NetApp

This document contains:

GENERAL TERMS

THESE GENERAL TERMS (INCLUDING ANY APPLICABLE PRODUCT, SERVICES AND COUNTRY TERMS) (COLLECTIVELY, "TERMS") SET FORTH THE DIRECT TERMS BETWEEN NETAPP, INC., NETAPP IRELAND, LTD. AND/OR A NETAPP AFFILIATE (COLLECTIVELY "NETAPP") AND CUSTOMER IN CONNECTION WITH CUSTOMER'S PURCHASE OR LICENSE (AS APPLICABLE) OF PRODUCTS AND SERVICES DIRECTLY FROM NETAPP OR INDIRECTLY FROM A NETAPP PARTNER OR, WHERE APPLICABLE, A NETAPP CLOUD PROVIDER. THE TERMS APPLY UNLESS CUSTOMER HAS ENTERED INTO A SEPARATE WRITTEN AGREEMENT WITH NETAPP GOVERNING SUCH PURCHASE OR LICENSE. BY PURCHASING OR LICENSING SUCH PRODUCTS OR SERVICES EITHER (1) VIA AN ORDER DIRECTLY WITH NETAPP OR INDIRECTLY WITH A NETAPP PARTNER OR CLOUD PROVIDER, (2) CLICKING A BOX INDICATING ACCEPTANCE, OR (3) ACCEPTING DELIVERY AND USING PRODUCTS OR SERVICES, CUSTOMER AGREES TO BE BOUND BY THESE TERMS.

IF CUSTOMER REGISTERS FOR A FREE TRIAL OR EVALUATION OF PRODUCTS OR SERVICES, THE APPLICABLE PROVISIONS OF THESE TERMS WILL ALSO GOVERN THAT FREE TRIAL OR EVALUATION, UNLESS CUSTOMER HAS A SEPARATE WRITTEN TRIAL OR EVALUATION AGREEMENT WITH NETAPP.

IF THE INDIVIDUAL ACCEPTING THESE TERMS IS ACCEPTING ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, SUCH INDIVIDUAL REPRESENTS THAT THEY HAVE THE AUTHORITY TO BIND SUCH ENTITY AND/OR ITS AFFILIATES TO THESE TERMS, IN WHICH CASE THE TERM "CUSTOMER" REFERS TO SUCH ENTITY AND ITS AFFILIATES.

1. DEFINITIONS

Capitalized terms have the definitions set forth below or as otherwise set forth in these Terms.

1.1 **Active IQ.** The portal and mobile application that displays remote diagnostics, including AutoSupport Data about Customer's Products, and provides Customer with remote support tools.

1.2 **Affiliate.** Any entity, directly or indirectly through one or more intermediaries, that is controlled by, or is under common control with, a party hereunder, but only for so long as such relationship exists. For purposes of this definition, "control" means the ability to direct its affairs and/or to control the composition of its board of directors or ownership of more than 50% (or such lesser percent as may be the maximum that may be owned by foreign interests pursuant to the applicable laws of the country of incorporation) of (a) the shares of stock entitled to vote for directors in the case of a corporation; or (b) the equity or interests in profits in the case of a business entity other than a corporation.

1.3 **AutoSupport™.** A telemetry mechanism that proactively monitors the health of Customer's Products and automatically provides configuration, status, performance and system events data ("AutoSupport Data") for diagnosis and response purposes.

1.4 **Cloud Provider.** A third party authorized by NetApp to offer or enable the use of Products or Services as part of such provider's cloud-based service.

1.5 **Cloud Service.** A NetApp cloud-based service (which may be infrastructure, platform or software) made available to Customer.

1.6 **Cloud Service Enabling Software.** NetApp Software that is solely necessary to facilitate Customer's use of a Cloud Service.

1.7 **Confidential Information.** All information, whether written, oral or in any other medium disclosed by or on behalf of the Disclosing Party to the Receiving Party for purposes arising out of or in connection with these Terms, that (a) in the case of information in tangible form, is marked "confidential" or "proprietary" or with words of similar import at the time of disclosure; (b) in the case of any information disclosed orally, visually or in any other intangible form, is designated "confidential" or "proprietary" at the time of disclosure, and if disclosed orally, is summarized in reasonable detail in a writing delivered to the Receiving Party within 30 days of disclosure; or (c) by its nature or the circumstances surrounding disclosure should reasonably be considered confidential or proprietary, including any reproduction of such information. Confidential Information of Customer includes Personal Information provided to NetApp; Confidential Information of

NetApp includes all Orders (including pricing). Confidential Information of each party includes business and marketing plans, technology and technical information, product plans and designs, and business processes disclosed by the Disclosing Party.

1.8 **Country Terms.** Additional terms that apply to Orders placed with NetApp Affiliates in certain countries outside the U.S. as set forth on the How to Buy Site.

1.9 **Customer.** The end user customer purchasing NetApp Products and Services for its own use.

1.10 **Customer Content.** Any data, content, or information in any form, format or media submitted by Customer that NetApp may operate on, where such operation is on the Customer's behalf as part of providing Products and Services.

1.11 **Disclosing Party.** The party disclosing Confidential Information.

1.12 **Documentation.** The then-current documentation published by NetApp on NetApp.com relating to the description, operation and use of NetApp Products and Services. Documentation includes technical program and interface documentation, user manuals, operating instructions and release notes.

1.13 **Engagement Document.** A NetApp-approved document that describes the Professional Services NetApp will provide to Customer, including but not limited to a statement of work, service brief or service description.

1.14 **Hardware.** NetApp-branded hardware, including its components and spare parts, and excluding any firmware and Third-Party Branded Products.

