RACKSPACE TECHNICAL AND ORGANIZATIONAL MEASURES

In addition to any security measures set out in the Agreement, Rackspace shall maintain and implement the following technical and organizational measures in relation to the security of the Customer Configuration.

1. DEFINED TERMS.

"**Customer Configuration**" means an information technology system (hardware, software, and/or other information technology components) which is the subject of the Services or to which the Services relate.

"**Customer Data**" means all data which Customer receives, stores, or transmits on or using the Customer Configuration.

"**Hosted System**" means a Customer Configuration provided by Rackspace for Customer's use at a Rackspace data center.

"Product Terms" means additional terms and conditions incorporated in a Service Order which contain product-specific obligations.

"**Rackspace Shared Infrastructure**" means the systems, networks and associated infrastructure managed by Rackspace and utilized to provide Rackspace support Services; excluding to the extent forming part of the Customer Configuration.

"**Rackspace Policies and Standards**" means Rackspace's internal policies and standards governing Rackspace's corporate management, service delivery and security.

"**Third Party Cloud Provider**" means a third party provider of cloud or other hosting services (including AWS, Google and Microsoft, as applicable).

"**Rackspace Personnel**" means Rackspace's employees, officers, directors and members and others to whom Rackspace gives access to Customer Data in accordance with this Agreement.

"**Rackspace Support Bastions**" means the designated systems maintained by Rackspace on Rackspace Shared Infrastructure and which are used by Rackspace Personnel to connect to the Customer Configuration.

"**Services**" means the Rackspace services identified in a specific Service Order.

"**Service Order**" means the document describing the Services Customer is purchasing, including any Rackspace online order, process, API, statement of work, or tool through which Customer requests or provisions Services.

2. TECHNICAL & ORGANIZATIONAL MEASURES.

A. PERSONNEL CONTROLS.

Reference	Personnel Controls - Control Description
A.1. Screening	Rackspace shall implement procedures requiring screening of individuals with access to organizational information systems when the role or position of such individuals with Rackspace provides access to Customer Data and as otherwise required by the Agreement. Rackspace shall conduct the appropriate level of background screening required by ISO/Payment Card Industry-Data Security Standard (PCI-DSS) as applicable to Rackspace, the Services and the role of the individual. Rackspace shall maintain documentation that validates that the appropriate level of screening requirements has been completed by Rackspace. Rackspace shall maintain and follow a written procedure for how Rackspace shall

© 2021 Rackspace US, Inc. - Global Terms - October 23, 2023 - Revision OT# 59969

Reference	Personnel Controls - Control Description
	comply with the screening and requirements, which shall be available for review by Customer upon request.
A.2. *Removal*	Rackspace shall implement procedures requiring that if an employee satisfies the screening requirements but Rackspace subsequently becomes aware of any information that would result in an employee failing any of the screening requirements, Rackspace shall promptly suspend or remove the employee's access to Customer Data and prohibit the employee from performing any Services for Customer involving access to Customer Data in accordance with any requirements under the Agreement.
A.3. *Personnel Policy*	Rackspace shall implement procedures that: (i) define appropriate IT security related roles and responsibilities for Rackspace Personnel; (ii) help ensure that Rackspace Personnel have access only to the systems they have a business need and authorization to use; identify an owner for critical systems and responsibilities for key tasks and assign those tasks to individuals capable of performing them as they relate to the Rackspace Shared Infrastructure; (iii) include confidentiality provisions within Rackspace employees' terms of employment; (iv) retain documentation of security awareness training, confirming the completion of this training for each member of Rackspace Personnel engaged in the provision of the Services requiring access to Customer Data; control the creation, change, and termination of Rackspace Personnel user accounts; and (v) and maintain a disciplinary process for policy violations.
A.4. *Code of Conduct*	Rackspace shall gain assent to the Rackspace Code of Business Conduct and Ethics from each of its employees upon hiring and all employees shall take part in an onboarding course designed to familiarize them with the company, its objectives and their responsibilities. Rackspace shall offer yearly training to employees on Rackspace's Code of Business Conduct and Ethics. Rackspace shall implement policies to communicate and maintain organizational values and behavioral standards consistent with the Code of Business Conduct and Ethics.
A.5. *Awareness*	As part of the implementation and ongoing support for information security policies, all Rackspace Personnel shall be required to participate in training and awareness sessions to support the importance of security within the Rackspace organization. Rackspace shall maintain an ongoing security awareness program for employees to provide updated guidance and practice information. Rackspace's corporate security team shall release regular notifications to employees focusing on prominent security issues.
A.6. *Competence*	Rackspace shall maintain 24/7/365 staffing to support Rackspace Shared Infrastructure systems that are critical to Rackspace's performance of the Services under the Agreement, including staffing support and data center operations teams with technicians certified in various areas of expertise.
A.7. *Hiring*	Rackspace shall base hiring decisions on factors relevant to the performance of Rackspace's obligations under its customer agreements including evaluating educational background, prior relevant experience, past accomplishments and evidence of integrity and ethical behavior.

