RapidScale Data Processing Agreement

This Data Processing Agreement ("DPA") between RapidScale and the Customer sets out the additional terms, requirements, and conditions on which RapidScale will obtain, handle, process, disclose, transfer, or store Personal Data when providing services under the Agreement. Unless otherwise defined in this DPA, all capitalized terms used in this DPA will have the meanings given to them in Section 14 "*Definitions and Interpretation*" of this DPA.

1. **DATA PROCESSING**.

    a. *Scope and Roles*. This DPA applies when Customer Data is processed by RapidScale; provided that, except as provided under Applicable Privacy Laws, this DPA does not apply to any data processed by a third-party product or service or any data that is transmitted through the Service(s), such as information entered on a non-RapidScale website or transmitted to a public network. The Customer and RapidScale acknowledge that for the purpose of any Applicable Privacy Law requirements, the Customer is the controller and RapidScale is the processor of the Customer Data. The Customer retains control of the Customer Data and remains responsible for its compliance obligations under Applicable Privacy Law, including providing any required notices and obtaining any required consents or legal bases for processing, and for ensuring the processing instructions it gives to RapidScale comply with all relevant legal requirements.

    b. *Customer Controls*. Customers can use the Service Controls to assist in meeting its obligations under Applicable Privacy Law, including its obligations to respond to requests from data subjects. Where required by Applicable Privacy Laws RapidScale will reasonably cooperate with Customer to erase or rectify inaccurate or outdated Customer Data by providing the Service Controls that Customer can use to erase or rectify Customer Data.

    c. *Details of Data Processing*. This sub-clause describes the general Customer Data categories and data subject types of RapidScale may process to fulfil the Business Purposes.

i. Subject matter: The subject matter of the data processing under this DPA is the processing of Customer Data necessary for RapidScale to provide the Services to the Customer, as described in the applicable Service Documents and Service Orders.

ii. Duration: The duration of the data processing is for the term of the Agreement and this DPA, unless a longer retention period is required by Applicable Privacy Laws or agreed upon in writing by the parties.

iii. Purpose: The purpose of the data processing under this DPA is to enable RapidScale to provide the Services as requested by the Customer and as necessary for the performance of the Agreement, including service delivery, security, maintenance, and support.

iv. Nature of the processing: The processing includes collection, storage, use, transmission, and deletion of Customer Data as necessary to provide RapidScale's Services, which include: RapidScale Public Cloud Services (e.g., Cloud Fabrics, General Public Cloud Services and Public Cloud Optimization) and Core Services (e.g., Public Cloud Application Services, Hosted Cloud, Network Services, End User Computing, DAAS, End Point Management, Data Protection, Support & Managed Services, Subscription Services and RapidScale Portal) as described in applicable Service Documents and purchased by Customer from time-to-time pursuant to a Service Order.

v. Type of Customer Data: All categories of Customer Data processed by the Services under Customer's RapidScale account. Customer may further specify those categories of Personal Data in each applicable Service Order.

vi. Categories of data subjects: the Data Subjects could include Customer's past and current clients, employees, suppliers, and users.

vii. Cross-Border Data Transfers Subject to Appropriate Safeguards: RapidScale will not transfer Customer Data outside the UK, EEA, or other jurisdictions with data transfer restrictions without the **prior written instructions or authorization of the Customer**, except where required to comply with applicable laws. Where such transfers occur, RapidScale shall implement appropriate safeguards,

including **Standard Contractual Clauses (SCCs), the UK International Data Transfer Agreement (IDTA), or other legally recognized mechanisms**.

viii. Approved Subcontractors: A list of RapidScale sub-processors is available upon written request.

ix. Compliance with Laws. Each party will comply with all laws, rules and regulations applicable to it, including Applicable Privacy Law.