1.15 **Order.** A NetApp-approved ordering document with Customer or Partner (as applicable), Purchase Order, Engagement Document or online order describing the Products or Services that the Customer is purchasing.

1.16 **Partner.** A third party authorized by NetApp to resell Products and Services to Customer.

1.17 **Personal Information.** Any information relating to, directly or indirectly, an identified or identifiable natural person or household, or is defined as "personal data" or "personal information" by applicable laws or regulations, as further described in the NetApp Privacy Policy, which can be accessed at NetApp Privacy Policy.

1.18 **Price List.** NetApp's then-current list of Products and Services, and their associated prices for the country of destination.

1.19 **Product Terms.** Additional terms that apply to specific Products, as set forth on the How to Buy Site.

1.20 **Products.** Collectively, Hardware, Software, and Third-Party Branded Products.

1.21 **Professional Services.** Consulting, installation, implementation and other services that are not Support Services to be provided to Customer by or on behalf of NetApp.

1.22 **Purchase Order.** An electronic order that Customer provides to NetApp for direct purchases of Products and Services from NetApp.

1.23 **Receiving Party.** The party receiving Confidential Information.

1.24 **Services.** Collectively, NetApp's Cloud Services, Support Services and/or Professional Services.

1.25 **Services Terms.** Additional terms that apply to specific Services, as set forth on the How to Buy Site.

1.26 **Software.** NetApp-branded software in object code format, including (as applicable) operating system software, protocols, firmware, backup and recovery, disaster recovery, storage efficiency, and management software.

1.27 **Support Services.** NetApp's generally available technical support and maintenance services for Products to be provided by or on behalf of NetApp.

1.28 **Terms.** These Terms and any Product Terms, Services Terms, and/or Country Terms, as applicable, which are hereby incorporated by reference.

1.29 **Third-Party Branded Products or Third-Party Branded Services.** Any hardware ("Third-Party Branded Hardware") or software ("Third-Party Branded Software") or services ("Third-Party Branded Services") manufactured, developed licensed or otherwise provided by a third party and resold by NetApp under the third party's brand name for use in conjunction with Hardware and Software.

1.30 **Usage Data (**also referred to as "**Functional Data**"). Data generated or derived from the usage, configuration, deployment, access, performance and operation of Products and Services. Usage Data includes, by example and not limitation, technical information about Customer's operating environment, configuration data, and system architecture, AutoSupport Data, aggregated quantitative information about number of users, capacity usage, account information, used bandwidth, storage

space, Product versions and other quantitative data derived from Customer's use of Products and Services and Service performance-related data.

2. COVERAGE AND SCOPE

2.1 Services Terms and Product Terms. Customer's acquisition of Products and/or Services is subject to additional terms as set forth in the Services Terms and Product Terms, respectively, described below. Applicable warranties for Products and Services, respectively, are set forth in the Product Terms and Services Terms.

1. **Cloud Services Terms -** Purchases of Cloud Services (a list of which is set forth at the How to Buy Site) are governed by the Cloud Services Terms.
2. **Hardware Terms** - Purchases of Hardware and Third-Party Hardware are governed by the terms within Hardware Terms.
3. **Software Terms** - Purchases of Software licenses (including Software and Third-Party Branded Software embedded within Hardware or standalone Software/Third-Party Branded Software) are governed by the Software Terms.
4. **Support Services Terms** - Purchases of Support Services are governed by the Support Services Terms.
5. **Professional Services Terms** - Purchases of Professional Services are governed by the Professional Services Terms.

2.2 Not for Resale. These Terms govern Customer's acquisition of Products and Services for Customer's internal use, and not for resale or distribution.

3. DIRECT PURCHASE TERMS

This Section applies only to a Customer that places an Order directly with NetApp (not through a Partner).

3.1 Orders. Customer will submit all Orders to NetApp electronically. Each Order will be based on, and refer to, a valid and current price quotation (where applicable) and will include relevant Product and/or Services information, appropriate legal entities, "ship to" and "bill to" locations (where applicable) and requested delivery date (where applicable). All Orders are subject to acceptance by NetApp.

3.2 Changes, Cancellation, and Rescheduling. Customer may modify or cancel Orders for Products or related Support Services up to 10 days prior to any scheduled shipment date, and Customer may reschedule a requested delivery date for Products and related Support Services one time per Order without additional charge. Product returns are subject to NetApp approval and applicable charges. Changes, cancellation, and rescheduling for Professional Services and Cloud Services is set forth in the applicable Services Terms.

3.3 Pricing. NetApp may, in its sole discretion, change the prices set forth on its Price List and may add or remove Products and Services from its Price List at any time. An Order received after the effective date of a price change, but pursuant to a valid and current NetApp quotation, will be invoiced at the price stated on the NetApp quotation.

3.4 Invoicing. NetApp may invoice shipments, including partial shipments, on delivery in accordance with the applicable trade term specified in the quotation or mutually executed Order.

3.5 Payment Terms. Customer will make full payment in the currency specified in the invoice, without set-off and in immediately available funds, no later than 30 days from the date of invoice (unless otherwise agreed in a mutually executed Order). Fees are non-refundable and payment obligations are non-cancelable, except as provided in these Terms, or where prohibited by law.

3.6 Remedies for Non-payment. Customer's payment of an amount less than the invoice amount will not be deemed as acceptance of payment in full, nor will any endorsement or statement on any check or letter accompanying any payment or check be deemed an accord and satisfaction. NetApp may accept such payment without prejudice to NetApp's right to recover the balance of any amount due or pursue any other remedy provided for in these Terms, or by law or in equity. NetApp has the right to apply any payment received from Customer to any account of Customer which is due and/or delinquent. If Customer fails to make timely payment, in addition to all other available remedies, NetApp will have the right to decline to make further deliveries of Products or provide further Services to Customer.

