Rackspace 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. The Customer remains the primary system/account administrator and is responsible for the integrity, security, maintenance and appropriate protection of Customer Data by (i) selecting and purchasing appropriate security Services (ii) implementing appropriate encryption and logical access controls and (iii) maintaining appropriate application security controls. Certain Rackspace services are available to help Customers meet these requirements.

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 US, Inc. or a Rackspace affiliate in connection with the provision of Services to the Customer (and expressly excludes third party hosting Services):

1.1.1 Servers and devices dedicated to your 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.

1.1.2 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 its current processes.

1.1.3 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.

1.1.4 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.

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

1.1.6 Except as specifically stated in the Agreement, Rackspace will not relocate the Customer Configuration from a Rackspace date center in one country to a data center in another country without your express written permission.

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

1.2. **Security Controls Audits & Reporting.** Rackspace shall engage qualified third party auditors to perform examinations of its systems and services in accordance with: the best practice recommendations of ISO 27002, for the purpose of auditing Rackspace’s compliance with ISO 27001; SSAE 16 and ISAE 3402 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 the 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 above, for details please contact your account manager.

1.3. **Administrative Controls**

1.3.1 **Screening**. Rackspace will perform pre-employment background screening of its employees who have access to customers' accounts, and is committed to employee supervision, training, and management.

1.3.2 **Rackspace Access**. Rackspace will restrict the use of administrative access codes for customer accounts 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 user name and password.

1.3.3 **Customer Access.** As the primary system administrator, the customer is responsible for the management of their accounts, 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, Rackspace may possess or otherwise store, process or transmit on the Customer's behalf, Rackspace agrees to provide (i) those physical, technical, and administrative safeguards described in the Agreement and (ii) the Services selected by the Customer and described in the Agreement; provided that the 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. **Reports of and Response to Security Breach.** Rackspace will report to you as soon as reasonably practicable in writing and in accordance with applicable law, of a material breach of the security of the Customer Configuration which results in unauthorized access to Customer Data resulting in the destruction, loss, unauthorized disclosure or alteration of Customer Data of which we become aware. Upon request, we will promptly provide to you all relevant information and documentation that we have available to us regarding the Customer Configuration in connection with any such event. Rackspace shall be under no obligation to notify routine security alerts in respect of the Customer Configuration (including without limitation, 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) save as otherwise specifically set out in the Agreement.

1.6. **Customer Data Return.** The Services enable you to retrieve, correct, or delete Customer Data. Depending on your Services, you may not have access to the Customer Configuration or Customer Data during a suspension of Services, or following the termination of the Agreement. You are responsible for retrieving a copy of your Customer Data prior to the termination of the Agreement Rackspace may delete your Customer Data at any time following termination of the Agreement.

2. Privacy Practices

Customer and Rackspace will comply with applicable laws in relation to their collection and processing of any Sensitive Data in the provision and use of the Services.

If and to the extent the EU Directive 95/46/EC or the EU General Data Protection Regulation (EU) 2016/679 (together with any transposing, implementing or supplemental legislation "GDPR") applies to the processing Personal Data (as defined therein): (a) Rackspace will

process Personal Data only in accordance with Customer's instructions except as required by applicable law, and Customer acknowledges that this Agreement, together with Customer's configuration and use of the Services represents its complete instructions to Rackspace on the processing of such Personal Data, and (b) the Data Protection Addendum available at https://www.rackspace.com/information/legal/GSAdataprocessingaddendum_MC will form part of this Agreement.

Rackspace US, Inc. and certain of its Affiliates participate and have certified compliance with the Swiss-U.S. Privacy Shield Frameworks ("Swiss Privacy Shield"), as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of Personal Data transferred from Switzerland to the United States. Rackspace Affiliates have entered into intra-group standard contractual clauses ("Model Clauses") notified to the Swiss data protection authority (available at https://www.rackspace.com/information/legal/IntracompanyDataProcessingAgreement); and Model Clauses or equivalent data processing agreements with subcontractors processing Personal Data outside of the EU.