will perform pre-employment background screening of its employees who have access to Customer's account, and is committed to employee supervision, training and management.

(B) Rackspace Access. Rackspace will restrict the use of administrative access codes for Customer's account to its employees and other agents who need the access codes for the purpose of providing the Services. Rackspace personnel who use access codes shall be required to log on using an assigned username and password.

(C) Customer Access. As the primary system and account administrator, Customer is responsible for the management of their account (including creation, change management and termination), and enforcement of related remote working and password controls.

1.4. PCI-DSS. With respect to the security of cardholder data, as that term is defined in the Payment Card Industry-Data Security Standard, which Rackspace may possess or otherwise store, process or transmit on Customer's behalf, Rackspace agrees to provide (i) those physical, technical, and administrative safeguards described in the Agreement and (ii) the Services selected by Customer and described in the Agreement; provided that Customer remains responsible for ensuring all PCI-DSS requirements are met with respect to such cardholder data. Rackspace maintains PCI-DSS Service Provider, or equivalent, accreditation with regards to dedicated hosting Services (excluding managed virtualization services).

1.5. Customer Data.

(A) Customer Data is, and at all times shall remain, Customer's exclusive property. Notwithstanding anything to the contrary in the Agreement, Customer remains the primary system and account administrator and is responsible for the integrity, security, maintenance and appropriate protection of Customer Data including by: (i) selecting, purchasing, and properly configuring appropriate Services; (ii) implementing adequate controls to maintain appropriate security, protection, and deletion of Customer Data (which shall include end-to-end encryption of Sensitive Data in transit and at rest, and logical access measures); (iii) ensuring that Rackspace is not provided with any access to Customer Data (including protected health information), except as otherwise explicitly set out in the Agreement; and (iv) using the data integrity controls to allow Customer to restore the availability of Customer Data in a timely manner (which shall include routine backups and archiving of Customer Data in an environment separate from the Customer Configuration). Rackspace makes available a number of security controls that Customer may elect to purchase as part of the Services. Rackspace will only back up data to the extent purchased by Customer as part of the Services, and stated on a Service Order.

(B) The Services provide Customer with controls that Customer may use to retrieve, correct or delete Customer Data prior to expiry or termination of the Agreement. Customer's access to the Customer Configuration or Customer Data may be restricted during a suspension or following termination of the Services or the Agreement. Customer is responsible for retrieving a copy of Customer Data prior to the termination of the Agreement. Rackspace may delete Customer Data at any time following Agreement termination.

(C) Customer will cooperate with investigation and resolution of outages and security incidents. Rackspace is not responsible to Customer or any third party for unauthorized access to Customer Data or for unauthorized use of the Services, including any losses or damages resulting from such unauthorized access or use, that is that is not solely caused by Rackspace's failure to meet its security obligations under the Agreement.

2. Privacy Practices. If and to the extent that the provision of Services by Rackspace to Customer involves the Processing of Customer Personal Data subject to Applicable Data Protection Law (as each of those terms are defined in the Data Processing Addendum), then the Data Processing Addendum (presently found at the following URL: https://www.rackspace.com/information/legal/GSAdataprocessingaddendum_MC) as periodically updated by Rackspace will form part of this Agreement.