3.7 Taxes and Duties. Customer is solely responsible for the payment of taxes (except taxes based on NetApp's net income), fees, duties and charges, and all related penalties and interest, that arise from its utilization or NetApp's provision of Products and/or Services. If such taxes are incurred, including any withholding taxes, the sum payable by Customer (in

respect of which such deduction or withholding is required to be made) will be increased to the extent necessary to ensure that NetApp receives payment in full of an amount equal to the invoiced amount. If Customer is tax-exempt, then Customer will provide NetApp with tax exemption certificates or other documentation acceptable to the taxing authorities not later than 30 days from the date Customer places an Order with NetApp. If Customer does not provide such documentation to NetApp, NetApp reserves the right to include such taxes in the invoice. In addition to the stated prices, Customer is responsible for all applicable duties, license fees and taxes for Products shipped across international borders in accordance with the applicable trade term specified or as otherwise may apply.

4. CONFIDENTIALITY

4.1 **General.** Confidential Information disclosed to the Receiving Party will remain the exclusive property of the Disclosing Party. The Receiving Party may use the Disclosing Party's Confidential Information solely for the purpose of fulfilling its obligations under these Terms. The Receiving Party agrees to disclose the Disclosing Party's Confidential Information only to those employees or agents who have a need to know in furtherance of these Terms and who are required to protect such Confidential Information against unauthorized disclosure under terms no less restrictive than those set forth herein. The Receiving Party will protect the Confidential Information from unauthorized use, access, or disclosure in the same manner as it protects its own proprietary information of a similar nature, and in any event with at least a reasonable degree of care.

4.2 **Exclusions.** Confidential Information does not include any information that: (a) is already known to the Receiving Party without restrictions at the time of disclosure; (b) is or becomes known to the general public through no act or omission of the Receiving Party in breach of these Terms; (c) is disclosed to the Receiving Party by a third party who is not, to the knowledge of the Receiving Party, in breach of an obligation of confidentiality; or (d) is independently developed by employees and/or contractors of the Receiving Party who did not have access to, and without use of, the Disclosing Party's Confidential Information.

4.3 **Period of Disclosure.** The Receiving Party's obligations regarding the Disclosing Party's Confidential Information will expire three years from the date of disclosure, provided, however, that any Confidential Information that constitutes a trade secret will remain subject to the obligations of this Section until such information no longer qualifies as a trade secret under applicable law.

4.4 **Legally Compelled Disclosure.** The Receiving Party may disclose the Disclosing Party's Confidential Information to the extent such disclosure is required pursuant to a judicial or administrative proceeding, provided that, unless prohibited by applicable law, the Receiving Party gives the Disclosing Party prompt written notice thereof and the opportunity to seek a protective order or other legal remedies.

4.5 **Return/Destruction.** Upon the Disclosing Party's written request, all Confidential Information (including all copies thereof) of the Disclosing Party will be returned or destroyed, unless the Receiving Party is required by law to retain such information, and the Receiving Party will provide written certification of compliance with this Section.

5. INTELLECTUAL PROPERTY RIGHTS AND PROTECTION

5.1 **General.** Software, Cloud Service Enabling Software and related Documentation are licensed, not sold, to Customer. Software, Cloud Service Enabling Software, Cloud Services and related Documentation are protected by intellectual property laws and treaties worldwide, and contains trade secrets, in which NetApp and its licensors reserve and retain all rights not expressly granted to Customer. No right, title or interest to any trademark, service mark, logo, or trade name of NetApp or its licensors is granted to Customer.

5.2 **IP Claims**. Subject to the terms and conditions of this Section, NetApp will defend or settle any claim brought by a third party against Customer that Hardware, Software, Documentation, Cloud Service Enabling Software and/or the Cloud Services sold and delivered by or for NetApp to Customer under these Terms (individually or collectively, "Covered Products") infringe any patent, trademark, or copyright ("IP Claim"). NetApp will pay settlement amounts or, if applicable, damages and costs finally awarded by a court of competent jurisdiction (collectively, "Damages") against Customer to the extent such Damages are specifically attributable to the IP Claim, provided that Customer: (a) promptly notifies NetApp in writing of the IP Claim; (b) provides information and assistance to NetApp to defend such IP Claim; and (c) provides NetApp with sole control of the defense or settlement negotiations.

5.3 **Remedies.** NetApp may, at its option, substitute or modify the applicable Covered Products, or the relevant portion thereof, so that it becomes non-infringing; procure any necessary license; or replace the applicable Covered Products. If NetApp determines that none of these alternatives is reasonably available, then Customer may cease using and, if applicable, return Covered Products or terminate its subscription to the Cloud Service, and Customer will be entitled to a pro rata refund of pre-paid fees received by NetApp for such Covered Products, as applicable.

5.4 **Exclusions.** Notwithstanding anything to the contrary in these Terms, NetApp has no obligation or liability for any IP Claim related to the Covered Products that arises from or relates to: (a) NetApp's compliance with, or use of, designs, specifications, inventions, instructions, or technical information furnished by or on behalf of Customer; (b) modifications to the Covered Products made by or on behalf of Customer without NetApp's prior written authorization; (c) Customer's failure to upgrade or use a new version of the Covered Products, to make a change or modification requested by NetApp, to implement or configure the Covered Product in a manner set forth by NetApp, or to cease using the Covered Products if requested by NetApp; (d) the Covered Products, or any portion thereof, in combination with any other product or service (including a Cloud Provider's services); (e) Third-Party Branded Products or Third-Party Branded Services; (f) any content or information stored on or used by Customer or a third party in connection with a Covered Product; or (g) Customer's breach of the use limitations prescribed by NetApp.