B. PHYSICAL SECURITY.

Reference	Physical Security - Control Description
B.1. Physical Security Policy	Rackspace shall maintain a formal physical and environmental security program for any Rackspace operated facilities used to perform the Services.
B.2. Physical Access	Rackspace shall implement procedures requiring (i) visitors to check in with reception/security, and provide a government issued ID, before being granted access to Rackspace facilities used to perform the Services; and (ii) use of visitor badges to identify visitors at Rackspace facilities. The visitor log shall be compiled and reviewed in the event of a security incident involving access to Rackspace facilities used to perform the Services.
B.3. Physical Security	Rackspace shall implement procedures for: (i) the administration of proximity-based access cards and biometric hand scanners (or other approved security authentication methods) for controlled building access, and secure access to specific areas of Rackspace operated facilities used to perform the Services; and (ii) disabling of physical access within the timeframe specified by Rackspace's access termination standard when physical access is no longer needed due to termination of employment or Services. Rackspace shall implement incident response procedures to manage and document physical security incidents at Rackspace operated facilities used to perform the Services.

C. SYSTEM SECURITY.

C.1. **System Access Controls**.

Reference	System Access Controls - Control Description
C.1.1. System Access & Bastions – Customer Configurations	For Hosted Systems: Rackspace shall implement procedures requiring that access to the Customer Hosted System and Customer VLANs shall occur through dedicated bastion servers designed for this purpose; and Rackspace employees shall authenticate with the bastion server using a dedicated user ID (e.g., an assigned corporate SSO credential). For Customer Configurations other than Hosted Systems: Rackspace shall implement procedures requiring that: (i) access to the control panel permitting access to the Customer Configuration requires 2-factor authentication, shall be managed through Rackspace's LDAP Active Directory group, and shall be limited to support personnel and those ancillary services teams at Rackspace who require such access for purposes of providing or supporting the Services; (ii) network security group rules are maintained on the Customer Configuration subnets to specifically allow access over established RDP and SSH ports for remote administration; (iii) the Customer Configuration bastion subnet is locked down to only allow remote access from the Rackspace Support Bastions; (iv) Rackspace manages and leverages local server users, which are tied back to established corporate identities; (v) server authentication requests are directed to a known Rackspace ADFS endpoint for dual factor authentication; (vi) as part of the user authentication flow, local user accounts are only enabled at the time that an authenticated access request is granted and are constrained to the requested device; and (vii) Rackspace maintains a list of approved technicians who can execute the user access workflow.

Reference	System Access Controls - Control Description
C.1.2. System Access Review	Rackspace shall maintain a formal program for the review of access to the Customer Configuration by any Rackspace employee (the "**Access Review Program**"). This does not include additional logging at the server or device or instance level (which Customer may enable at their option or request assistance where forming part of the Services). The Access Review Program is designed to ensure that no active IDs or accounts exist that are not linked to one or more Rackspace Personnel; IDs or accounts for terminated Rackspace Personnel are deleted as appropriate; and that Rackspace is complying with its access provisioning process.
C.1.3. System Remote Access	Rackspace Personnel may use a Virtual Private Network (VPN) utilizing two-factor authentication (e.g., token and password) to connect remotely to Rackspace networks. Rackspace shall implement procedures requiring that once inside the Rackspace network, support staff members are required to complete a second level of authentication via the Rackspace Support Bastion/jump hosts/gateway servers to access Customer Configurations.
C.1.4. Password Policy	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. Rackspace shall maintain a formal policy with respect to the requirements for password and authentication in regard to Rackspace's access to Customer Configurations and the Rackspace Shared Infrastructure (the "**Password Policy**"). The Password Policy shall provide for a secure method of assigning and selecting passwords or require the use of unique identifier technologies (e.g., biometrics or token devices); require control of data security passwords to ensure that such passwords are kept in a location or format that does not compromise the security of the data they protect; require Rackspace to prevent or limit users from further access after a number of unsuccessful attempts to gain access; detail requirements for access to each user account relating to the Rackspace Shared Infrastructure including the authentication requirements set out in the Agreement or (if and to the extent not otherwise set out in the Agreement) industry standard requirements; and requirements that all Rackspace managed computing devices shall be configured to lock (i.e., prevent access to the computing device) after a period of inactivity (which period of inactivity shall be no longer than 15 minutes or the applicable period of time set out in the Agreement) requiring users of the applicable computing device to enter their credentials in order to regain access to the computing device.
C.1.5. Encryption or Pseudonymization	Customers are responsible for implementing adequate controls to maintain appropriate security and protection of data, which shall include encryption and logical access measures. Encryption of data stored within the Customer Configuration may be employed by electing to purchase or use capabilities provided by Rackspace or otherwise obtained by Customer from third parties.

