RUBRIK ENTERPRISE EDITION RANSOMWARE RECOVERY WARRANTY AGREEMENT

This Rubrik Enterprise Edition Ransomware Recovery Warranty Agreement ("**Warranty Agreement**") describes the terms and conditions for the provision of a Ransomware Recovery Warranty ("**Warranty**") by Rubrik, Inc. ("**Rubrik**") to Customer for its purchase of an Eligible Solution (defined below). This Warranty Agreement governs the Warranty, which must be approved by Rubrik and stated in the quote for the Eligible Solution between the authorized Rubrik reseller and Customer. Unless expressly defined herein, capitalized terms shall have the meaning ascribed to them in the Customer Agreement.

1. DEFINITIONS.

1.1 **"Customer**" means the company purchasing an Eligible Solution from Rubrik through an authorized Rubrik reseller.

1.2 **"Customer Agreement"** means the agreement(s) between Rubrik and Customer governing Customer's use of the Eligible Solution.

1.3 **"Discovery Time"** means the exact time at which the Customer first discovers the Ransomware incident.

1.4 **"Eligible Solution"** means a subscription to Rubrik Enterprise Edition along with a concurrent subscription to a Customer Experience Manager ("CEM") service.

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

1.6 **"Health Check"** means a periodic audit performed by Rubrik personnel and the resulting recommendations for various Rubrik platform configurations and system statuses, including but not limited to security best practices, data backup and SLA Policies to ensure the Rubrik platform is optimized for data protection, recovery and restore operations.

1.7 **"Payment"** means reimbursement of Recovery Incident Expenses that directly result from a Recovery Incident.

1.8 **"Pre-existing Incident"** means the actual or reasonably suspected presence of Ransomware in the Customer environment prior to the Customer's applicable Warranty Period.

1.9 **"Ransomware Incident"** means a malware software program that infects Customer's systems from external sources (i.e. in the wild), which installs, persists, and encrypts a material portion of files ("**Ransomware**"), and continues to demand payment ("**Ransom**") in order to decrypt the encrypted files. For clarification, Ransomware does not include any malware introduced by the Customer or any third party to Customer's internal systems, whether intentionally (i.e. malware testing) or through a breach in the system's security.

1.10 "**Recovery Incident**" means an unsuccessful Recovery (defined in Section 2.1).

1.11 **"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 Warranty 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 Rubrik's prior written approval to procure such services or incur such expenditures; (2) paid to a third-party pre-approved in writing by Rubrik; (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 Rubrik in its sole discretion. The foregoing fees and expenses incurred by a Customer's Affiliate as a result of a Recovery Incident, and based on the use of an Eligible Solution by such Customer's Affiliate shall, for purposes of this definition only, be deemed expenses incurred by Customer so long as such Customer Affiliate also complies with terms set forth herein. Recovery Incident Expenses do not include any third-party restoration, recovery, or recreation attempts on a Rubrik platform or a Rubrik hosted cloud platform.

1.12 **"SLA Policy"** means a configurable set of policies that the Customer applies in the Eligible Solution to achieve specific data protection objectives which includes point-in-time snapshots or backups of data sources, how long to keep the data, and replication/archive requirements.

2. RANSOMWARE RECOVERY WARRANTY.

2.1 **The Warranty**. Rubrik warrants to Customer that in the event of a Ransomware Incident with an Event Date that occurs during the Warranty Period, the Eligible Solution will enable Customer to materially restore the Customer data that was successfully backed up using the Eligible Solution software onto Rubrik hardware, Rubrik-certified third party hardware, or a Rubrik hosted cloud platform, to the last good backup within the Customer's SLA Policy during the Warranty Period ("**Recovery**"). If Recovery of such Customer data is not successful due to a failure of the Eligible Solution software as determined by Rubrik, Customer's sole and exclusive remedy, and Rubrik's entire liability, subject

to the terms herein, will be to reimburse Customer for its Recovery Incident Expenses directly resulting from the Recovery Incident ("**Payment**"), up to a maximum amount not to exceed the applicable Cap set forth in the table below.

Amount of Customer Data Protected by the Eligible Solution	**Payment Cap (USD)("Cap")**
250 TB to < 500 TB	$250,000
500 TB to < 750 TB	$500,000
750 TB to < 5 PB	$1,000,000
5 PB and above	$5,000,000

The Customer data tiers above are calculated based on the amount of data Customer protects using the Eligible Solution software (i.e., data Customer backs up using products other than the Eligible Solution will not count toward those data tiers). Aggregate Payments for multiple Recovery Incidents with Event Dates in the Warranty Period shall not exceed the Cap. This Warranty extends only to Customer and its Recovery Incident Expenses 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.