5.5 **Entire Liability.** Notwithstanding anything to the contrary in these Terms, this Section states NetApp's entire liability and Customer's sole and exclusive remedies for IP Claims.

6. LIMITATION OF LIABILITY

6.1 **Liability Exclusions.** To the extent permitted by applicable law, regardless of the basis of the claims (e.g., whether in contract, tort (including negligence), statute, products or strict liability, or any other form of action), in no event will NetApp or its suppliers or subcontractors be liable to Customer for special, incidental, exemplary, indirect or consequential damages; downtime costs; loss or corruption of data; loss of revenues, profits, goodwill, or anticipated savings; procurement of substitute goods and/or services; and/or interruption of business. This exclusion is independent of any remedy set forth in these Terms.

6.2 **Cumulative Liability.** To the extent permitted by applicable law, NetApp's liability to Customer is limited to direct damages in an amount not to exceed US$1,000,000. This limitation is cumulative and not per incident.

6.3 **Exceptions.** The limitations set forth in Sections 6.1 (Liability Exclusions) and 6.2 (Cumulative Liability) will not apply to liability for: (a) claims arising from death or bodily injury caused by a Party's negligence or gross negligence; (b) claims arising from a Party's willful misconduct or fraud; or (c) IP Claims under Section 5.2 (IP Claims). These limitations will also not apply to any other liabilities which cannot be excluded under applicable law.

6.4 **Disclaimer of Liability for Trial/Pre-Release Products and Services**. To the extent permitted by law, NetApp disclaims all liability arising out of Customer's use of any Trial, No-Charge or Pre-Release Products or Services (defined below).

7. WARRANTY DISCLAIMER

TO THE EXTENT PERMITTED BY APPLICABLE LAWS, THE WARRANTIES SET FORTH IN THE PRODUCT TERMS, SERVICES TERMS AND COUNTRY TERMS ARE CUSTOMER'S SOLE AND EXCLUSIVE WARRANTIES AND REMEDIES.

8. COMPLIANCE WITH LAWS

8.1 **Compliance with Anti-Bribery and Other Laws.** Each party will comply with all applicable laws and regulations, including but not limited to applicable country laws relating to anti-corruption or anti-bribery, the requirements of the U.S. Foreign Corrupt Practices Act, as amended, the U.K. Bribery Act, and legislation implementing the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions.

8.2 **Export.** Customer acknowledges that Products, Services and access to technology and intellectual property (collectively, "Materials") are subject to export controls under the laws and regulations of the United States, the European Union, and other countries (as applicable), and that Products and Services may include technology controlled under export and import regulations, including encryption technology. Customer agrees to comply with all such laws and regulations, and to provide NetApp destination end use and end user information. Materials are intended for Customer's own use. Customer will not resell, export, re-export, divert or transfer Materials to Prohibited Persons or into Restricted Countries. "Prohibited Persons" means sanctioned individuals and entities, including without limitation persons on the U.S. Denied Persons, Entity and Specially Designated Nationals Lists. "Restricted Countries" means countries and regions subject to embargoes or trade sanctions programs, including without limitation Cuba, Iran, North Korea, Syria, Russia, Belarus, The Crimean, Luhansk and Donetsk regions of Ukraine, and the Kherson and Zaporizhzhia oblasts of Ukraine. Customer will not use Materials for any purposes prohibited by United States or other applicable laws, including but without limitation, the development, design, manufacture or production of nuclear, missile, chemical, biological weaponry or other weapons of mass destruction. Customer is responsible for obtaining all required authorizations, permits, and licenses to import, export, re-export or

transfer Materials. Customer agrees to obligate, by contract or other similar assurances, the parties to whom Customer re-exports or otherwise transfers Materials to comply with all obligations set forth in this Section.

8.3 **Privacy/Data Processing Addendum.** In the event Customer provides NetApp with access to Personal Information in order for NetApp to provide Products or Services hereunder, the Parties will ensure that such Personal Information is disclosed and handled in accordance with all applicable data protection laws and the confidentiality provisions set forth in these Terms. To the extent that NetApp receives Personal Information from Customer, the NetApp Privacy Policy (found at NetApp Privacy Policy) will apply to NetApp's management and usage of such Personal Information and is hereby incorporated by reference. Article 28 (1) of the European Union General Data Protection Regulation ("GDPR") requires an agreement between a controller and processor, and between a processor and sub processor, that processing of Personal Information be conducted in accordance with technical and organizational measures that meet the requirements of the GDPR and ensure the protection of the rights of data subjects. To the extent NetApp acts as a data processor of Personal Information on behalf of Customer: (a) NetApp will comply with the additional terms and conditions applicable to NetApp in the NetApp Data Processing Addendum; and (b) NetApp will not retain, use, or disclose such Personal Information for any purpose other than providing or improving Products or Services in accordance with these Terms. NetApp certifies that it understands the foregoing restrictions and will comply with them.

9. TERM AND TERMINATION

9.1 **Term**. These Terms are effective as of the date Customer first agrees to these Terms and will continue until the applicable Order subject to these Terms has expired or has been terminated. The term of an Order is as specified in the particular Order.

