



NetApp Ransomware Recovery Guarantee Terms and Conditions

This NetApp Ransomware Recovery Guarantee is governed by the terms and conditions set forth below, including Rider A which applies to Keystone Storage as a Service only (“**Terms and Conditions**”).

DEFINITIONS.

“**Customer**” means a NetApp Customer purchasing, for their own use, an Eligible Array from NetApp or a NetApp authorized reseller.

“**Documentation**” means NetApp-supplied technical documentation describing the features, functions and operation of the associated products.

“**Eligible Array**” means a single HA Pair running on new FAS, AFF A- Series, AFF C-Series, ASA A-Series or ASA C-Series running ONTAP based storage array system, with ONTAP One, identified in the related Order Documentation and is configured with validated SnapLock Compliance Volumes for storing Qualifying Workloads. Eligible Arrays do not include Customer’s existing systems or arrays.

“**Guarantee Program**” means the NetApp Ransomware Recovery Guarantee described in these Terms and Conditions.

“**HA Pair**” means two identical storage controllers that are configured to serve data independently during normal operation, and in the event of an individual controller failure provide high availability by transferring data processes from the failed storage controller to the surviving controller.

“**NetApp Professional Services**” means NetApp’s consulting, installation, managed services, implementation and other services that are not Support Services, to be provided by or on behalf of NetApp and governed by NetApp Professional Services Terms and as further described in the relevant engagement document.

“**Order Documentation**” means the applicable NetApp price quotation (and the engagement document, if required for the purchase of NetApp Professional Services), corresponding Purchase Order and the associated Documentation for the products or Services purchased or licensed under these Terms and Conditions.

“**Purchase Order**” means an electronic order provided to NetApp consistent with these Terms and the corresponding price quotation for the purchase of Eligible Array and Services.

“**Ransomware**” means software designed to, without authorization, prevent or disable access to data.

“**Ransomware Incident**” means any incident involving Ransomware and where a monetary or equivalent fee is required to be paid or other action is required to be taken by Customer in order to access data on an Eligible Array.

“**Qualifying Workloads**” means Network Attached Storage (NAS) Snapshots stored in NetApp Professional Services validated SnapLock Compliance Volumes or Snapshots which contain logical unit numbers (LUNs) stored in NetApp Professional Services validated SnapLock Compliance Volumes replicated via SnapMirror Vault. For avoidance of doubt, Qualifying Workloads do not include active data stored in NAS workloads, S3, and any Storage Area Network (SAN) protocol such as Internet Small Computer Systems Interface (iSCSI) or Fibre Channel (FC) or direct LUN support.

“**Recover**” or “**Recovery**” refers to the recovery of qualified Snapshots from SnapLock Compliance Volumes on an Eligible Array starting from the most recent SnapLock Compliance Volume replicated immediately preceding the time of Ransomware Incident. Recovery does not guarantee that data within the Snapshot may not be corrupted or encrypted prior to being vaulted to a SnapLock Compliance Volume.

“**Services**” means NetApp’s Support Services and/or NetApp Professional Services.

“**Snapshot**” means a point-in-time copy of a defined collection of data. For the purposes of this Guarantee, Snapshots stored in SnapLock Compliance Volumes must only contain Qualifying Workloads.

“**SnapLock Compliance Volume(s)**” means a Snapshot copy that has been locked to provide protection from Ransomware Incidents using the SnapLock Compliance clock feature. When a Snapshot is locked, the volume

expiry time is set to the expiry time of the Snapshot copy. If more than one Snapshot copy is locked, the volume expiry time reflects the longest expiry time among all Snapshot copies.

“**Support Services**” means NetApp’s generally available technical support and maintenance services for the products that are subject to this Guarantee to be provided by or on behalf of NetApp.

THE GUARANTEE.

In the event of a Ransomware Incident, NetApp guarantees during the Guarantee Term that Customer and/or NetApp will be able to Recover Snapshots stored in a SnapLock Compliance Volume on the Eligible Array(s) (the “**Guarantee**”). The requirements below must be met during the Guarantee Term and are subject to these Terms and Conditions set forth herein. The Guarantee process will be initiated by Customer’s notification to NetApp of a Ransomware Incident which will trigger the activities for Recovery listed in the engagement document, which may require signature. The Guarantee is not a commitment by NetApp that Customer will experience zero data loss. The Recovery completion time depends on the complexity of the request.

GUARANTEE TERM.

The guarantee term (“**Guarantee Term**”) begins on the date NetApp Professional Services notifies Customer that successful validation of a SnapLock Compliance Volume on the Eligible Array has been completed (“**Validation Notification Date**”). The Guarantee Term will end twelve (12) months from the Validation Notification Date. Prior to the commencement of the NetApp Professional Services the Customer may request for the Guarantee to match the support term of the Customer’s NetApp Support Services Agreement of the Eligible Array (“**Matching Support Term**”). However, during the Matching Support Term each coverage year will require a NetApp Professional Services engagement to confirm a new validation of the Eligible Array (“**New Guarantee Term**”). The New Guarantee Term will begin from the new Validation Notification Date. The Customer may choose to renew either on a single Guarantee Term or additional Matching Support Term subject to validation process above.

