****Ask your Druva Sales representative for a signable copy of this agreement****

This Druva Data Resiliency Guarantee Agreement ("**Agreement**") describes the terms and conditions for the provision of a guarantee ("**Guarantee**") by Druva Inc. ("**Druva**") to Customer in respect of its purchase of an Eligible Druva Solution (defined below).

1. DEFINITIONS.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with Customer. **"Control"** for purposes of this definition means direct or indirect ownership or control of more than 50% of the voting interests of Customers.

"Availability SLA" means that the Cloud Services will be available not less than 99.5% of the time during a Reporting Period according to the following calculation:

Availability = (total hours in Reporting Period – unscheduled maintenance which causes unavailability – scheduled maintenance) / (total hours in reporting period – scheduled maintenance) X 100%.

Unscheduled maintenance may be required to resolve issues that are critical for Customer and/or performance of the Cloud Services. Druva will use its commercially reasonable efforts to notify Customer at least six (6) hours prior to the unscheduled maintenance.

The following shall be excluded when calculating Availability: (i) unavailability caused by force majeure; (ii) any problems resulting from Customer combining or merging the Cloud Services with any hardware or software not supplied by Druva or not identified by Druva in writing as compatible with the Cloud Services; (iii) interruptions or delays in providing the Cloud Services resulting from telecommunications or Internet service provider failures; or (iv) any interruption or unavailability resulting from Customer's use of the Cloud Services in an unauthorized or unlawful manner or any interruption resulting from the misuse, improper use, alteration or damage of the Cloud Services.

"Cloud Services" means Druva's software-as-a-service solution for managing data availability and information governance, any feature or functionality add-ons, and any modified versions of, and upgrades, updates and additions to such solution, ordered by Customer under a valid order form that is accepted by Druva.

"Confidentiality SLA" means that Customer Data is not compromised as a result of a Security Incident.

"Customer" means the entity purchasing an Eligible Druva Solution directly from Druva or indirectly through an authorized Druva reseller.

"Customer Agreement" means the fully signed agreement(s) governing Customer's use of the Eligible Druva Solution between: 1. Druva and Customer; or 2. Customer and an authorized Druva reseller.

"Customer Data" means the data, information, and materials of Customer that Customer or its authorized users uploads to, stores on, or accesses with an Eligible Druva Solution.

"Customer Policies" means a configurable set of policies that the Customer applies correctly to the Cloud Services, including to the Eligible Druva Solution, to achieve specific data protection objectives.

"Discovery Time" means the exact time at which the Customer first discovers the Ransomware Incident or Security Incident.

"Durability SLA" means 99.999% of Customer Data backed up is recoverable. The Durability SLA does not extend to unsuccessful recovery of Customer Data due to failure of a third party cloud service provider.

"Eligible Druva Solution" means a subscription of at least thirty-six (36) months for the following Druva solutions: 1. Druva Enterprise or Druva Elite; and 2. Druva Backup Security Posture and Observability.

"Event Date" means the date the Ransomware Incident or Security Incident ("Incident") first occurred; provided, however that each Incident that forms part of the same, continuous, related or repeated Ransomware Incident or Security Incident ("**Related Incident")** shall be deemed to have the Event Date of the earliest Incident or Pre-existing Incident (if applicable) that forms part of the Related Incident.

"Guarantee Period" means the period beginning on the date Customer deploys the Eligible Druva Solution and ending on the earlier of the: 1. End date of the Eligible Druva Solution's initial subscription term; or 2. The termination date of this Agreement.

"Health Check" means the performance and configuration review by Druva and the resulting recommendations for various Druva platform configurations and system statuses, including but not limited to security best practices, data backup and related policies to ensure the Druva platform is optimized for data protection, recovery and restore operations.

"Health Check Period" means the period beginning on the subscription start date for the Eligible Druva Solution and ending ninety (90) days thereafter, unless otherwise agreed in writing and signed by an authorized representative of each party.