9.2 **Termination**. A party may terminate these Terms and any applicable Order for cause: (a) upon 30 days written notice to the other party of a material breach (including for Customer's failure to remit payments when due) if such breach remains uncured at the expiration of such period; or (b) if the other party becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors. Termination will not (a) relieve Customer from its payment obligations with respect to any sums accrued prior to termination, which will become immediately due and payable; or (b) entitle Customer to any refund unless otherwise set forth in these Terms. Upon termination of these Terms, all rights to use any Software and related Documentation licensed under the Software Terms cease and Customer will, at NetApp's request, promptly return or destroy all copies of such Software and Documentation, including any license enablement keys, in Customer's possession or under Customer's control, unless the license granted to Customer under the Software Terms is a perpetual license, Customer remains in full compliance with these Terms and NetApp has not terminated these Terms for cause.

9.3 **Surviving Provisions**. The following Sections will survive termination of these Terms in accordance with the terms set forth herein: Section 4 (Confidentiality), Section 5 (Intellectual Property Rights and Protection), Section 6 (Limitation of Liability), Section 7 (Warranty Disclaimer), Section 8 (Compliance with Laws), Section 9 (Term and Termination) and Section 10 (General Provisions). In addition, any sections of the Terms which, upon a plain reading, are intended to survive termination or expiration of the Terms, will survive such termination or expiration.

10. GENERAL PROVISIONS

10.1 **Updates**. NetApp reserves the right to update these Terms without prior notice to Customer. The version of these Terms that are in effect at the time NetApp accepts an Order will govern the applicable transaction.

10.2 **Order of Precedence**. In the event of a conflict between the terms set forth in the General Terms, Services or Product Terms, Country Terms or an Order, the following order of precedence will apply:

1. Country Terms
2. Product Terms or Services Terms (as applicable to the Order)
3. General Terms
4. Order (excluding any pre-printed terms on a Customer Purchase Order)

10.3 **Third-Party Licenses.** Customer represents and warrants that it has obtained, and/or will obtain, all applicable third-party licenses necessary to operate any third-party software required in connection with the use of the Products and for NetApp to freely and without interruption perform Services. NetApp is not liable or responsible for Customer's failure to obtain any such licenses.

10.4 Evaluation/Trial/Beta/No-Charge Products and Services. Unless there is a separate written agreement between the parties related to Products or Services provided on an evaluation, trial, alpha, beta, pre-release, preview or no-charge basis, the following provisions will apply.

10.4.1 Cloud Services. NetApp may offer:

1. a no-cost, no-obligation trial to a Cloud Service ("Trial Cloud Service") to Customer which will commence on the initial date Customer accesses the Trial Cloud Service and will conclude at the end of the trial period delineated by NetApp, or sooner if: (a) Customer purchases a pre-paid subscription to the Cloud Service; (b) Customer uses the Cloud Service on a pay as you go basis; or (c) NetApp terminates Customer's use of the Trial Cloud Service;
2. a Cloud Service or feature of a Cloud Service available to Customer that NetApp has identified as alpha, beta, pre-release, demonstration, or preview (each a "Beta Cloud Service"); unless otherwise agreed in writing by NetApp, a Beta Cloud Service may only be used in non-production environments and not for commercial purposes; or
3. a Cloud Service at no cost to Customer, up to certain limits prescribed by NetApp ("No Charge Cloud Service").

10.4.2 Products. NetApp may offer Products for evaluation, demonstration or trial ("Trial Products") or alpha, beta, pre-release, or preview Products ("Pre-Release Products"). Such Trial or Pre-Release Products will be provided or licensed, as applicable, by NetApp at no cost for a 90-day period from initial delivery to Customer, or such other period as agreed by NetApp in writing ("Evaluation Period"). These Products are provided to Customer for evaluation, demonstration, and internal, non-commercial use only and Customer will not use the Trial or Pre-Release Products for production use or in a production environment. Customer is responsible for the Trial Products from the date of delivery until the Trial Product is returned to, and received by, NetApp, a NetApp-authorized carrier, or NetApp's agent, as evidenced by a bill of lading or document of title ("Possession Period") where applicable. Customer will reimburse NetApp for any loss or damage to the Trial Products sustained during the Possession Period, except for reasonable wear and tear. Customer must keep the Trial Products free and clear of all liens and encumbrances, and will defend, at its own expense, the rights, title and interest of NetApp in and to the Trial Products. The Trial Products will remain NetApp's property, even if it becomes attached or affixed to real property, and NetApp will exclusively maintain title and ownership to all Trial Products. In no event will title to the Trial Products that consist of Hardware transfer to Customer unless purchased by Customer. Trial and Pre-Release Products that are Software may only be used up to the maximum amounts of storage capacity, number of hosts or other measure of usage as prescribed by NetApp. Customer agrees to deinstall (or delete, as applicable) the Trial Product at the expiration of the Evaluation Period and make it available for pickup by NetApp (or return or destroy the applicable license keys as requested by NetApp). If Customer does not return (or destroy as applicable) the Trial Product within 30 days of the end of the Evaluation Period, Customer will pay the then-current list price for the Trial Product. Unless otherwise agreed in writing by the parties, such purchase will be governed by the Terms then in effect. Customer is solely responsible for erasing all Customer Content from the Trial Product before being returned to NetApp and acknowledges that any Customer Content remaining on any Trial Product that is returned to NetApp may be disposed of or destroyed by NetApp without any liability of NetApp.