C.2. **Vulnerability Assessments**.

Reference	Vulnerability Assessments - Control Description
C.2.1. Customer Testing	Subject to Rackspace's written consent (in respect of Hosted Systems) or agreement of any applicable Third Party Cloud provider (in respect of Third Party Cloud provider infrastructure), Customer may perform network and application security scans that test the Customer Configuration for: (i) security vulnerabilities;

Reference	Vulnerability Assessments - Control Description
	(ii) denial of service vulnerabilities; (iii) system access; and/or (iv) other intrusive activities such as password cracking. Unless identified in the Service Order, the Services do not include support for such activities. If, as a result of such activities, Customer identifies any vulnerabilities on the Rackspace Shared Infrastructure then Customer must inform Rackspace and Rackspace shall subsequently correct any discovered vulnerabilities on Rackspace Shared Infrastructure within a commercially reasonable timeframe or as otherwise required by the Agreement.
C.2.2. Monitoring, AoC	Rackspace shall perform ongoing monitoring and testing of the Rackspace Shared Infrastructure (to include vulnerability scanning, scheduled penetration testing, and maintenance) in accordance with any applicable PCI-DSS standards, and applicable Rackspace Policies and Standards. Rackspace shall make available its Attestation of Compliance to Customer on an annual basis, where applicable.

C.3. **System Defense**.

Reference	System Defense - Control Description
C.3.1. System Defense - General	Rackspace shall: (i) apply security measures to the Rackspace Shared Infrastructure in accordance with Rackspace Policies and Standards; (ii) maintain and monitor (on an active 24/7/365 basis) firewalls around the Rackspace Shared Infrastructure in accordance with Rackspace Policies and Standards; and (iii) apply security measures to web servers used by Rackspace to provide the Services and the Rackspace customer portal in accordance with the Rackspace Policies and Standards.
C.3.2. DDoS Mitigation	Rackspace shall utilize tooling to seek, detect and trace network-wide anomalies, including denial-of-service (DoS) attacks and worms against the Rackspace Shared Infrastructure. Rackspace shall implement procedures requiring: (i) access control lists (ACLs) to be used on Internet edge routers on Rackspace Shared Infrastructure to seek to mitigate distributed denial of service (DDoS) attacks against the Rackspace Shared Infrastructure; (ii) evaluation of existing and potential threats by aggregating traffic from across the Rackspace Shared Infrastructure through network-wide, router-based sampling; (iii) continuous monitoring of connectivity and performance for multiple bandwidth providers, including routers and switches; and (iv) utilization of fully redundant routing and switching equipment for Rackspace's core networking infrastructure elements of the Rackspace Shared Infrastructure.
C.3.3. Separation	Rackspace shall use logically separate networks (vLANs) for internal traffic, and for the administration of Customer environments from specified networks within the Rackspace Shared Infrastructure.
C.3.4. Role Based Access Controls – Rackspace Shared Infrastructure	Rackspace shall implement procedures requiring: (i) secure access to core networking infrastructure elements of the Rackspace Shared Infrastructure, utilizing the inherent access control functionality in TACACS+/ACS software (or equivalent); (ii) limitations upon administrator access to network devices supporting Rackspace Shared Infrastructure to authorized Rackspace Personnel, and granting of new administrator access to network devices supporting Rackspace infrastructure through a maintained new user creation process; (iii) role-based access, with deviations requiring managerial approval; and (iv) review of TACACS+/ACS (or equivalent) access lists on a periodic basis to verify that

Reference	System Defense - Control Description
	users on the list still require access to network devices and correction of any discrepancies found.
C.3.5. Security Services	Rackspace shall provide a firewall, IDS and any other security devices in Customer's dedicated Hosted System only to the extent Customer purchases such device(s) and then in accordance with the applicable Product Terms for such devices.
C.3.6. Rackspace Support Bastion Security	Rackspace shall maintain a formal program to help to ensure that the Rackspace Support Bastions used to access the Customer Configuration have malicious software protections in place, are maintained in good technical working order, are regularly scanned for vulnerabilities, and are patched with the latest applicable software updates.
C.3.7. Policy, Demarcation	Rackspace shall maintain a formal program for implementing security measures to seek to secure access to the Rackspace Shared Infrastructure, requiring all access points and boundaries to Rackspace's network to be clearly documented, and protections against unauthorized access to be implemented.