2. **CUSTOMER INSTRUCTIONS.** RapidScale will only process the Customer Data to the extent, necessary for the Business Purposes and strictly in accordance with the Customer's documented instructions and Applicable Privacy Laws. RapidScale will not process the Customer Data for any other purpose unless explicitly instructed by the Customer in compliance with Applicable Privacy Laws. If RapidScale determines that a Customer instruction conflicts with applicable law, it will promptly notify the Customer, unless prohibited by law. RapidScale will not be required to comply with any instruction that would cause it to violate applicable law but will work with the Customer in good faith to find a legally compliant solution.

   RapidScale must promptly comply with any Customer request or instruction requiring RapidScale to amend, transfer, delete the Customer Data, or stop, mitigate, or remedy any unauthorized processing. Except as directed by the Customer, RapidScale will not retain, use, or disclose Personal Data from Customer for any commercial purpose other than (a) for the limited and specific purposes of providing the Services under the Agreement; (b) using the Personal Data for the operational purposes permitted by Applicable Privacy Law; such as security, fraud prevention, and debugging; and (c) for complying with legal obligations, including regulatory requirements or law enforcement requests . Except as instructed by Customer or as otherwise permitted under the Agreement, RapidScale will not retain, use, or disclose Personal Data outside of its direct business relationship with Customer or "sell" or "share" (as defined by Applicable Privacy Law) the Personal Data. Except as permitted by Applicable Privacy Law or this DPA, RapidScale agrees not to combine Personal Data with other Personal Data that RapidScale receives from another entity or that RapidScale collects itself; provided that this does not restrict RapidScale from combining data as authorized by Customer or processing Personal Data in the same system(s) that process Personal Data on behalf of itself or others.

3. **CONFIDENTIALITY OF CUSTOMER DATA.** RapidScale will maintain the confidentiality of all Personal Data and will not disclose Customer Data to third parties unless (a) the Customer or this DPA expressly authorizes the disclosure; or (b) as required to engage sub-processors under a written contract imposing equivalent data protection obligations or as required by Applicable Privacy Law; or (c) as required by law. If RapidScale is legally required to process or disclose Customer Data to a third party, it will notify the Customer before complying with the request, unless legally prohibited from doing so. If permitted, RapidScale will provide the Customer with an opportunity to object or challenge the disclosure

4. **RAPIDSCALE PERSONNEL**. RapidScale restricts its personnel from processing Customer Data without authorization by RapidScale as described in the Security Standards. RapidScale imposes appropriate obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security. RapidScale will ensure that all its personnel who have access to or are involved in processing Personal Data:

    a. are informed of the Personal Data's confidential nature and use restrictions and are obliged to keep the Personal Data confidential;

    b. have undertaken training on the privacy and data protection requirements relating to handling Personal Data and how it applies to their particular duties; and

    c. are aware both of RapidScale's duties and their personal duties and obligations under the Privacy and Data Protection Requirements and this Agreement.

5. **SECURITY OF PROCESSING**

    a. *TOMs*. RapidScale must at all times implement appropriate technical and organizational measures designed to safeguard Personal Data against unauthorized or unlawful processing, access, copying, modification, storage, reproduction, display, or distribution, and against accidental loss, unavailability, destruction, or damage including, but not limited to, the security measures set out in Annex 1.

b. *Customer Security Controls*. Customer can elect to implement technical and organizational measures to protect Customer Data. RapidScale makes available Service Controls that Customer can elect to use. Customer is responsible for (a) properly configuring the Services, (b) using the Service Controls to allow Customer to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident, and (c) taking such steps as Customer considers adequate to maintain appropriate security, protection, and deletion of Customer Data, which includes use of encryption technology to protect Customer Data from unauthorized access and measures to control access rights to Customer Data.