REQUIREMENTS.

To be eligible for the Guarantee, each of the following requirements (“**Requirements**”) must be met during the entire duration of the Guarantee Term:

- Customer must purchase the following, listed on the same Purchase Order, and maintain throughout the Guarantee Term:
 - An Eligible Array consisting of NetApp FAS with ONTAP One, or
 - AFF A-Series or C-Series with ONTAP One, or
 - ASA A-Series or C-Series with ONTAP One, and
 - The NetApp Ransomware Recovery Assurance Service which is provided by NetApp Professional Services
- Eligible Arrays must be running one of the following protection technologies:
 - Snapshot copies protected by SnapLock Compliance volumes
 - SnapLock for SnapMirror vault
- Customer must have current active NetApp Support Services Agreement.
- NetApp Professional Services will validate the SnapLock Compliance volumes on the Eligible Array.
- Customer will ensure all best practices, recommendations, and configuration are met as specified by NetApp Professional Services.
- The minimum ONTAP version that an Eligible Array must run under this Guarantee Program is:
 - For FAS, AFF A-Series and C-Series: ONTAP version 9.12.1 P1 or later
 - For ASA A-Series: ONTAP version 9.13.1 P2 or later
 - For ASA C-Series: ONTAP version 9.13.1 P2 or later
- If an ONTAP patch is released, the applicable nodes of each Eligible Array must have the latest patch applied to the arrays within 60 days of availability.
- Customer must be in compliance with all applicable NetApp licenses.
- The Eligible Array must be operated in accordance with the applicable system Documentation.
- NetApp Professional Services will provide written details of Eligible Arrays and SnapLock Compliance volumes protected under the Guarantee, along with the start date of the Guarantee Term to Customer.

- Any SnapLock Compliance volumes that are added to the Eligible Array after the start date of the Guarantee Term must be validated by NetApp Professional Services in order to fall under the Guarantee. The addition of SnapLock Compliance volumes does not extend the Guarantee Term.
- AutoSupport (ASUP) must be enabled on the Eligible Arrays at all times for the duration of the Guarantee Term.

EXCEPTIONS TO GUARANTEE.

The following are exceptions and situations not covered by the Guarantee:

- Insider threats and incidents caused by Customer's negligence.
- Ransomware Incidents occurring prior to the start of the Guarantee Term or Ransomware Incidents related to such prior events.
- Payments or actions required to be made to a third party in response to a Ransomware Incident.
- Payments based on the actual or perceived value of the data.

VOIDANCE OF GUARANTEE.

Any of the following causes the Guarantee to be void:

- Customer moves SnapLock Compliance Volumes away from the Eligible Array specified in the NetApp Professional Services configuration report.
- Customer fails to meet all Requirements throughout the Guarantee Term or has tampered with or provided incomplete audit logs from the Eligible Array.
- Any non-compliance with an applicable NetApp license.
- Customer does not operate the Eligible Array in accordance with the NetApp Documentation for the Eligible Array.
- The Eligible Array is physically missing, damaged or tampered with, has been disassembled, or is not functioning properly in any way.
- NetApp, for any reason, is unable to gain access to the Eligible Array to assist with the Recovery process.

REMEDIES.

Subject to these Terms and Conditions, and as a prerequisite to making a claim under this Guarantee the following steps must have taken place prior to raising a claim under the Guarantee Program:

- a) Customer must create a ticket with NetApp Professional Services informing of a Ransomware Incident,
- b) Customer must work with NetApp Professional Services to Recover qualified Snapshots from the SnapLock Compliance Volumes on an Eligible Array, and
- c) Ticket must have been, at NetApp's discretion, closed by both NetApp Support Services and Professional Services and marked as failed (an "Unsuccessful Close").

Upon completion of the steps above Customer must submit a claim in writing to NetApp within seven (7) days from Unsuccessful Close of the Ransomware Incident at ng-RRG-Claim@netapp.com. Any claim submitted after the Guarantee Term is expired or terminated is not covered by the Guarantee, unless Customer has already created a ticket in accordance with section a) above with NetApp Professional Services, informing NetApp of Ransomware Incident prior to the end of the Guarantee Term. If a Ransomware Incident continues to cause issues with prevention or disabling of access to data, all such recurring issues are deemed to have the same event time as the first occurrence of such Ransomware Incident.

Customer must make the Eligible Array available for audit by NetApp at the time of the claim. Determination of whether the Eligible Array fulfils the Requirements of the Guarantee will be made solely in accordance with an assessment performed by NetApp. If no claim is submitted during the Guarantee Term, then the Guarantee is deemed to have been met.

If NetApp determines that a SnapLock Compliance Volume on an Eligible Array has failed to meet the Guarantee, then NetApp will, in its sole discretion, provide payment to Customer based on the type and capacity of the affected Eligible Array. The failure of NetApp and Customer to successfully Recover from the SnapLock Compliance Volume will have no bearing on the successful completion of the Ransomware engagement and will not result in additional remedies.

