ACCEPTABLE USE POLICY

This Acceptable Use Policy ("**AUP**") describes activities prohibited on Rackspace Services for the protection of Rackspace and its Representatives, Services, network and other customers. Questions regarding this policy should be directed to abuse@rackspace.com.

1. ABUSE GENERALLY. Customer shall not use the Services or any related software, system, or network to engage in, foster, solicit or promote illegal, or irresponsible behavior including:

1.1. conduct likely to breach any laws, codes, or regulations applicable to the parties (including conduct infringing or misappropriating intellectual property, or confidential or proprietary information; or which is fraudulent, unfair, deceptive or defamatory);

1.2. unauthorized access to, monitoring or use of, or interference with an internet account, computer, systems, networks, data or traffic;

1.3. intentionally, knowingly or recklessly introducing any malicious code into the Services;

1.4. conduct violating rules and conventions of any domain registrar, email service, bulletin board, chat group, or forum used in conjunction with Rackspace Services or network (including using false, misleading or deceptive TCP-IP packet header information in an email or newsgroup posting);

1.5. deceitfully collecting, transmitting or using information, or distributing software which covertly gathers or transmits information about a user;

1.6. distributing advertisement delivery software unless the user affirmatively consents to download and installation based on clear and conspicuous notice of the nature of the software, and can easily remove software using standard tools included on major operating systems;

1.7. conduct likely to result in retaliation or adverse action against Rackspace or its services, network, website or Representatives (including resulting in listing of Rackspace IP space on an abuse database);

1.8. conduct which breaches Customer's security obligations, or any activity in connection with the Services that may expose Rackspace to a security vulnerability;

1.9. conduct intended to withhold or cloak identity or contact information, registering to use Services under a false name, or using an invalid or unauthorized credit card in connection with Services;

1.10. gambling activity violating any applicable codes of practice, required licenses, or technical standards;

1.11. use of any Rackspace provided shared system in a way that unnecessarily interferes with the normal operation of the shared system, or consumes a disproportionate share of system resources; and

1.12. conduct creating a risk to safety or health, national security or law enforcement.

2. OFFENSIVE BEHAVIOR. Customer shall not be abusive or offensive to Rackspace Representatives. Customer shall not publish, transmit or store on or via the Services content or links to content that Rackspace reasonably believes relates in any manner to child pornography, bestiality, non-consensual sex acts, or live sex acts; or is excessively violent, incites or threatens violence, contains harassing content or hate speech, violates a person's privacy, is malicious or morally repugnant.

3. NO HIGH RISK USE. Customer may only use the Services for commercial purposes; and Customer shall not use the Services in any situation where failure or fault of the Services could lead to death or serious bodily injury of

©2016 Rackspace US, Inc. – Global Terms – 20 September 2021 Revision – OT# 46379

any person, or to physical or environmental damage (including in connection with aircraft or other modes of human mass transportation, or nuclear or chemical facilities).

4. MAIL REQUIREMENTS. For bulk or commercial email sent by or on behalf of Customer using the Services or from any network that directly or indirectly refers recipients to a site hosted using the Services (including using third party distribution lists), Customer shall:

4.1. post a privacy policy for each associated domain;

4.2. post an email address for complaints in a conspicuous place on any associated website, promptly respond to messages sent to that address, and have means to track anonymous complaints;

4.3. obtain affirmative consent to receive e-mail from intended recipients using reasonable means to verify ownership of the e-mail address, honor and notify recipients of consent revocation, and evidence consent within 72 hours of recipient or Rackspace request; and

4.4. include the recipient's e-mail address in the e-mail body or "TO" line.

5. VULNERABILITY TESTING. Customer shall not attempt to test the vulnerability of a Rackspace system or network including those provided in connection with the Services, or attempt to breach security measures, of said system or network by any means. Notwithstanding the foregoing, Customer may conduct vulnerability testing of their Hosted System with Rackspace's prior written consent.