6. **SUBPROCESSING**.

a. *Authorized Subprocessors*. Customer provides general authorization to RapidScale's use of subprocessors to provide processing activities on Customer Data on behalf of Customer ("**Subprocessor**") in accordance provided that RapidScale may only authorize a third party (subcontractor) to process the Personal Data if:

i. to the extent required by Applicable Privacy Laws, the Customer is provided with an opportunity to object within 30 days after RapidScale supplies the Customer with full details regarding such subprocessor;

ii. RapidScale enters into a written contract with the subprocessor that contains terms substantially the same as those set out in this DPA and, upon the Customer's written request, provides the Customer with copies of such contracts; and

iii. RapidScale maintains control over all Customer Data it entrusts to the subprocessor.

b. Where the subprocessor fails to fulfil its obligations under the written agreement described in clause 6 (a) ii, RapidScale remains fully liable to the Customer for the subprocessor 's performance of its agreement obligations. The parties consider RapidScale to control any Personal Data controlled by or in the possession of its subprocessor.

c. Upon the Customer's written request, and subject to reasonable confidentiality and security requirements, RapidScale will provide the Customer with relevant documentation or certifications demonstrating a sub-processor's compliance with its obligations regarding Customer Data. If such documentation is insufficient to verify compliance, the Customer may request an audit of the sub-processor, which shall be conducted by RapidScale or an independent third-party auditor engaged by RapidScale, with the results made available to the Customer upon request. RapidScale shall ensure that its sub-processors provide reasonable cooperation in such audits.

7. **DATA SUBJECT REQUESTS AND COMPLAINTS.**

a. RapidScale must promptly notify the Customer if it receives any complaint, notice, or communication that relates directly or indirectly to the processing of the Customer Data or to either party's compliance with Applicable Privacy Law application to the subject matter of the Agreement.

b. RapidScale must notify the Customer within 5 working days if it receives a request from an individual for access to their Personal Data or similar request to exercise one of the Data Subject's personal data rights.

c. Taking into account the nature of the processing, the availability of the Service Controls to Customer are the technical and organizational measures by which RapidScale will provide reasonable assistance to the Customer in fulfilling the Customer's obligations to respond to data subjects' requests, complaints, or regulatory inquiries in accordance with Applicable Privacy Laws.

8. **SECURITY INCIDENTS**.

a. *Security Incident*. RapidScale will notify Customer of a Security Incident involving Personal Data without undue delay but no later than required by Applicable Privacy Law. The notification will include, to the extent known at the time, a description of the nature of the Security Incident, and any initial mitigation measures taken or proposed. RapidScale will provide further updates as additional information becomes available. RapidScale will take appropriate measures to address the Security Incident, including measures to mitigate any adverse effects resulting from the Security Incident.

b. *RapidScale Assistance.* RapidScale will reasonably cooperate with the Customer to assist in its compliance with Applicable Privacy Laws, including any obligations to notify supervisory authorities, regulators, or affected data subjects. RapidScale will provide relevant information in a phased manner as it becomes available, taking into account the nature of the processing, the information available to RapidScale. However, the Customer, as the controller, is responsible for assessing whether the Security Incident requires regulatory or data subject notification and determining the appropriate actions. Taking into account the nature of the processing, Customer agrees that it is best able to determine the likely consequences of a Security Incident and the identity of any impacted data subject.

c. *Unsuccessful Attempts.* The Customer acknowledges that not all security events constitute a Security Incident requiring notification. RapidScale will assess security events in good faith and notify the Customer without undue delay if an event involves unauthorized access, disclosure, loss, alteration, or destruction of Personal Data. RapidScale's obligation to report or respond to a Security Incident under this Section does not constitute an admission of fault or liability regarding the Security Incident.

d. *Communication*. Notification(s) of Security Incidents, if any, will be delivered to one or more of the email addresses listed in a Service Order.

e. *Notification Obligations*. If RapidScale notifies Customer of a Security Incident, or Customer otherwise becomes aware of any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data, Customer will be responsible for (a) determining if there is any resulting notification or other obligation under Applicable Privacy Law and (b) taking necessary action to comply with those obligations. This does not limit RapidScale's obligations under this Section 8.