10.4.3 NOTWITHSTANDING ANY WARRANTIES SET FORTH IN THESE TERMS TO THE CONTRARY, ANY TRIAL, PRE-RELEASE OR NO CHARGE PRODUCT OR SERVICE THAT NETAPP PROVIDES TO CUSTOMER IS PROVIDED "AS IS." ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE ARE EXCLUDED TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAWS, INCLUDING WARRANTIES OF PERFORMANCE AND THE IMPLIED WARRANTY OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

10.5 Force Majeure. Neither party will be liable to the other for any alleged loss or damages resulting from acts of God, acts of civil or military authority, governmental priorities, fire, floods, earthquakes, epidemics or pandemics, quarantine, energy crises, strikes, labor trouble, terrorism, war, riots, accidents, shortages, delays in transportation, or any other causes beyond the reasonable control of a party (a "Force Majeure Event"). A Force Majeure Event will not relieve Customer's obligation to make payments due hereunder for Products or Services actually delivered. If the Force Majeure Event continues for more than 30 days, the parties will negotiate in good faith the termination of the affected Order.

10.6 Data Security and Recovery. Except as set forth in these Terms, Customer is solely responsible for its use of Products and Services, including Personal Information managed or stored using Products and Services. Customer is solely responsible for (a) management of its data back-up, data recovery, and disaster recovery measures; and (b) undertaking the

supervision, control and management of Products, including following industry-standard processes, procedures and requirements for (i) the security of data, accuracy of input and output, and back-up plans, including restart and recovery in the event of a Force Majeure Event or a Product error or malfunction; and (ii) reconstruction of lost or altered files, data, and programs. NetApp will have no responsibility or liability with respect to Customer's internal processes and procedures related to the protection, loss, confidentiality, or security of Customer's data or Customer Content in connection with Customer's use of the Products and Services.

10.7 Usage Data. From time to time, NetApp may collect Usage Data generated in the course of Customer's use of NetApp Products and Services. NetApp collects Usage Data for various reasons, including for NetApp, its agents, service providers and subcontractors to provide technical support, identify, diagnose and address performance issues, improve Products and Services, and for other business purposes in support of the development, deployment, operation, support, provision, and enhancement of Products and Services. NetApp retains all right, title and interest in Usage Data excluding any Customer Personal Information contained therein. Details about NetApp's Usage Data collection processes are set forth in NetApp's Privacy Policy at NetApp Privacy Policy.

10.8 Audit. Customer grants NetApp and its independent accountants the right to audit Customer or Customer's subcontractors once annually during regular business hours upon reasonable notice to verify compliance with these Terms. If an audit discloses any over-usage or material non-compliance, Customer will promptly pay to NetApp any additional fees upon notice to Customer, including reasonable costs of conducting the audit.

10.9 Modification/Substitution/Discontinuation of Products. NetApp has the sole discretion, at any time, to change, substitute, or discontinue Products and Services set forth on the Price List. NetApp will use commercially reasonable efforts to provide 60 calendar days prior notice when any Product or Service is no longer going to be available for purchase.

10.10 Hazardous Environments. Products and Services are not designed or intended for use in or in the design, construction, operation, or maintenance of a nuclear facility or similar hazardous environment. NetApp will not be liable for any damages resulting from such use.

10.11 Severability; Waiver. In the event any provision of these Terms is held by a court of competent jurisdiction to be unenforceable for any reason, such provision will be changed and interpreted to accomplish the objectives of such provision to the greatest extent possible under applicable law and the remaining provisions will be unaffected and remain in full force and effect. Any waiver or failure to enforce any provision of these Terms on any occasion will not be deemed a waiver of any other provision or of such provision on any other occasion. Either party's exercise of any right or remedy provided in these Terms will be without prejudice to its right to exercise any other right or remedy.

10.12 Assignment. Customer may not assign any rights or delegate any obligations under these Terms without the prior written consent of NetApp. Any purported assignment by Customer without NetApp's prior written consent will be null and void.

10.13 Subcontractors. NetApp may use subcontractors to fulfill its obligations under these Terms. NetApp will be responsible for its subcontractors' obligations hereunder.

10.14 Independent Contractors. The relationship of the parties under these Terms is that of independent contractors. Nothing set forth in these Terms will be construed to create the relationship of principal and agent, franchisor/franchisee, joint venture, or employer and employee between the parties. Neither party will act or represent itself, directly or by implication, as an agent of the other.

10.15 Publicity. No advertising, publicity releases, or similar public communications concerning these Terms, Products, or Services will be published or caused to be published by either party without the prior written consent of the other party. Notwithstanding the foregoing, Customer agrees to be mentioned in the list of buyers of NetApp Products and/or Services and that its logo and trademark may be used for this purpose only.

10.16 U.S. Government Customers. This Section applies only to U.S. Government customers. The Products and related Documentation and the Cloud Services are "commercially available off the shelf" items and the Professional Services and Support Services (including but not limited to deliverables or documents provided thereunder) are "commercial services" as defined in FAR 2.101, and their use is subject to the policies, as applicable, set forth in FAR part 12, specifically but not limited to FAR subpart 12.211 and 12.212, as well as DFARS subpart 212.2, specifically but not limited to 212.211 and 212.212. U.S. Government customers will not be subject to applicable audit costs specified in these Terms. Disputes will be subject to resolution pursuant to the Contract Disputes Act of 1978. Nothing contained in this Section is meant to derogate the rights of the U.S. Department of Justice as identified in 28 U.S.C. § 516. All other terms remain in effect as written.

10.17 Contracting Entity, Notices, Governing Law, and Venue. These Terms, the interpretation hereof, and any dispute arising hereunder will be governed by the laws of the state and/or country where the NetApp entity that entered into the

applicable Terms (and, where applicable, the Order) is incorporated, excluding any relevant conflict of law provisions. The United Nations Convention on Contracts for the International Sale of Goods will not apply to these Terms or any Order.