D. CHANGE & CONFIGURATION MANAGEMENT.

Reference	Change & Configuration Management – Hosted Systems - Control Description
D.1. Change Process	Rackspace shall cooperate with Customer to create a run book or account management guidelines ("**Run Book**") for any Hosted System, which shall contain the controls applicable to system or network changes and detail the system or change management process as agreed upon with Customer. Rackspace shall provide Customer with a mechanism to apply patches to the Hosted System and shall apply patches at Customer's request, as stipulated in the Run Book.
D.2. Run Book	Rackspace shall make the Hosted System Run Book and any attendant documentation available to Customer promptly upon Customer's request, shall update the Run Book with any commercially reasonable process management controls in respect of the Hosted System requested by Customer, and shall otherwise cooperate with Customer in good faith to review or implement such system/network change management processes for the Hosted System as Customer requests.
D.3. Windows	Rackspace shall maintain change windows for implementing or completing system/network changes to the Hosted System which comply with any change window requirements set out in the Agreement.
D.4. Approval, History	Customer is required to approve material changes to be made by Rackspace to the Hosted System before the change is implemented, except in the cases of predefined proactive Rackspace Shared Infrastructure maintenances, urgent security patches and fixes, downtime events where Customer cannot be reached (or has provided prior approval for action), and emergency maintenances (in which case Rackspace shall provide Customer with reasonable notification of such change activity). The history of tickets associated with the Rackspace account shall be available for review through the Rackspace customer portal, thereby providing

Reference	Change & Configuration Management – Hosted Systems - Control Description
	a history of changes to the Hosted System performed by the Rackspace support team.

E. MEDIA PROTECTION.

Reference	Media Protection – Hosted Systems - Control Description
E.1. Single-Pass	Rackspace shall zero-fill (meaning to format the hard disk drive by filling available sectors with zeroes) any hard disk drive dedicated to Customer's use as part of a Hosted System prior to re-using the hard disk drive in a Rackspace data center.
E.2. Physical Destruction	Upon Customer's written request during the term of the Agreement, Rackspace shall destroy (via hole punch, de-gaussing, or other mechanism) any of the media dedicated to Customer's use as part of a Hosted System, and Rackspace shall provide documentation or certification to Customer of such destruction. Rackspace may charge Customer a fee for such Services at its then current rates, as applicable.
E.3. Multi-Pass	Customer may designate the hard drives dedicated to Customer's use as part of a Hosted System as requiring a 3-pass wipe (on failure, as possible, or on replacement or cancellation) upon written notice to the Rackspace account manager. Rackspace shall perform a 3-pass wipe on such media upon a failure, replacement, or cancelation event, and Customer agrees to reimburse Rackspace at Rackspace's then current rates for such Services.
E.4. Geographic Control	Except as otherwise specifically stated in the Agreement, Rackspace shall not relocate the Customer's Hosted System from a Rackspace data center in one country to another country without Customer's express written permission. Customer acknowledges that off-site backup involves the transport of encrypted media containing Customer Data to a third party site.

F. RISK ASSESSMENT.

Reference	Risk Assessment - Rackspace Shared Infrastructure - Control Description
F.1. Risk Assessment Policy	Rackspace shall incorporate risk management throughout its business operations. Rackspace's Global Enterprise Security (GES) team shall conduct internal information security risk assessments regarding Rackspace Shared Infrastructure.
F.2. Risk Assessment Oversight	Rackspace shall manage identified risks to the Rackspace Shared Infrastructure on an ongoing basis through formal project management processes, provide an overall strategic plan, and operationalize that plan.
F.3. Control Performance Review	Rackspace shall assign managerial and supervisory personnel to be responsible for monitoring the quality of internal Rackspace Shared Infrastructure security control performance as a routine part of their job responsibilities. Rackspace's management shall review key reports to verify appropriate actions have been taken.