9. **CUSTOMER AUDITS.**

a. To the extent required under Applicable Privacy Law, RapidScale will permit the Customer and its authorized third-party representatives to audit RapidScale's compliance with its DPA obligations upon at least 10 days' notice, during the term and for three years after this DPA terminates. RapidScale will provide reasonable cooperation and assistance for such

audits. The notice requirement shall not apply where the Customer reasonably believes that a Security Breach has occurred or is occurring, or if RapidScale is in material breach of its obligations under this DPA or any Applicable Privacy Law.

b. To the extent permitted under Applicable Privacy Law, RapidScale may satisfy any audit or inspection request by providing a copy of its Due Diligence Package

10. **TRANSFERS OF PERSONAL DATA.**

a. Location. Once Customer has made its choice, RapidScale will not transfer Customer Data from Customer's selected location(s) except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or valid and binding order of a governmental body.

b. If the Applicable Privacy Law restrict cross-border Personal Data transfers, the Customer will only transfer that Personal Data to RapidScale under the following conditions:

1. RapidScale, either through its location or participation in a valid cross-border transfer mechanism under Applicable Privacy Law (such as SCCs, Binding Corporate Rules, an adequacy decision under GDPR or the UK GDPR, or an equivalent framework under applicable law), is legally permitted to receive that Personal Data. RapidScale must identify in Section 1 c(vii) the lawful transfer mechanism(s) that enables it to receive such Personal Data and must promptly inform the Customer of any changes that affect compliance.

2. RapidScale must inform the Customer if its ability to lawfully receive Customer Data under the identified transfer mechanism is invalidated or materially impacted.

c. The Customer has ensured that the transfer is otherwise legally permissible under the Applicable Privacy Law.

d. *Standard Contractual Clauses*. SCCs will only apply to a Data Transfer. When Customer is acting as a Controller, the Controller-to-Processor SCCs will apply to a Data Transfer. Processor-to-Processor SCCs s shall apply where the

Customer is acting as a processor on behalf of a third-party controller, and RapidScale is acting as a sub-processor.

Taking into account the nature of the processing, Customer agrees that it is unlikely that RapidScale will know the identity of Customer's controllers because RapidScale has no direct relationship with Customer's controllers and therefore, Customer will fulfil RapidScale's obligations to Customer's controllers under the Processor-to-Processor Clauses.

The parties agree that, with respect to the elements of the SCCs that require the parties' input: (a) the content of this DPA prepopulates the relevant sections of Annex I and Annex II of the SCCs; (b) Option 2 of Clause 9 (general authorization of sub-processors) of the SCCs shall apply in relation to Customer's authorization of the use of Subprocessors and RapidScale shall notify Customer in writing of any intended changes to that list through the addition or replacement of Subprocessors at least 30 days in advance and in accordance with Section 6(a) of this DPA; (c) notwithstanding any clause to the contrary in the Agreement, the parties agree that any dispute arising from the SCCs shall be resolved by the courts located in Germany in accordance with Clause 18 of the SCCs; (d) the parties agree that both the Docking Clause 7 in the SCCs and the optional wording in Clause 11 of the SCCs relating to an independent dispute resolution body shall not be included; and (e) Customer may exercise its right of audit under clause 8.9 of the SCCs as set out in, and subject to the requirements of, Section 9 of this DPA.

e. *Supplementary Measures & Transfer Impact Assessments:* Where required under Applicable Privacy Laws, both parties agree to conduct and document a Transfer Impact Assessment (TIA) or Transfer Risk Assessment (TRA), as appropriate, before executing any Data Transfer under the SCCs. If the assessment indicates that the Third Country does not provide an essentially equivalent level of protection, Customer shall implement appropriate supplementary measures.

f. *Legal Invalidity & Alternative Mechanisms:* If at any time the SCCs are invalidated, deemed insufficient, or require amendment due to changes in law (e.g., regulatory guidance, court rulings such as Schrems II), the parties agree to work together in good faith to establish an alternative lawful data transfer mechanism consistent with Applicable Privacy Law requirements.

g. RapidScale will not transfer any Customer Data to another country unless the transfer complies with the Applicable Privacy Law.