6. CUSTOMER PROVIDED LICENSES AND SUPPORT. Customer shall comply with the applicable license terms governing use of any Open Source Software or Third Party Software provided by Rackspace. If Customer uses any non-Rackspace provided software on the Customer Configuration then Customer represents and warrants that Customer shall maintain: (i) the legal right to use the software; and (ii) as applicable to the Services, adequate original software vendor support (or similar authorized support) permitting Rackspace to perform any installation, patching, upgrades, or management which Rackspace has agreed to provide. On Rackspace's request, Customer shall sufficiently certify in writing (or, as reasonably requested, evidence) that Customer is in compliance with this section and any other license or support obligations under the Agreement. If Customer fails to certify licensing or support as requested, Rackspace may charge Customer its standard fee for licensed use of the software, until the required certification is provided.

7. EXPORT CONTROL. Customer shall ensure Services are not used in breach of export laws, controls, regulations or sanction policies of the United States or Customer's applicable jurisdiction. Customer shall ensure Services are not used by any person or entity suspected of involvement or affiliation with those involved in activities or causes relating to: human trafficking; illegal gambling; terrorism; narcotics trafficking; arms trafficking or the proliferation, development, design, manufacture, production, stockpiling, or use of nuclear, chemical, or biological weapons, weapons of mass destruction, or missiles.

8. COOPERATION WITH INVESTIGATIONS AND PROCEEDINGS. Customer agrees Rackspace may permit a relevant authority to inspect Customer's content or traffic if Rackspace is legally required to do so, provided Rackspace gives Customer reasonable prior notice (where permitted by applicable law and regulation). Rackspace may report to appropriate authorities any Customer conduct Rackspace believes violates applicable law, without notice to Customer (including providing any information about Customer, its users, or traffic). Rackspace may cooperate in response to a formal request from a law enforcement or regulatory agency investigating conduct Rackspace believes violates applicable law, or in a civil action that on its face meets the requirements for such a request. Customer shall cooperate with Rackspace's reasonable investigation and resolution of any suspected breach of the Agreement.

9. DOMAIN NAMES, IP ADDRESSES AND DNS RECORDS. Customer must maintain valid information with Customer's domain name registrar for any domain hosted on the Services, and only use IP addresses assigned to Customer by Rackspace in connection with the Services. Customer agrees Rackspace may modify, transfer, or

delete any DNS record or zone on Rackspace managed or operated DNS servers or services upon request from the registrant or administrative contact according to the registrar's WHOIS system.

10. CHANGES TO AUP. Rackspace may amend the AUP by publishing a revised version at www.rackspace.com/information/legal/aup, or in the event of a material adverse AUP change by providing Customer at least 30 days prior written notice. The revised AUP shall become effective as to Customer on the first to occur of: (i) Customer's execution of a new Service Order or agreement incorporating the revised AUP or (ii) the first day of an agreement renewal term beginning at least 30 days after revised AUP publication, or (iii) expiry of written notice provided pursuant to this section. If compliance with the revised AUP would adversely affect Customer's use of the Services, Customer may terminate the affected Services for convenience by giving Rackspace written notice of Customer's objection no later than the date that the revised AUP would otherwise have become effective as to Customer; Customer may continue using the Services for up to an additional 90 days subject to the prior version of the AUP. Rackspace may, at its discretion, waive the AUP change as to Customer in which case the notice of termination shall be of no effect.

11. AUP BREACH. If Customer breaches the AUP (including unintentionally, resulting from Customer's failure to use reasonable security precautions, or as a result of activity occurring without Customer authorization) Rackspace may block any content or traffic, may be relieved of its obligation to provide all or a portion of the Services, suspend the Services, or terminate the Services in accordance with the Agreement, at its election**.** No credit shall be available under any Service Level Agreement for interruptions of Services resulting from an AUP breach. Customer's use of the Services to assist another entity in an activity that would breach this AUP if performed by Customer is an AUP breach.