# RACKSPACE® SUPPLIER COMPLIANCE TERMS

These Rackspace Supplier Compliance Terms shall apply in addition to any other terms and conditions of Supplier's Agreement with Rackspace. In the event of a conflict, these Rackspace Supplier Compliance Terms shall take precedence over any other term or condition of the Agreement. Rackspace may amend these Rackspace Supplier Compliance Terms at any time and at its sole discretion. Any changes will be effective upon the posting of such changes on the Rackspace website, and Supplier is responsible for reviewing this location and informing itself of all applicable changes or notices. Supplier should refer regularly to the Rackspace website to review the current terms. SUPPLIER'S CONTINUED PROVISION OF PRODUCTS OR SERVICES AFTER RACKSPACE'S POSTING OF ANY CHANGES SHALL CONSTITUTE SUPPLIER'S ACCEPTANCE OF SUCH CHANGES OR MODIFICATIONS.

**1. SUPPLIER CODE OF CONDUCT.** Supplier shall comply with the Rackspace Code of Conduct available at www.rackspace.com/information/legal/supplier-code-of-conduct.

**2. COMPLIANCE WITH LAW**. Supplier shall perform its obligations under the Agreement in compliance with applicable laws and regulations, including as set out below.

**2.1. Data Protection Laws**. Supplier shall comply with Applicable Data Protection Law (as defined in the Rackspace Supplier Data Processing Addendum) and shall not do anything or omit to do anything which would cause Rackspace or any third party associated with Rackspace (including without limitation a Rackspace customer) to breach Applicable Data Protection Law. If Supplier processes any data which is Personal Data (as defined in the Rackspace Supplier Data Processing Addendum) then Supplier shall comply with the Rackspace Supplier Data Processing Addendum available at www.rackspace.com/information/legal/SDPA. Supplier shall not transfer Rackspace Personal Data outside of the country of origin of the Rackspace Personal Data (or in the case of Rackspace Personal Data originating from the EEA, then the EEA), without the prior written consent of Rackspace. If and to the extent that Supplier: (if) creates, receives maintains or transmits protected health information on behalf of Rackspace, its Customers or End-Users; or (ii) otherwise meets the definition of "Business Associate" under 45 CFR § 160.103, then Supplier shall comply with the Rackspace Supplier Business Associate Agreement (BAA) available at www.rackspace.com/information/legal/SBAA

**2.2. Anti-Corruption Laws**. Supplier shall comply with Applicable Anti-Corruption Law and shall not do anything or omit to do anything which would cause Rackspace or any third party associated with Rackspace (including without limitation a Rackspace customer) to breach Applicable Anti-Corruption Law. "**Applicable Anti-Corruption Law**" means all applicable laws, rules, and regulations in relation to anti-corruption or anti-bribery which may include, but is not limited to: the US Foreign Corrupt Practices Act, the UK Bribery Act 2010, the Canadian Corruption of Foreign Public Officials Act, the Colombian Anti-Corruption Statute, the Brazilian Law No. 9,613, the Venezuelan Anti-Corruption Law, the Hong Kong Prevention of Bribery Ordinance, the Chinese Company Law, the Chinese Anti-Unfair Competition Law, the Japanese Unfair Competition Prevention Law, the Malaysian Anti-Corruption Commission Act, the New Zealand Crimes (Bribery of Foreign Public Officials) Amendment Act, the Singapore Prevention of Corruption Act, the South Africa Prevention and Combating of Corrupt Activities, the Australian Criminal Code Amendment (Bribery of Foreign Public Officials) Act, the German Act on Bribery of Foreign Public Officials in International Business Transactions, the Swiss Unfair Competition Act, relevant provisions in the respective country's criminal code and any amended or replacement legislation. Supplier shall not offer, promise or give to, or demand or accept from any Rackspace employee, agent or other personnel anything of value as an incentive to obtain or retain Rackspace's business or otherwise as an inducement.