10.18 Country Terms. For any Customer domiciled outside of the United States, additional terms applicable to transactions in such country are set forth in the applicable Country Terms set forth on the How to Buy Site, which will replace or supplement the equivalent provisions set forth in these Terms.

10.19 Feedback from Evaluation Products and Services. To the extent Customer uses Pre-Release, Evaluation or Trial Products or Services, NetApp can use without restriction, any Customer feedback or suggested improvements concerning the functionality and performance of the Pre-Release Products or Services ("Feedback"). Feedback is proprietary and considered NetApp Confidential Information.

10.20 Product and Services Restrictions. Except to the extent required under applicable law, Customer will not directly or indirectly: (i) use Products and Services for any benchmarking or competitive purposes or activities, including but not limited to, developing similar or competing products or services or publishing or providing any benchmark or comparison test results; or (ii) reverse-engineer or disassemble the Products and Services.

10.21 Notices. Except as specifically stated, all notices or other communications required or permitted under these Terms must be in writing and must be delivered by personal delivery, certified overnight delivery, or registered mail (return receipt requested), and will be deemed given upon personal delivery or upon confirmation of receipt. In addition, the parties consent to notice by email or electronic transmission sent to the email address provided by Customer and for NetApp to the following email address: General.Counsel@netapp.com.

10.22 Entire Agreement/Amendments. These Terms may not be changed except by an amendment signed by an authorized representative of each party. In the event of a dispute between the English and non-English version of these Terms (where translated for local requirements), the English version of these Terms will govern, to the extent permitted by applicable laws. These Terms, including any supplemental terms referenced herein, (a) represent the entire agreement and understanding between the parties with respect to the Products and Services acquired hereunder; (b) supersede any previous communications, representations or agreements between the parties; and (c) prevail over any conflicting or additional terms in any Order, acknowledgement, or similar communications. Orders issued to NetApp are deemed to incorporate and be subject to these Terms, except where the parties expressly agree in writing to variations thereto. The pre-printed terms or general terms and conditions on any Customer-provided or Partner-provided Order, or other similar non-NetApp document will have no effect.

10.23 Interpretation. Headings are inserted only for convenience and ease of reference and are not to be considered in the construction or interpretation of any provision of these Terms. Any use of the word "including" in these Terms will not be deemed to limit the meaning of the preceding word or phrase. Each party has been given the opportunity to independently review these Terms with legal counsel and each party has the requisite experience and sophistication to understand, interpret, and agree to the particular language of the provisions. Therefore, in the event of any ambiguity in or dispute regarding the interpretation of these Terms, the drafting of the language will not be attributed to either party.

[REMAINDER OF PAGE LEFT INTENTIONALLY BLANK]

NetApp

CLOUD SERVICES TERMS

1. CLOUD SERVICES

1.1. Scope. A list of NetApp Cloud Services subject to these Cloud Services Terms is available at the How to Buy Site (each, a "Cloud Service").

1.2. Access Rights. Subject to these Cloud Services Terms and during the specified period of continuous time for which Customer is authorized ("Subscription Term"), Customer may access and use the Cloud Service for Customer's own internal use, including in support of service offerings Customer may provide to its end customers (but, for clarity, not as a standalone product or service). This includes the right, as part of Customer's authorized use of the Cloud Service, to download and use any Cloud Service Enabling Software, and related Documentation describing the features and functions of the Cloud Service. The rights granted in this Section are non-exclusive, non-transferable, non-sublicensable, and revocable.

1.3. Use Limitations. Customer will not, nor will Customer allow any third party, to: (a) modify, adopt or create a derivative work of, the Cloud Service, Cloud Service Enabling Software or Documentation; (b) publish or provide any benchmark or comparison test results that pertain to the Cloud Service; (c) reverse engineer, decompile or disassemble the Cloud Service or any applicable Cloud Service Enabling Software, or otherwise reduce either to human-readable form except to the extent required for interoperability purposes under applicable laws or as expressly permitted in open-source licenses; (d) use the Cloud Service or any Cloud Service Enabling Software in excess of any limitations (e.g., user limits, time limits, capacity limits, free trials) prescribed by NetApp; (e) remove, conceal, or modify any identification, proprietary, intellectual property, or other notices in the Cloud Service, Cloud Service Enabling Software or Documentation; (f) access or use the Cloud Service in violation of laws or regulations; (g) use the Cloud Service to violate the rights of others; (h) use the Cloud Service to try to gain unauthorized access to or interrupt any service, device, data, account, or network; or (i) use the Cloud Service in high-risk, hazardous environments requiring fail-safe performance, including without limitation in the operation of nuclear facilities, aircraft navigation or control systems, air traffic control, or weapons systems in which the failure of the Cloud Service could lead to severe physical or environmental damages.

1.4. Unauthorized Use. Use of the Cloud Service, Cloud Service Enabling Software or Documentation outside of the scope of these Cloud Services Terms constitutes a material breach, and Customer agrees to promptly pay, upon notice, any additional Cloud Service fees calculated in accordance with the Price List.

1.5. Third-Party and Open Source Software. Notwithstanding other statements in this Section, third-party software components, including free, copyleft and open source software components, if any, embedded in the Cloud Service or Cloud Service Enabling Software ("Third-Party Embedded Software") are distributed in compliance with the licensing terms and conditions attributable to such Third-Party Embedded Software. Copyright notices and licensing terms and conditions applicable to Third-Party Embedded Software may be provided with the Cloud Enabling Software or available for review with the Documentation at https://mysupport.netapp.com/, within a "NOTICE" file (e.g., NOTICE.PDF or NOTICE.TXT) or included within the downloaded files, and/or reproduced within the materials or Documentation accompanying the Cloud Service or Cloud Service Enabling Software. Third-Party Embedded Software that is delivered as part of the Cloud Service or Cloud Service Enabling Software is included in the applicable warranty, support and indemnification provisions provided it is not removed or used separately from the Cloud Service or Cloud Service Enabling Software.