2.2 **Pre-existing and Related Ransomware Incidents.** This Warranty does not extend to Pre-existing Incidents or Related Ransomware Incidents that include a Pre-existing Incident. Except as set forth in this Section 2.2, all Recovery Incident Expenses resulting from a Related Ransomware Incident shall be subject to the terms, conditions, exclusions and Cap in effect on the Event Date of the first discovered Ransomware Incident that forms part of the Related Ransomware Incident.

2.3 **Disclaimer.** EXCEPT FOR THE LIMITED WARRANTY PROVIDED IN SECTION 2.1 OF THIS WARRANTY AGREEMENT AND ANY WARRANTIES PROVIDED IN THE CUSTOMER AGREEMENT, THE ELIGIBLE SOLUTION IS PROVIDED AS IS.

3. CONDITIONS PRECEDENT TO WARRANTY PAYMENT. Rubrik shall only provide Payment to Customer if, at the time of the Ransomware Incident and throughout the Warranty Period:

1. Customer has maintained an active subscription for the Eligible Solution (both Rubrik Enterprise Edition and CEM);
2. Customer had deployed the most recent version of the Eligible Solution software as further described in Section 4.3 with the latest security patch available prior to the applicable Ransomware Incident;
3. Customer had completed all Health Checks and implemented all Health Check recommendations in a timely manner;
4. The Event Date and Discovery Time of the Ransomware Incident occurred, was discovered by Customer, and reported to Rubrik during the Warranty Period, and in accordance with Section 5;
5. Customer has remained in compliance with its Customer Agreement, including without limitation any payment obligations;
6. Customer has fully cooperated with Rubrik, including without limitation by (i) implementing all remedial and security measures recommended by Rubrik including the Requirements, (ii) providing all reasonably requested information, and (iii) complying with the Reimbursement Request process set forth in Section 6;
7. Any systems to which the Customer seeks to restore Customer data successfully backed up by Rubrik are free of any malware, bugs, back-doors or other malicious code, and are otherwise secured; and
8. This Warranty is not restricted or prohibited by applicable law.

4. 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 Warranty, in addition to the measures set forth in Section 3, Customer must comply with the following minimum security requirements throughout the Warranty Period ("**Requirements**"):

4.1 **Data Security Best Practices.** Customer must follow the Rubrik security best practices as defined in the latest version of the Security Hardening Best Practices Guide, which can be found on the Rubrik support portal or provided upon request and includes without limitation the following:

<u>Data Health</u>

- Back-ups are successful and meet the SLA Policies
- Retention lock is enabled in the SLA Policies

<u>User Access</u>

- Multi-factor authentication for all user accounts
- SSH key-based with passphrase protected keys for CLA authentication

- User roles are assigned with least privilege access

Data Encryption

- Data-at-rest and in-transit are always encrypted
- Secure protocols 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

4.2 **Customer Health Checks.** Customer must agree to the following Health Checks, including granting Rubrik the necessary access and permissions to conduct the Health Checks:

- At initial deployment – the Customer must notify the CEM before deploying the Eligible Solution software in production, and the CEM will conduct an initial deployment Health Check to confirm the Eligible Solution software is configured properly and meets the applicable Requirements at that time
- On a monthly basis
- Upon a Ransomware Incident – as part of this Health Check, Customer will allow Rubrik to audit and verify the required security measures under this Warranty Agreement have remained in place throughout the Warranty Period

4.3 **Additional Requirements.** Customer must:

- Implement updates and upgrades to the Eligible Solution software as soon as reasonably practicable, consistent with industry best practices and in consultation with the CEM; and in no event later than six (6) months after the date of the latest release;
- Protect the Customer data under this Warranty with the SLA Policies recommended by Rubrik;
- Include Customer data under this Warranty under the defined snapshot retention period in the applicable SLA Policy;
- Implement Radar and Sonar for ransomware detection and data classification;
- Send product metrics to Rubrik and open recommended ports/services for data transmission;
- Implement change management best practices and informs CEM of any planned changes; and
- Implement such other security measures and best practices as may be recommended by Rubrik from time to time over the course of the Warranty Period.

5. NOTIFICATION OF RANSOMWARE INCIDENT. If Customer discovers a Ransomware Incident during the applicable Warranty Period, Customer must notify Rubrik within twelve (12) hours of the Discovery Time of such Ransomware Incident by calling the Rubrik support team at the applicable hotline number found on www.rubrik.com/support/.

6. REMEDIATION AND REIMBURSEMENT REQUEST PROCESS.

6.1 **Remediation and Reimbursement Request.** Subject to this Warranty Agreement, if all remedial measures recommended by Rubrik after a Ransomware Incident have been exhausted and Rubrik determines a Recovery Incident occurred, Customer may submit a request for reimbursement of Recovery Incident Expenses ("**Reimbursement Request**"). Customer must submit such Reimbursement Request to Rubrik within one (1) year of Rubrik confirming a Recovery Incident and the Reimbursement Request shall include all information available to Customer regarding the Ransomware Incident and Recovery Incident. Rubrik shall review Customer's Reimbursement Request and Customer shall provide any additional information reasonably requested by Rubrik at any time.