Reference	Risk Assessment - Rackspace Shared Infrastructure - Control Description
F.4. Risk Assessments	Rackspace shall undertake security risk assessments of the Rackspace Shared Infrastructure and Rackspace corporate networks per the Rackspace Policies and Standards including: (i) identifying and assessing reasonably foreseeable internal and external threats and risks to the privacy, confidentiality, security, integrity and availability of personal information; (ii) assessing the likelihood of, and potential damage that can be caused by identified threats and risks; (iii) assessing the adequacy of Rackspace's information security program, and personnel compliance with program training; (iv) assessing the adequacy of service provider arrangements; (v) adjusting and updating Rackspace's information systems and information security program to limit and mitigate identified threats and risks and to address material changes to relevant technology, business practices, personal information practices and the sensitivity of personal information that Rackspace processes; and (vi) assessing whether Rackspace's information security program is operating in a manner reasonably calculated to help prevent and mitigate information security incidents.

G. BUSINESS CONTINUITY PLANNING.

Reference	Business Continuity Planning - Rackspace Shared Infrastructure - Control Description
G.1. Business Continuity Policy	Rackspace maintains an policy which includes: (i) defined requirements for information security and continuity of information security management in respect of Rackspace Shared Infrastructure during Rackspace business recovery events; and (ii) defined management structure to prepare for, mitigate and respond to a Rackspace business recovery event involving Rackspace Shared Infrastructure using personnel with the necessary authority, experience and competence; and verification, review and testing of defined information security continuity controls related to the Rackspace Shared Infrastructure on a regular basis.
G.2. Business Continuity Plan	Rackspace maintains an internal business continuity plan designed to permit Rackspace to resume its business operations following an interruption ("**Business Continuity Plan**"). This Business Continuity Plan does not cover Customer Configuration directly (and is no substitute for redundancy or data backup, and in no way guarantees the restoration of the Customer Configuration or any Customer Data in the event of severe business interruption).

H. DATA CENTER CONTROLS.

Reference	Data Center Controls – Rackpace Shared Infrastructure - Control Description
H.1. Additional Physical Controls	Rackspace shall implement procedures requiring that: (i) Rackspace Personnel are on duty at Rackspace operated data center facilities 24/7/365; (ii) two-factor authentication is used to gain access to the server room floors of Rackspace Shared Infrastructure; (iii) electromechanical locks within Rackspace Shared Infrastructure are controlled by biometric authentication (e.g., biometric scanner) and key-card/badge; and (iv) closed circuit video surveillance, with a video retention period of at least 90 days, is installed at entrance points on the interior and exterior of the buildings housing Rackspace operated data centers hosting Rackspace Shared Infrastructure, and is monitored by authorized personnel.

Reference	Data Center Controls – Rackpace Shared Infrastructure - Control Description
H.2. Environmental Controls	Rackspace Shared Infrastructure data center facilities are equipped with redundant HVAC units to maintain consistent temperature and humidity levels. Rackspace shall implement procedures that require Rackspace Shared Infrastructure HVAC systems to be inspected regularly, and air filter changed as needed. Redundant lines of communication exist within the Rackspace Shared Infrastructure to telecommunication providers providing Rackspace customers with failover communication paths in the event of data communications interruption. Rackspace Shared Infrastructure data centers are equipped with sensors to detect environmental hazards, including smoke detectors and floor water detectors. Rackspace Shared Infrastructure data centers are also equipped with raised flooring to protect hardware and communications equipment from water damage. Rackspace Shared Infrastructure data centers are equipped with fire detection and suppression systems, and fire extinguishers. Fire detection systems, sprinkler systems and chemical fire extinguishers within Rackspace Shared Infrastructure are inspected at least annually. Rackspace Shared Infrastructure data center facilities are equipped with uninterruptible power supplies (UPS) to mitigate the risk of short-term utility power failures and fluctuations. The Rackspace Shared Infrastructure UPS power subsystem is at least N+1 redundant with instantaneous failover in the event of a primary UPS failure. The Rackspace Shared Infrastructure UPS systems are inspected and/or serviced at least annually. Rackspace Shared Infrastructure data center facilities are equipped with diesel generators to mitigate the risk of long-term utility power failures and fluctuations. Rackspace Shared Infrastructure generators are tested at least every 120 days internally and tested at least annually by a third party contractor to maintain appropriate operability in the event of an emergency.

I. INCIDENT RESPONSE.

Reference	Incident Response - Control Description
I.1. Notification	Rackspace shall comply with its reporting obligations under the Agreement. 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 in the Agreement or Rackspace's express obligations in the Agreement.
I.2. Incident Response Policy	Rackspace shall maintain a documented process to report, evaluate and respond to security incidents identified on the Rackspace Shared Infrastructure, including rating and remediating such incidents within commercially reasonable timeframes depending on the severity of the incident.