11. **TERMINATION**. This DPA will continue in force for so long as: the Agreement remains in effect; RapidScale retains any Customer Data related to the Agreement in its possession or control including backups and archived copies; or any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Agreement in order to protect Personal Data will remain in full force and effect.

    If a change in any Applicable Privacy Law or either party's circumstances prevent a party from fulfilling its data processing obligations under this DPA or the Agreement, the parties shall promptly suspend the processing of Customer Data until compliance with the applicable requirements is achieved. Both parties agree to make reasonable, good-faith efforts to modify or supplement the Agreement to ensure compliance, including implementing supplementary measures where required (e.g., SCCs, contractual updates, technical safeguards). If compliance cannot be achieved within 45 days, either party may terminate the Agreement by providing written notice to the other party.

12. **RETURN OR DELETION OF CUSTOMER DATA.**

    a. At any time up to the date of termination, and for 90 days following, subject to the terms and conditions of the Agreement, RapidScale will return or delete Customer Data when Customer uses Service Controls to request such a return or deletion. No later than the end of this 90-day period, Customer will close all RapidScale accounts containing Customer Data. Customer authorizes this retention following termination to allow Customer to transition the Customer Data.

    b. At the Customer's request, RapidScale will give the Customer a copy of, or access to, the Customer Data in its possession or control

    c. On termination of the Agreement for any reason or expiry of its term, RapidScale will securely destroy or, if directed in writing by the Customer, return and not retain, the Customer Data related to this agreement in its possession or control, except where required by applicable law, and, in such cases, shall only retain one copy strictly for legal, regulatory, or audit compliance purposes for a period not exceeding 12 months, unless a longer

retention period is legally required. Any retained Customer Data shall remain subject to confidentiality and security obligations as outlined in this DPA.

d. If any law, regulation, government, or regulatory body requires RapidScale to retain any documents or materials that RapidScale would otherwise be required to return or destroy, it will notify the Customer in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

e. Customer will close all RapidScale accounts containing Customer Data.

13. **ENTIRE AGREEMENT.**

The EU Standard Contractual Clauses (EU SCCs) adopted by the European Commission are hereby incorporated reference and form an integral part of this DPA. The parties shall comply with the obligations set forth in the EU SCCs. For data transfers subject to the UK GDPR, the parties agree to apply the UK Addendum to the EU SCCs, as approved by the UK Information Commissioner's Office (ICO) on 21 March 2022. The UK Addendum is incorporated by reference, and the parties agree to comply with its terms.

Except as amended by this DPA, the Agreement will remain in full force and effect. In the event of any conflict between the Agreement and this DPA, the terms of this DPA shall prevail. However, if there is any conflict between this DPA (including its annexes) and Standard Contractual Clauses (SCCs), the terms of the SCCs shall take precedence.

14. **GOVERNING LAW AND JURISDICTION.**

This DPA shall be governed by the laws applicable to the data protection regime governing the processing of Personal Data. Where processing is subject to the EU GDPR, the laws of the relevant EEA Member State shall apply. For processing under the UK GDPR, the laws of England and Wales shall govern. If other data protection laws apply, the governing law shall be that of the relevant jurisdiction.

Where the EU SCCs or the UK Addendum apply, their governing law provisions shall prevail. This clause applies solely to this DPA and does not alter the governing law of the main Agreement, except as required by applicable law.

15. **DEFINITIONS AND INTERPRETATION.**

All capitalized terms used in this DPA will have the meanings given to them below:

"Agreement" means the RapidScale Terms and Conditions available at rapidscale.com/terms-and-conditions, as updated from time to time, or any other Agreement entered into between RapidScale and the Customer as a result of which Customer Data is processed.