"Immutability SLA" means that the last successful backup of Customer Data will be recoverable in the event of a Ransomware Incident. The Immutability SLA does not extend to unsuccessful recovery of Customer Data due to (i) Customer's lost access credentials (including encryption keys), which Druva is unable and has no obligation to recover, (ii) failure of a third party cloud service provider; or (iii) conditions or policies not covered by, or inconsistent with, Customer Policies.

"Payment" means reimbursement of Recovery Incident Expenses that directly result from a Recovery Incident or reimbursement of Security Incident Expenses that directly result from a Security Incident.

"Pre-existing Incident" means the actual or reasonably suspected presence of Ransomware in the Customer environment (i) prior to the Customer's applicable Guarantee Period or (ii) during a period

of non-compliance with any Health Check and/or the Requirements within the Customer's applicable Guarantee Period.

"Ransomware" means malware from an unauthorized external source, which blocks access to a Customer's computer system, files and/or data ("Customer Files") by encrypting a material portion of Customer Files and rendering them unusable. Ransomware does not include any malware introduced by the Customer (or any third party technology used or licensed by the Customer) to the Customer's internal systems, whether intentionally (e.g., malware testing) or through a breach in the Customer systems' security.

"Ransomware Incident" means a demand for payment made by a cybercriminal in exchange for decrypting the encrypted Customer Files infected by the Ransomware.

"Recovery" means in the event of a Ransomware Incident with an Event Date that occurs during the Guarantee Period, the Eligible Druva Solution will enable Customer to materially restore the Customer Data that was successfully backed up using the Eligible Druva Solution during the Guarantee Period.

"**Recovery Incident**" means an unsuccessful Recovery.

"Recovery Incident Expenses" means solely (and to the exclusion of all other fees, expenses, losses, settlements and damages) the reasonable and necessary fees and expenses to restore, recover, or recreate Customer Data under the Guarantee at the time of the Ransomware Incident to the extent incurred by Customer as a direct result of a Recovery Incident. The foregoing fees and expenses constitute "Recovery Incident Expenses" only if: (1) incurred by Customer after obtaining Druva's prior written approval to procure such services or incur such expenditures; (2) paid to a third party pre-approved in writing by Druva; (3) incurred by Customer within one (1) year following the Discovery Time of the applicable Ransomware Incident; and (4) payment and/or reimbursement does not violate any applicable domestic or foreign law, statute, regulation or rule as determined by Druva in its sole discretion. For clarity, Recovery Incident Expenses do not include (i) any third party payment demand or ransom in connection with the Ransomware, (ii) any third-party restoration, recovery, or recreation attempts on a Druva platform or a Druva hosted cloud platform, (iii) the cost of restoration, recovery, or recreation for Customer's environment(s) managed or protected by Druva and not successfully replicated to Eligible Druva Solution software or a Druva hosted cloud platform, (iv) attorney's fees, or (v) third party consultant or expert fees.

"Reliability SLA" means that during a Reporting Period 99% of backups will complete successfully in accordance with Customer Policies and within forty-eight (48) hours of a failed backup. The Reliability SLA shall be void if any one of the following occurs: 1. The backup cannot be performed or completed because of any actions, policies, or restrictions of third-party data hosts or service providers; 2. The Customer device or data source is corrupted, offline, or otherwise inaccessible during the backup window; 3. The Customer's network, device or data source is insufficient for the required data transfer; or 4. A force majeure event.

"Reporting Period" means a calendar month.