The payment amounts for a claim will be presented to Customer upon commencement of the Guarantee Program from the NetApp representative. Such payment is Customer's sole and exclusive remedy for a failure

of Guarantee under these Terms and Conditions. Customer is limited to one claim request per Eligible Array during the Guarantee Term.

LIMITATION OF LIABILITY.

EXCEPT AS EXPRESSLY SET FORTH IN THE REMEDIES SECTION OF THESE TERMS AND CONDITIONS OF THIS GUARANTEE, IN NO EVENT WILL NETAPP 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 INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, OR EXEMPLARY DAMAGES ARISING OUT OF OR RELATED TO THIS GUARANTEE, 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 NETAPP HAVE LIABILITY FOR MORE THAN ONE RANSOMWARE INCIDENT PER ELIGIBLE ARRAY PER CUSTOMER AND NETAPP'S TOTAL LIABILITY UNDER THE GUARANTEE FOR SUCH RANSOMWARE INCIDENT WILL NOT UNDER ANY CIRCUMSTANCES EXCEED FIVE MILLION DOLLARS (\$ 5,000,000). Multiple claims or Ransomware Incidents shall not expand the limitation specified in the foregoing sentence. If the limitation of liability in this Section is determined to be invalid under applicable law, this Guarantee shall be deemed null and void.

MISCELLANEOUS.

General. This Guarantee is exclusively governed by these Terms and Conditions and is void where prohibited or restricted by law. Unless otherwise restricted by law, these Terms and Conditions will be construed pursuant to the governing law as set forth in (a) Customer's separate written agreement with NetApp that governs Customer's purchase of the Eligible Array and Services, or (b) in the absence of such agreement, or if the Customer is purchasing the Eligible Array from a NetApp reseller, the applicable terms of sale on NetApp's How to Buy site at <https://www.netapp.com/how-to-buy/sales-terms-and-conditions/> that apply to Customer's purchase of the Eligible Array. In the event of any conflict between these Terms and Conditions and the terms referenced in (a) or (b) above, as applicable, these Terms and Conditions will prevail with respect to this Guarantee Program. All other terms and conditions in the terms referenced in (a) or (b) above that are not expressly modified by this Guarantee Program remain in full force and effect. NetApp reserves the right to change the terms and conditions of this Guarantee and the Guarantee Program, or modify or terminate the Guarantee and the Guarantee Program, at any time without notice and without recourse to the Customer.

Third Party Beneficiaries. These Terms and Conditions are 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 these Terms and Conditions or pursue claims relating to it against NetApp.

No Insurance. This Guarantee 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 Array are solely for the use of such Eligible Array and are not to be construed as an insurance premium.

RIDER A

ADDITIONAL TERMS AND CONDITIONS APPLICABLE TO KEYSTONE STaaS ORDERS

This Rider A provides additional terms and conditions in order to expand the application of the NetApp Ransomware Guarantee to certain qualified Keystone STaaS customers and Keystone STaaS orders. In the event of a conflict between this Rider A and any of the terms and conditions set forth above, this Rider A shall prevail,

DEFINITIONS.

“**Customer**” as defined above means a NetApp Customer purchasing Keystone STaaS from NetApp or a NetApp authorized reseller.

“Order Documentation” and Purchase Order” as defined above refer to the applicable Keystone STaaS order

“NetApp’s Support Services” as described above refer to the services described in the applicable Keystone STaaS Service Description.

GUARANTEE TERM.

“Matching Support Term” as defined above means the applicable Keystone STaaS Subscription Term.

REQUIREMENTS.

- Customer must apply to NetApp for inclusion into the Guarantee program, and NetApp will accept or reject Customer’s application prior to the acceptance of a Keystone STaaS order.
- Customer must purchase the required NetApp Ransomware Recovery Assurance Service separately from the associated Keystone STaaS order.

REMEDIES.

- Customer’s sole remedy for a NetApp failure to meet the Guarantee is a Keystone STaaS credit against future invoices. References to “payment amounts” in the Remedies section above refer to Keystone STaaS credit amounts. Credit amounts are paid out on a per-subscription basis and subject to a cap of 10% of Customer Committed Value (“CCV”). Credits shall be paid during the current subscription term of the applicable Keystone STaaS order. Any unused credits at the end of a subscription term shall be carried over in the event such subscription is renewed. Customer may adjust 1/12 of the total eligible credit in any particular month, provided that Customer’s billing period is monthly
- By way of example for a monthly subscription, the total credit would be spread over the next 12 months and can be spread over the next 12 months and can be adjusted against any future Keystone invoices for the remainder of the term of the subscription. In the event the remaining term is less than 12 months, Customer may renew the subscription and continue to adjust the remaining credit, or adjust the credit against any other NetApp invoice.
- By way of example for an annual subscription, the credit would be adjusted towards the next Keystone invoices, if available. If Customer has no future Keystone invoices, the credit may be adjusted against any other NetApp invoice.

MISCELLANEOUS.

In sub-sections (a) and (b) of the General section set forth above, references to Customer purchases of Eligible Arrays shall refer to Customer purchase of Keystone STaaS.