"**Applicable Privacy Law**" means all applicable laws and regulations relating to the processing, protection, or privacy of Personal Data, including where applicable, the guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction. This includes, but is not limited to the GDPR, UK GDPR and applicable U.S. privacy law or regulation.

"**Business Purpose"** means the services described in the Agreement or any other purpose specifically identified in this DPA.

"**Customer Data**" means the Personal Data that is uploaded to the Services under Customer's RapidScale accounts.

"**Data Transfer**" means a transfer of the Customer Data that is subject to GDPR or UK GDPR and is transferred, either directly or via onward transfer, to any country that does not benefit from an adequacy decision under the Applicable Privacy Law.

"**GDPR**" means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"**Personal Data**" means personal data, personal information, personally identifiable information or other equivalent term (each as defined in Applicable Privacy Law).

"**Processing, processes, and process**" means any activity that involves the use of Personal Data, or as the Applicable Privacy Law may otherwise define the terms processing, processes, or process. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including organizing, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring Personal Data to third parties.

"**Security Incident**" means a breach of RapidScale's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

"**Security Standards**" means the security standards attached to this DPA as Annex 1.

"**Service Controls**" means the controls, including security features and functionalities, that the Services provide, as described in the Service Documents.

"**Standard Contractual Clauses**" or "**SCCs**" "means, collectively: (a) the EU Standard Contractual Clauses for the transfer of Personal Data from the European Economic Area (EEA) to third countries, as set out in the annex to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021, pursuant to Regulation (EU) 2016/679 (GDPR); (b) the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU SCCs, as approved by the UK Information Commissioner's Office (ICO); and (c) any other applicable contractual clauses approved under data protection laws governing international transfers of Personal Data. As of the date of this Agreement, a reference to "Controller-to-Processor Clauses" means Module 2 (controller-to-processor), and "Processor-to-Processor Clauses" means Module 3 (processor-to-processor) of the EU SCCs.

"**Third Country**" means a country outside the EEA not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR).

"**UK GDPR**" means the GDPR as applicable as part of UK domestic law by virtue of section 3 of the EU (Withdrawal) Act 2018, as amended by the Data Protection, Privacy and Electronic Communications (EU Exit) Regulations 2019.

Annex 1 Security Standards

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the Agreement. The following Technical and Organizational Security Measures apply to the following RapidScale Services:

Generally, RapidScale does not require access to Customer Data to perform most of its Services. However, RapidScale offers certain Services that require access to Customer Data including, without limitation, customized service offerings, artificial intelligence services, machine learning services, database management/administration services, or

application modernization services (the "**Limited Services**"). Upon purchase of a Limited Service, Customer must disclose to RapidScale the nature of the data that will be accessed by such Limited Services.

RapidScale employees have privileged level access to Customer Data where single sign-on, privileged accounts are used. RapidScale follows security practices and any applicable laws to implement the appropriate level of security and privacy controls. This will ensure an appropriate level of security taking into account the nature, scope, context, and purposes of processing and the risks for the rights and freedoms of natural persons, including maintaining the following safeguards to protect Customer Data:

Organizational Safeguards

- *Security Program*. RapidScale has designated an information security team that identifies reasonably foreseeable internal and external risks, assesses the sufficiency of safeguards, and adjusts the security program based on business changes. RapidScale reviews risks and prioritizes security-related projects and initiatives.
- *Security Policies*. Information security policies are made available to relevant personnel and reviewed periodically.
- *Hiring*. RapidScale requires all workforce members to review and agree to its information security policies.
- *Training*. RapidScale trains workforce members that have access to Customer Data concerning appropriate privacy, security practices, secure coding practices and compliance with RapidScale's data protection obligations. RapidScale also provides mandatory information security training upon hire and annually thereafter.
- *Third-Party Assessments*. RapidScale conducts risk assessments for all vendors that process Customer Data.
- *Industry Standards*. RapidScale complies with the following industry standards: SOC 1 Type 2, SOC 2 Type 2, PCI, ISO 27001, HIPAA, HITRUST, GDPR.