"Security Incident" means a breach of the security of the Eligible Druva Solution solely caused by Druva that directly results in the unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

"Security Incident Expenses" means the following damages incurred because of a Security Incident: (a) data breach notifications, (b) credit monitoring services, (c) fraudulent transactions, (d) the establishment of a call center to respond to inquiries from Customers clients and/or personnel, and/or (e) fines, costs or penalties imposed upon Customer by a governmental authority. The foregoing fees and expenses constitute "Security Incident Expenses" only if: (1) incurred by Customer after obtaining Druva's prior written approval to procure such services or incur such expenditures; (2) paid to a third party pre-approved in writing by Druva; (3) incurred by Customer within one (1) year following the Discovery Time of the applicable Security Incident; and (4) payment and/or reimbursement does not violate any applicable domestic or foreign law, statute, regulation or rule as determined by Druva in its sole discretion. For clarity, Security Incident Expenses do not include (i) any third-party restoration, recovery, or recreation attempts on a Druva platform or a Druva hosted cloud platform, (ii) the cost of restoration, recovery, or recreation for Customer's environment(s) managed or protected by Druva and not successfully replicated to Eligible Druva Solution software or a Druva hosted cloud platform, (iii) attorney's fees, or (iv) third party consultant or expert fees.

2. DATA RESILIENCY GUARANTEE.

Subject to the terms, conditions and exclusions in this Agreement and for the duration of the Guarantee Period, Druva guarantees to Customer that it will satisfy each of these five SLAs: (a) Availability SLA; (b) Durability SLA; (c) Reliability SLA; (d) Confidentiality SLA; and (e) Immutability SLA (the "Guarantee"). This Guarantee extends only to Customer and does not extend to any third parties (including, but not limited to suppliers, service providers, end-clients, and employees or agents of Customer) or any of their losses or damages.

3. REMEDY FOR BREACH OF AVAILABILITY SLA, DURABILITY SLA OR RELIABILITY SLA.

If Druva fails to meet the Availability SLA, Durability SLA or Reliability SLA ("SLA Failure"), then Druva will provide a service credit to Customer equal to 10% of one month of Eligible Druva Solution subscription fees for each period of failure.

Any Customer request for a service credit under this Agreement may only be made on a calendar month basis and must be submitted in writing to Druva within ten (10) days after the end of the relevant calendar month or shall be deemed to have been waived by Customer.

If the same SLA Failure occurs in three (3) consecutive Reporting Periods (e.g. failure of the Availability SLA in three consecutive calendar months), then Customer shall have the right to terminate the Customer Agreement upon written notice to Druva and Customer shall receive (directly or through the reseller with which Customer contracted) a prorated amount of the applicable fees prepaid by

Customer covering the whole months that would have remained in the subscription period, absent such early termination.

The right to a service credit and the right to terminate the Customer Agreement (according to the foregoing paragraph) shall be the sole and exclusive remedy available to Customer in the event of an SLA Failure. For the duration of the Guarantee Period, Customer's rights and remedies in respect of the Availability SLA shall prevail over the same or similar SLA in the Customer Agreement and Customer shall be barred from receiving service credits available to Customer in the Customer Agreement.

4. REMEDY FOR BREACH OF CONFIDENTIALITY SLA OR IMMUTABILITY SLA

Subject to the terms herein, Customer's sole and exclusive remedy, and Druva's entire liability for Druva's failure to meet the Confidentiality SLA or the Immutability SLA, will be to reimburse Customer for its Recovery Incident Expenses directly resulting from the Recovery Incident or, in the case of a Security Incident, for its Security Incident Expenses directly resulting from the Security Incident, up to a maximum payment amount not to exceed the applicable Cap set forth in the table below.

Aggregate Payments for multiple Recovery Incidents with Event Dates in the Guarantee Period shall not exceed the Cap.

Annualized Total Amount of Subscription Fees Paid by Customer for all Druva solutions, including any Eligible Druva Solution*	**Payment Cap ("Cap")***
$25,000 - $49,999	**$100,000**
$50,000 - $99,999	**$250,000**
$100,000 - $249,999	**$750,000**
$250,000 - $499,999	**$2,000,000**

$500,000 - $999,999	**$4,500,000**
$1,000,000+	**$10,000,000**

*Figures expressed in U.S. Dollars are subject to foreign currency conversion where applicable and at the prevailing rate when payment is made

Pre-existing and Related Incidents. This Guarantee does not extend to Pre-existing Incidents or Related Incidents that include a Pre-existing Incident. Except as set forth in this Section 4, all Recovery Incident Expenses resulting from a Related Ransomware Incident and all Security Incident Expenses shall be subject to the terms, conditions, exclusions and Cap in effect on the Event Date of the first discovered Ransomware Incident or first discovered Security Incident that forms part of the Related Ransomware Incident.