**2.3. Economic Sanctions Laws**. Supplier shall comply with all laws administered by the United States Office of Foreign Asset Controls or any other governmental entity imposing sanctions and trade embargoes ("**Economic Sanctions Laws**") against designated countries ("**Embargoed Countries**"), entities, and persons.


© 2020 Rackspace US, Inc. – Supplier Addendum – 31 October 2025 Revision – OT# 57709

(collectively "**Embargoed Targets**"). Supplier is not an Embargoed Target or otherwise subject to any Economic Sanctions Law. Supplier shall comply with all Economic Sanctions Laws. Without limiting the generality of the foregoing, Supplier shall not broker, finance, or otherwise facilitate any transaction in violation of any Economic Sanctions Law.

**2.4. Securities Laws**. Supplier acknowledges that Rackspace Technology, Inc. is a publicly traded company and that US securities laws and comparable laws and regulations in other jurisdictions prohibit any person who has material non-public information about a publicly-traded company from: (i) purchasing or selling securities of that company; or (ii) communicating that information to any other person under circumstances in which it is reasonably foreseeable that this person is likely to purchase or sell securities of that company. Supplier shall comply with any such laws and regulations. Supplier agrees that it will not use, or cause any third-party to use, any Confidential Information (as defined by the Agreement), or other material non-public information regarding Rackspace in violation of the U.S. securities laws.

**2.5. Secure Information Laws**. Supplier shall comply with applicable law governing the particular type of information comprising the Secure Information (as defined in the Supplier Secure Information Addendum), and shall not do anything or omit to do anything which would cause Rackspace or any third party associated with Rackspace (including without limitation a Rackspace customer) to breach such laws. Supplier shall comply with security practices and standards prescribed under applicable law. Supplier shall not attempt to access Rackspace's secure network(s) or other information systems, without Rackspace's prior written consent, either via its personnel performing Services onsite or remotely. Rackspace's consent for such access may be revoked at any time in Rackspace's sole discretion. If Supplier has access to or the potential to affect Secure Information, then Supplier shall comply with the Rackspace Supplier Secure Information Addendum available at www.rackspace.com/information/legal/SSIA. If Services will be performed inside a Rackspace owned or leased data center, Supplier's personnel who will have access to the production area of the data center will be deemed to have access to Secure Information. Supplier personnel who perform Services on, or otherwise attend, Rackspace's premises must comply with Rackspace's on-site security requirements, as they may be modified from time to time. Specifically, but without limitation, Supplier's personnel may not bring a firearm on any part of Rackspace premises (including the vehicle parking area). Rackspace may require any Supplier personnel to leave its premises for any reason or no reason in Rackspace's sole discretion, provided, however, that if Rackspace has not provided reasonable grounds for requiring the personnel to leave, then Supplier shall be relieved of its obligations under the Agreement to the extent it is delayed in performing them by reason of the removal.

**2.6. US Public Sector Laws**. Where the Products or Services provided by Supplier under any Order are designated for use by or in connection with a Rackspace end user that is an agency, supplier to, or instrumentality of the Government of the United States, then Supplier shall comply with the Rackspace US Public Sector Supplier Addendum available at www.rackspace.com/information/legal/USPSSA.

**2.7. Covered Telecommunications Equipment or Services**. This section shall only apply when Supplier enters into an MSA with a US based Rackspace entity. If this section applies, Supplier shall not provide to a US based Rackspace entity any covered telecommunications equipment or services within the meaning of 48 CFR 52.204-25; or provide to Rackspace or itself use any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system within the meaning of 48 CFR 52.204-25, as modified by the interim rule at 85 Fed. Reg. 42665, released July 14, 2020. Supplier further represents, as required under 48 C.F.R. 52.204-26, that it has reviewed the list of excluded parties on www.sam.gov and that it does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government of the United States in the performance of any contract, subcontract, or other contractual instrument. Supplier also agrees to flow-down this provision in substantially similar form to its subcontractors, and require such subcontractors to also flow-down this provision onwards to its own subcontractors in substantially similar form.