6.2 **Payments.** Customer shall provide Rubrik with evidence of Recovery Incident Expenses in accordance with Rubrik's instructions. During the Warranty Period, and for a period of three (3) years thereafter, Rubrik 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 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 (2) to relate to a Pre-Existing Incident, Rubrik 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 Rubrik 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 that relates to a Pre-Existing Incident. Rubrik shall have no obligation to make any Payments that are prohibited by law. Customer must provide Rubrik such evidence and assurances that no Payment would be used by Customer to any person or entity subject to economic sanctions administered or enforced by the U.S. Treasury Department Office of Foreign Assets Control (OFAC), including any such person or entity listed on OFAC's Specially Designated Nationals and Blocked Persons (SDN) List or otherwise prohibited under relevant law.

7. GENERAL.

7.1 **Entire Agreement.** This Warranty Agreement constitutes the entire agreement between Customer and Rubrik regarding the Warranty 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 Warranty Agreement is in addition to the Customer Agreement; nothing in this Warranty Agreement is intended to supersede, modify or amend the Agreement, including any warranties therein. For the avoidance of doubt, the confidentiality terms in the Customer Agreement apply to this Warranty including without limitation any communications or information related to a Recovery Incident. In the event of any conflict or inconsistency between the terms of the Warranty Agreement and the Customer Agreement, the Warranty Agreement shall prevail. Rubrik may revise the terms and conditions of this Warranty Agreement or terminate the Ransomware Recovery Warranty program at any time without notice and without recourse to Customer; however, such modification or termination will not affect the Warranty Agreement in place at the time of a previous purchase of an Eligible Solution by the Customer. In the event of a successful Recovery, Customer agrees to participate in a Rubrik marketing case study on such Recovery.

In addition to and without limiting Rubrik's rights set forth above in the immediately preceding paragraph, Rubrik reserves the right to modify or terminate this Warranty Agreement generally or in any jurisdiction, at any time, in its sole discretion, if: (i) the Warranty 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; (ii) Rubrik is required to obtain a license or permit of any kind to continue to provide this Warranty in any jurisdiction; or (iii) Rubrik determines or a court or arbitrator holds that the provisions of the Warranty or this Warranty Agreement violate applicable law. If Rubrik modifies or terminates this Warranty Agreement in accordance with the foregoing, Rubrik will process all Reimbursement Requests that the 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.

7.2 **Limitation of Liability.** IN NO EVENT WILL RUBRIK 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 RUBRIK'S LIABILITY UNDER OR ARISING FROM THIS WARRANTY AGREEMENT EXCEED CUSTOMER'S CAP AS SET FORTH IN SECTION 2.1 ABOVE FOR THE WARRANTY PERIOD. Multiple claims or Recovery Incidents shall not expand the limitation specified in the foregoing sentence. Any Payments, damages or losses paid under this Warranty Agreement shall accrue towards any liability cap set forth in the Customer Agreement. If the limitation of liability in this Section 7.2 is determined to be invalid under applicable law, this Warranty Agreement shall be deemed null and void.

7.3 **Governing Law.** This Warranty 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 Warranty Agreement, the Parties irrevocably consent to exclusive jurisdiction and venue in the state and federal courts located in Santa Clara County. The United Nations Convention of Contracts for the International Sale of Goods (1980) is hereby excluded in its entirety from application to this Warranty Agreement. Nothing in this Section 16.15 (Governing Law) will limit or restrict either Party from seeking injunctive or other equitable relief from a court of competent jurisdiction.

7.4 **Term and Termination**. The Warranty Period commences on the date the Customer's CEM performs the initial Health Check and confirms the Eligible Solution is configured to meet the Requirements and shall continue for the term of the Eligible Solution's initial subscription term, unless terminated earlier in accordance with this Section 7.4 or the Customer Agreement ("**Warranty Period**"). Termination of the Customer Agreement shall terminate this Warranty Agreement. Termination of this Warranty Agreement shall not terminate the Customer Agreement. Customer may not assign this Warranty Agreement without the prior written consent of Rubrik, 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 Rubrik with notice of any such assignment no later than thirty (30) days after such assignment or change in control event is public. Any assignment in violation of this section shall be void and shall void this Warranty. Subject to the foregoing, all rights and obligations of the parties under this Warranty Agreement shall be binding upon and inure to the benefit of and be enforceable by and against the successors and permitted assigns.

7.5 This Warranty 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 Warranty Agreement or pursue claims relating to it against Rubrik.

7.6 This Warranty 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.