Election of Remedies – Security Incident. Notwithstanding anything to the contrary herein and to the extent that the Customer Agreement permits recovery for a claim from facts giving rise to a Security Incident, Customer shall elect between its remedy permitted by: 1. the Customer Agreement or 2. this Agreement. This election of remedies is required to prevent a double recovery.

DISCLAIMER. EXCEPT FOR THE LIMITED GUARANTEE PROVIDED IN SECTION 2 OF THIS AGREEMENT AND ANY WARRANTIES PROVIDED IN THE CUSTOMER AGREEMENT, THE ELIGIBLE DRUVA SOLUTION IS PROVIDED AS IS.

5. CONDITIONS PRECEDENT TO GUARANTEE PAYMENT OR SERVICE CREDITS.

Druva shall only provide payment to Customer (or service credits where applicable) if, at the time of the Ransomware Incident or Security Incident (or Druva's breach of the Availability SLA, Durability SLA, or Reliability SLA where applicable) and throughout the Guarantee Period:

1. Customer has maintained an active subscription for the Eligible Druva Solution with a total annual subscription of no less than twenty-five thousand U.S. dollars ($25,000) or the equivalent amount in foreign currency (calculated as of the date of the initial subscription);
2. Customer had deployed the most recent version of the Eligible Druva Solution and any applicable security patches;
3. The Event Date and Discovery Time of the Ransomware Incident occurred, was discovered by Customer, and reported to Druva during the Guarantee Period, and in accordance with Section 7;

4. The Event Date and Discovery Time of the Security Incident occurred, was discovered by Customer, and reported to Druva during the Guarantee Period, and in accordance with Section 7;

5. Customer has remained in compliance with its Customer Agreement, including without limitation any payment obligations;

6. Customer has fully cooperated with Druva, including without limitation by (i) implementing and complying with all remedial and security measures required by Druva including the Requirements, (ii) providing Druva with all documentation (including any internal or external security investigation reports), permissions, and access to relevant systems and environments required to verify Customer is entitled to Payment, and (iii) complying with the Reimbursement Request process set forth in Section 8;

7. Any systems to which the Customer seeks to restore Customer Data successfully backed up by Druva are free of any malware, bugs, back-doors or other malicious code, and are otherwise secured;

8. Customer has completed and passed the Health Check prior to the expiration of the Health Check Period; and

9. This Guarantee is not restricted or prohibited by applicable law.

6. REQUIREMENTS.

Customer acknowledges and agrees that security threats evolve over time, and Customer is responsible for maintaining the security (including securing its access credentials) in accordance with the then-current industry best practices. To qualify for the Guarantee, in addition to the measures set forth in Section 5, Customer must comply with the following minimum security requirements throughout the Guarantee Period ("**Requirements**"):

Data Security Best Practices. Customer must follow Druva's security best practices, which include the following:

Data Health

- Back-ups are successful and meet the Customer Policies
- Data lock is enabled for the Customer Data in the Customer Policies

User Access

- Multi-factor authentication is enabled for all user accounts
- SSH key-based with passphrase protected keys for CLI authentication
- User roles are assigned with least privilege access

Data Encryption

- Data-at-rest and in-transit are always encrypted
- Secure protocol for third-party systems

Application Access

- Create IP whitelisting that limits connections to Customer owned networks only
- SSL-certificate security for User Interface (UI) and APIs

API Security

- Secure service accounts
- Scoped API roles with least privilege

Customer Health Check. Customer must agree to the following Health Check, including granting Druva the necessary access and permissions to conduct such Health Check, and implementing Druva's resulting recommendations:

- At initial deployment the Customer must notify the Druva Global Customer Services ("GCS") before deploying the Eligible Druva Solution in production, and GCS will conduct the Health Check during the Health Check Period to confirm that the Eligible Druva Solution is configured properly and meets the applicable Requirements

- Upon a Ransomware Incident or Security Incident, Customer will allow Druva to audit and provide Druva documentation, permissions, and access to relevant systems and environments required to verify the required security measures under this Agreement have remained in place throughout the Guarantee Period

Additional Requirements. Customer shall:

- Implement updates and upgrades to the Eligible Druva Solution software as soon as reasonably practicable, consistent with industry best practices and in consultation with GCS;

- Protect the Customer Data under this Guarantee with the Customer Policies recommended by Druva;

- Include Customer Data under the defined snapshot retention period in the applicable Customer Policies;

- Implement security and data protection best practices consistent with Customer's security policies;

- Send product metrics to Druva and open recommended ports/services for data transmission;

· Implement change management best practices and inform GCS of any planned changes; and

· Implement such other security measures and best practices as may be required by Druva during the Guarantee Period.

7. NOTIFICATION OF RANSOMWARE INCIDENT OR SECURITY INCIDENT.

If Customer discovers a Ransomware Incident or Security Incident during the applicable Guarantee Period, Customer must notify Druva within twenty-four (24) hours of the Discovery Time of such Ransomware Incident or Security Incident by downloading and completing the incident report form located here: https://www.druva.com/resilience-guarantee/incident-report.docx.

8. REMEDIATION AND REIMBURSEMENT REQUEST PROCESS.

Remediation and Reimbursement Request. Subject to this Agreement, if all remedial measures recommended by Druva after a Ransomware Incident or Security Incident have been exhausted and Druva reasonably determines that a Recovery Incident or Security Incident occurred, Customer may submit a request for reimbursement of Recovery Incident Expenses or Security Incident Expenses ("**Reimbursement Request**"). Customer must submit such Reimbursement Request to Druva within two (2) months of Druva confirming a Recovery Incident or Security Incident and the Reimbursement Request shall include all information available to Customer regarding the Ransomware Incident, Recovery Incident or Security Incident. Druva shall review Customer's Reimbursement Request and Customer shall provide any additional information reasonably requested by Druva at any time.

Payments. Customer shall provide Druva with evidence of Recovery Incident Expenses or Security Incident Expenses in accordance with Druva's instructions. During the Guarantee Period, and for a period of three (3) years thereafter, Druva shall have the right, at its own expense, to inspect, and Customer shall maintain and provide, Customer's records related to such Recovery Incident Expenses or Security Incident Expenses upon reasonable written request during regular business hours. Except to the extent a Reimbursement Request arises out of an event that is later determined (1) not to be a Ransomware Incident or Security Incident, or (2) to relate to a Pre-Existing Incident, Druva hereby waives any and all rights it has or may have to reimbursement of Payments from Customer. Customer shall promptly (but in no event later than 30 days after written notice) reimburse Druva for all Payments related to a Reimbursement Request that arises out of an event that is later determined not to be a Ransomware Incident or Security Incident, or that relates to a Pre-Existing Incident. Druva shall have no obligation to make any Payments that are prohibited by law.

9. GENERAL.

Entire Agreement. This Agreement constitutes the entire agreement between Customer and Druva regarding the Guarantee and supersedes any and all prior agreements or communications between the

parties with regard to the subject matter hereof. For the avoidance of doubt, this Agreement is in addition to and separate from the Customer Agreement; nothing in this Agreement is intended to supersede, modify or amend the Customer Agreement, including any warranties therein. For the avoidance of doubt, the confidentiality terms in the Customer Agreement apply to this Agreement including without limitation any communications or information related to a Recovery Incident or Security Incident. In the event of any conflict or inconsistency between the terms of the Agreement and the Customer Agreement, the Agreement shall prevail. Druva may revise the terms and conditions of this Agreement or terminate the Guarantee program at any time without notice and without recourse to Customer; however, such modification or termination will not affect the latest version of the Agreement electronically accepted by Customer. In the event of a successful Recovery, Customer agrees to participate in a Druva marketing case study on such Recovery.