**2.8. Conflict Minerals**. Supplier represents and warrants that it is in full compliance with all applicable all laws (including section 1502 of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010) relating to minerals mined in conditions of armed conflict and human rights abuses ("**Conflict Minerals Laws**") and any other applicable governmental or industry guidelines or codes (including the Code of Conduct of the Electronics

Industry Citizenship Coalition) relating to Conflict Minerals. "**Conflict Minerals**" means minerals or substances covered under the Conflict Minerals Laws as they may be amended from time to time including columbite-tantalite, also known as coltan (the metal ore from which tantalum is extracted); cassiterite (the metal ore from which tin is extracted); gold; wolframite (the metal ore from which tungsten is extracted); or their derivatives. Specifically, Supplier represents and warrants that it does not use Conflict Minerals from any Covered Country for any materials contained in the Products, unless specifically disclosed in writing in accordance with the provisions of this section. "**Covered Country**" means any country, territory, or jurisdiction designated under the Conflict Minerals Laws as they may be amended from time to time including the Democratic Republic of the Congo, and any country that shares an internationally recognized boarder with the Democratic Republic of the Congo, which, as of the Effective Date, includes Angola, Burundi, Central African Republic, the Republic of the Congo, Rwanda, South Sudan, Tanzania, Uganda, and Zambia. Supplier will, at Rackspace's request, make available to Rackspace and/or Rackspace's agents and representatives, full material declarations that identify the sources and amount of all substances contained in the Products. Unless Rackspace specifically agrees in writing that a particular Product may contain a particular material, Supplier will, and will ensure all third party suppliers, also provide Rackspace with a statement that the Products do not contain any Conflict Minerals. Upon delivery of any Products, Supplier will declare each Product's compliance with all Conflict Minerals Laws and identify any substances that are banned or must be declared under applicable Conflict Minerals Laws, and make available to Rackspace and its agents and representatives any documentation supporting such declaration. Without limiting the generality of the foregoing, Supplier agrees to disclose to Rackspace, upon Rackspace's request, to the extent known or discoverable by Supplier or any third party supplier following inquiry, the original source of all minerals contained in the Product. Supplier agrees to fully cooperate with Rackspace, including disclosing from whom Supplier or any third party supplier purchased the minerals, so that Rackspace may make a reasonable inquiry into country of origin of any Conflict Minerals for purposes of fulfilling the reporting requirements of any applicable Conflict Minerals Laws. Without limitation to the foregoing, at Supplier's sole cost and expense, Supplier will provide any cooperation as Rackspace may require in order to meet any obligations Rackspace may have under any applicable Conflict Minerals Laws including in the preparation of any reports Rackspace may file with the US Securities and Exchange Commission or in conducting additional due diligence to comply with any applicable Conflict Minerals Laws.

**2.9. Greenhouse Gas (GHG) Reporting Standard.** Upon written notice, Supplier shall cooperate with commercially reasonable requests by Rackspace related to compliance with GHG Reporting Standard (and any similar requirements applicable to Rackspace from time to time in any applicable jurisdiction) including but not limited to: providing Rackspace with access to emissions reports, data and systems, allowing Rackspace to audit emissions reports, data and systems, and/or cooperating with Rackspace in any compliance or enforcement actions. "**GHG Reporting Standard**" means (i) the Greenhouse Gas Protocol Corporate Accounting and Reporting Standard, Revised Edition 2015, (ii) Greenhouse Gas Protocol, GHG Protocol Scope 2 Guidance, An Amendment to the GHG Protocol Corporate Standard, 2015, and (iii) Greenhouse Gas Protocol, Corporate Value Chain (Scope 3) Accounting and Reporting Standard, Supplement to the GHG Protocol Corporate Accounting and Reporting Standard, 2011, each as amended periodically.