Physical Safeguards

- *Access Control:* RapidScale's colocations where Customer Data is hosted within a third-party facility have physical security systems that are monitored. These measures include: (i) key card access monitoring; (ii) video monitoring of all entrance

locations to the facilities; (iii) flood alert systems; (iv) temperature monitoring; and (v) management of user access. Unauthorized persons are prohibited from gaining access to premises, buildings, or rooms, where systems are located which Process Customer Data. RapidScale's facilities that Process Customer Data are monitored via video surveillance. Networking and other required equipment are secured in areas restricted only to personnel that require access to provide the Service(s) to Customer.

- *Termination of Access:* RapidScale terminates access to its facilities when a workforce member is terminated by RapidScale. This process has been documented.
- *Data Destruction:* RapidScale complies with its written policies and procedures with respect to its retention of Customer Data. RapidScale has a process in place to delete data after a predetermined time for each data type. RapidScale securely destroys or returns Customer Data in accordance with its Data Processing Agreements and does not maintain data longer than is reasonably necessary for a legitimate business purpose (including providing Services for Customer). Equipment that contains Customer Data shall be erased prior to recycling so that the Customer Data cannot be read or reconstructed.

Technical Safeguards

- *Data Access Controls:* RapidScale has policies and procedures in place designed to ensure that access to Customer Data by our workforce members is within their scope of duty and is appropriate based on job function.
- *Segmentation:* Each Customer has their own logical environment with separate controls and control enforcement in alignment with their own standards and controls."
- *Data Minimization:* RapidScale only collects Customer Data where necessary for the operation of the Service(s).
- *Privileged Access:* RapidScale manages the issuance of privileged credentials including multifactor authentication. RapidScale monitors and manages the users and access to Customer Data. Credentials follow RapidScale's privileged access management policy requirements. Credentials will not be hardcoded in any system, code, or configuration.

- *Anti-malware:* RapidScale complies with its malicious code and anti-virus/malware detection standards, which sets forth procedures for implementing malicious code protection on specified systems. Controls are developed, implemented, monitored, and maintained to ensure appropriate notification of malware events and review of malware controls, to prevent compromise of confidentiality, availability, and integrity of the Services.
- *Security Patches:* RapidScale implements standards related to system updates and deployment of security patches on a regular basis. Updates rated as critical shall be evaluated for impact and deployed on an accelerated timeline.
- *System Security:* RapidScale's individually assigned computers are configured to automatically lock after a period of inactivity. Business systems that are deemed critical by RapidScale are backed up and encrypted. Remote access to Customer environments is through encrypted secure communications.
- *Incident Response:* RapidScale complies with its incident management process; a written procedure for responding to Personal Data Breach (including notifying impacted Customers). Following the occurrence of any Personal Data Breach, the team will perform a root cause analysis and create a remediation plan designed to prevent similar incidents from occurring in the future. RapidScale's security incident management procedure is reviewed at least annually.
- *Vulnerability Management and Penetration Testing: Vulnerability* scans are conducted on a regular basis against RapidScale's internal and external systems. Vulnerabilities are regularly reviewed and prioritized for remediation based on severity and assigned a remediation timeline. RapidScale conducts at least annual pen tests on all publicly exposed systems and platform tools that are leveraged to provide services to RapidScale clients.
- *Product and Platform Testing: Testing* is required for any changes prior to production deployment.
- *Encryption:* RapidScale utilizes commercially available and industry standard encryption technologies for Customer Data at rest and in motion.
- *Resilience and Business Continuity:* RapidScale supports the alignment of business continuity and disaster recovery program with industry standards including recovery of time objectives and business continuity plans and implements and maintains its

disaster recovery process; a written policy that defines procedures for disaster recovery (including procedures for backup and recovery for in scope systems). RapidScale supports redundancy of information processing facilities for disaster recovery purposes. RapidScale reviews and validates all established and implemented disaster recovery processes at least annually.