In addition to and without limiting Druva's rights set forth above in the immediately preceding paragraph, Druva reserves the right to modify or terminate this Agreement generally or in any jurisdiction, at any time, in its sole discretion, if: (i) the Guarantee is construed to be an offer to insure or constitute insurance or an insurance contract or insurance service agreement by any governmental or regulatory authority in any jurisdiction; or (ii) Druva determines or a court or arbitrator holds that the provisions of this Agreement violate applicable law. Druva may also terminate the Agreement upon sixty (60) days advance written notice in the event that it winds down the Guarantee program. If Druva modifies or terminates this Agreement in accordance with any of the foregoing, Druva will process all Reimbursement Requests that Customer submitted prior to or as of the effective date of such modification or termination unless such processing is prohibited by law, regulation, ordinance, order, or decree of any governmental or other authority.

Limitation of Liability. IN NO EVENT WILL DRUVA, ITS RESELLERS OR ITS SUPPLIERS BE LIABLE (UNDER ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STATUTE, TORT OR OTHERWISE) FOR ANY LOST PROFITS, LOST BUSINESS OPPORTUNITIES, BUSINESS INTERRUPTION, OR SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES, OR SUCH DAMAGES OR LOSSES WERE REASONABLY FORESEEABLE; AND IN NO EVENT SHALL DRUVA'S LIABILITY UNDER OR ARISING FROM THIS RESILIENCY GUARANTEE AGREEMENT EXCEED CUSTOMER'S CAP AS SET FORTH IN SECTION 4 ABOVE FOR THE GUARANTEE PERIOD. Multiple claims, Recovery Incidents or Security Incidents shall not expand the limitation specified in the foregoing sentence. Any Payments, damages or losses paid under this Agreement shall accrue towards any liability cap set forth in the Customer Agreement. If the limitation of liability in this Section 9 is determined to be invalid under applicable law, this Agreement shall be deemed null and void.

Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the State of California, U.S.A., without applying conflict of law rules. With respect to all disputes and actions arising from or related to this Agreement, the Parties irrevocably consent to exclusive

jurisdiction and venue in the state and federal courts located in Santa Clara County, California. The United Nations Convention of Contracts for the International Sale of Goods (1980) is hereby excluded in its entirety from application to this Agreement. Nothing in this Section (Governing Law) will limit or restrict either Party from seeking injunctive or other equitable relief from a court of competent jurisdiction.

Term and Termination. Termination of the Customer Agreement shall terminate this Agreement. Termination of this Agreement shall not terminate the Customer Agreement. The rights and remedies available to Customer pursuant to Sections 3 and 4 above shall not survive termination of this Agreement.

Assignment. Customer may not assign this Agreement without the prior written consent of Druva, except to an Affiliate in connection with a corporate reorganization or in connection with a merger, acquisition, or sale of all or substantially all of its business and/or assets provided Customer provides Druva with notice of any such assignment no later than thirty (30) days after such assignment or change in control event is public.

No Third Party Rights. This Agreement is not intended to and shall not be construed to give any third party any interest or rights (including, without limitation, any third party beneficiary rights) with respect to or in connection with any agreement or provision contained herein or contemplated hereby. For the avoidance of doubt, only the Customer has the right to enforce this Agreement or pursue claims relating to it against Druva.

Not Insurance. This Agreement is not intended to constitute an offer to insure, does not constitute insurance or an insurance contract, and does not take the place of insurance obtained or obtainable by the Customer. Any fees paid by Customer in connection with the Eligible Druva Solution are solely for the use of such Eligible Druva Solution and are not to be construed as an insurance premium.