**2.10. Development and Use of AI**. The Services may not utilize or incorporate AI unless expressly stated in the Agreement or Order. Where Rackspace agrees that the Services may utilize or incorporate AI, Supplier (i) shall ensure that the use of AI does not breach, or cause Rackspace or any third party associated with Rackspace (including without limitation a Rackspace customer) to breach applicable law; (ii) shall ensure that the AI Services meet the requirements of the NIST AI Risk Management Framework (AI RMF), or provide written details of any deviation from AI RMF best practices prior to the effective date of the Agreement; (iii) shall on request provide a full written description of the AI Services, the underlying AI model and algorithms, the data or information processed within the AI Services (including training data), the output of the AI Services, and the results of testing of the AI Services; (iv) shall on request provide adequate information on the safety, security, privacy, validity, reliability, explainability, fairness, management of bias, and limitations in performance having implications on appropriate use of the AI Services; (v) shall not use Rackspace data or information (including output generated by Rackspace using the AI Services) for any other purposes (including in AI model training) other than the provision of Services to Rackspace, without the express written consent of a Rackspace authorized representative; (vi) shall ensure the AI Services do not result in the unauthorized or unlicensed use or disclosure of Rackspace data or information (including AI output generated by Rackspace); (vii) shall on request ensure that AI outputs are identifiable as being AI generated using robust provenance or watermarking (or both); and (viii) shall immediately notify Rackspace of potential vulnerabilities, risks or biases in the AI

Services. For the purposes of this section, "**AI**" means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.

**3. BACKGROUND SCREENING**. To the extent permitted by applicable law, for US personnel, Supplier shall conduct a background screening of each individual to whom it gives access to the Confidential Information (as defined by the Agreement) disclosed by Rackspace; such checks to be completed at the federal, state, and county levels, including each county where the individual has lived for the past seven years (or other reasonable requirements that Rackspace may communicate to Supplier from time to time). To the extent permitted by applicable law, for non-US personnel, Supplier shall use commercially reasonable efforts to meet the same criteria as established for US personnel plus a public records search and adverse media search, subject to general business practices in the respective country and industry, and further subject to reasonable availability of information and documentation. For all personnel, Supplier shall ensure each individual to whom it gives access to Confidential Information does not appear on any international sanctions list. The screening must be performed by a reputable third party screening service prior to the date that the individual is given access to Confidential Information. Supplier shall not disclose Confidential Information to an individual who has been found guilty of a felony offense or crime involving fraud, dishonesty, or moral turpitude. If subsequent to a background screening conducted in accordance with these requirements Supplier becomes aware of information that would result in an individual not satisfying a screening requirement, Supplier shall promptly suspend of remove that individual's access to Rackspace Confidential Information.

**4. RACKSPACE AUDIT**. Supplier shall maintain, at no additional cost to Rackspace, in a reasonably accessible location, all records pertaining to its compliance with the Agreement. Rackspace may, at its sole expense, perform a confidential audit of such Supplier records referenced above and Supplier's information technology systems, during normal business hours and at such reasonable times as Rackspace and Supplier may determine. Records available for review shall exclude any records pertaining to Supplier's other customers deemed proprietary and confidential and Supplier confidential and proprietary records not associated with the Agreement. Supplier agrees to cooperate fully with any such request or audit. Without limiting the foregoing, Supplier agrees that it will cooperate with any operational audit or certification process undertaken by Rackspace intended to evidence that Rackspace or a Rackspace customer meets hosting industry security standards (such as a Payment Card Industry Certification or applicable ISO standards), International Standards for Assurance Engagements No. 3402, or Statement on Standards for Attestation Engagements No. 16 or equivalent standards applicable in the relevant jurisdiction. Any breach of these Rackspace Supplier Compliance Terms shall constitute a material breach of the Agreement. The rights and obligations in this section 4 shall survive for the duration of the Agreement and for six years following expiration or termination of the Agreement.

**5. REGULATED END USER AUDIT**. This section shall apply only when the Services are provided for the benefit of a Rackspace end customer who is regulated under Applicable Financial Services Law or is subject to oversight by a Regulator ("**Regulated End User**"). Upon a Regulated End User or Rackspace's request, and on no less than 30 days advance notice (or such shorter notice legally required by a Regulator), Supplier shall permit audits as necessary to fulfil any legally enforceable request to a Regulated End User or Rackspace by any Regulator. A Regulator may also carry out its own audit of Supplier or may appoint a third party auditor to carry out an audit on its behalf, on reasonable prior written notice (or such shorter notice required under Applicable Financial Services Law). Supplier shall cooperate and provide assistance in respect of the audit in a commercially reasonable and timely manner. If the Regulated End User (or their affiliate) is subject to a Banking Act Measure: (i) the Regulated End User may transfer, novate or assign its rights and obligations under the Rackspace customer agreement, and Supplier shall provide all reasonable assistance to Rackspace and the Regulated End User (and their affiliates or businesses) to support any restructuring, reorganisation or transfer; and (ii) Supplier shall ensure that access to any key operational assets by Rackspace, the Regulated End User (and their affiliates and businesses) and the Regulator is not disrupted. Supplier shall provide all reasonable assistance to Rackspace to facilitate the effective planning for and effective taking of actions in the event of circumstances in which all or part of the Regulated End User's business is likely to fail, or the failure of all or part of the Regulated End User's business (including any necessary assistance executing the Recovery Plan and otherwise ensuring the continuity of the Services). Notwithstanding the exercise of any Banking Act Measure, or any deterioration in the financial circumstances of the Regulated End User (or affiliate), Supplier shall continue to provide the Services for the benefit of the Regulated End User in compliance with the terms of this Agreement without any variation due to the exercise of rights pursuant to the Banking Act Measure. Provisions which purport to limit, condition, constrain, restrict delay or block the exercise of rights pursuant to Banking Act Measure

shall be void and have no effect. "**Applicable Financial Services Law**" means the laws and regulations binding on the Regulated End User (as amended or replaced from time to time) including as related to financial services - including the Financial Services and Markets Act 2000 (FSMA), Directive 2004/39/EC (MiFID I), Directive 2014/65/EU (MiFID II) and Regulation (EU) 600/2014 (MiFIR), Directive 2009/138/EC (Solvency II) and Directive 2014/59/EU (BRRD) and the Banking Act 2009 (and any other delegated acts, implementing or secondary legislation, or associated procedures); together with any Regulator guidance or supervisory expectations. "**Banking Act Measure**" means any measure that is taken by a Regulator in relation to the Regulated End User (or an affiliate) under the Banking Act 2009, as amended or replaced from time to time. "**Recovery Plan**" means the recovery and resolution plans drawn up by the Regulated End User providing for measures to be taken by the Regulated End User to address or remove the causes of distress, and to restore its financial position following a significant deterioration of its and/or the Regulated End User's financial situation, as well as to achieve the stabilization of the Regulated End User's group, when in a situation of distress. "**Regulator**" means any entity, committee or body (including, as applicable, the Bank of England and European Banking Authority) entitled to supervise, regulate, investigate or influence the affairs of Regulated End User under Applicable Financial Services Law.

**6.** **GENERAL**: Supplier shall provide a written statement confirming that it has complied with all obligations set out in the Rackspace Supplier Compliance Terms on written request by Rackspace. Supplier shall immediately report to Rackspace any act or omission which may reasonably be regarded as a breach of the Rackspace Supplier Compliance Terms. Supplier shall ensure that its Affiliates, contractors and subcontractors agree to and comply with contractual provisions that are no less stringent than the obligations set out in the Rackspace Supplier Compliance Terms.