1.6. Third Party Beneficiaries. If required by NetApp's agreement with a Third-Party Embedded Software licensor, such licensor will be a direct and intended beneficiary of these Cloud Services Terms and may enforce them directly against Customer.

2. DIRECT PURCHASE TERMS

This Section applies only to Orders for Cloud Services that Customer places directly with NetApp.

2.1. Order Acknowledgement. NetApp may limit, refuse, or cancel any Cloud Service Order at its sole discretion. NetApp may also require additional information before accepting or processing any Order. NetApp will provide Customer with an email confirmation (where applicable) upon receipt of Customer's Cloud Service Order. Such order confirmation represents NetApp's confirmation of receipt and does not signify NetApp's acceptance of Customer's Order, nor does it constitute confirmation of NetApp's offer to sell. NetApp reserves the right at any time after receiving Customer's Order to accept or decline the Order for any reason. However, if NetApp cancels an Order after Customer has submitted payment, NetApp will refund the amount received by NetApp without interest.

2.2. Delivery. Delivery of a Cloud Service occurs when NetApp makes the enabling key or access credentials available electronically to Customer or, if an enabling key is not required, when NetApp makes such Cloud Service available for Customer's use.

2.3. Monthly Billing Date. Customer's monthly billing date is the earlier of (a) the date of the month that Customer originally started Customer's subscription on or (b) the last day of the month. For example, if Customer signed up for its subscription on

January 31st, Customer's monthly billing date would be the 31st of any month with 31 days, or the day the relevant month ends, which may be the 28th, 29th or 30th (depending on the month).

2.4. Pay Per Use, Monthly, Annual, and Multi-Year Service Subscriptions. Cloud Services may be ordered on a pay per use, monthly subscription, annual subscription, or multi-year subscription basis.

2.5. Changes, Cancellation, and Renewals.

2.5.1. Monthly Service Subscriptions. Unless otherwise agreed to in writing, Customer's monthly Cloud Service subscription will automatically renew for additional one-month terms unless cancelled in accordance with these Cloud Services Terms. Customer must cancel Customer's monthly subscription in writing no later than 14 days before Customer's monthly billing date. In the event Customer cancels its monthly subscription, Customer will not receive a refund, but Customer will receive the Cloud Service for the remainder of the billing month Customer cancels in, and no further charges will be incurred. NetApp reserves the right to cancel Customer's monthly subscription upon 30 days prior written notice. If NetApp exercises this right Customer will not receive a refund, but Customer will receive the Cloud Service for the remainder of the billing month in which the cancellation is effective, and no further charges will be incurred. NetApp may modify its prices and fees and apply new fees upon 30 days prior written notice.

2.5.2. Annual and Multiyear Subscriptions. Annual and multi-year subscriptions are non-cancellable. If Customer has agreed that its annual or multi-year subscription will automatically renew at the end of a Subscription Term, then the subscription will automatically renew for additional periods equal to the expiring Subscription Term or one year (whichever is shorter), unless either party gives the other written notice of non-renewal no later than 90 days before the end of the then current Subscription Term.

2.6. Invoicing. NetApp is entitled to invoice Customer for a Cloud Service on a periodic basis, as determined by NetApp, upon the start of a Subscription Term. If Customer is using a Cloud Service on a pay per use basis, NetApp calculates and bills fees and charges monthly, based on Customer's actual usage of the Cloud Service, and NetApp will be entitled to invoice Customer for the Cloud Service on a periodic basis, as determined by NetApp, in arrears.

3. CUSTOMER CONTENT AND SECURITY

3.1. Ownership. Customer retains all right, title, and interest in Customer Content. NetApp acquires no rights in Customer Content, other than the rights Customer grants to NetApp to provide the Cloud Service.

3.2. Use. NetApp will use Customer Content solely to provide and improve the Cloud Service and, if applicable, provide related technical support.

3.3. Disclosure. NetApp will not disclose Customer Content outside of NetApp or its Affiliates except to the extent required to make the Cloud Service available for Customer's use or to the extent such disclosure is required by applicable law. NetApp will give Customer reasonable notice of a request of a governmental or regulatory body for Customer Content to allow Customer to seek a protective order or other legal remedies (except to the extent NetApp's compliance with this Section would cause it to violate a court order or other legal requirement).

3.4. Security. NetApp will implement reasonable technical and organizational safeguards designed to protect Customer Content against unauthorized loss, destruction, alteration, access, or disclosure. NetApp may modify such safeguards from time to time, provided that such modifications will not materially reduce the overall level of protection for Customer Content. NetApp also maintains a compliance program that includes independent third-party audits and certifications.

3.5. Security Incident. If NetApp discovers that a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Content in the possession or control of NetApp (a "Security Incident") has occurred, NetApp will notify Customer promptly and without undue delay, unless otherwise prohibited by law or otherwise instructed by a law enforcement or supervisory authority. In addition to providing such notification, NetApp will promptly take reasonable steps to mitigate the effects of the Security Incident and to minimize any damage resulting from the Security Incident. Customer must notify NetApp promptly about any possible misuse of its accounts or authentication credentials of which it becomes aware related to the Cloud Service.

4. PERFORMANCE AND OPERATIONS

4.1. Service Specific Terms. Certain Cloud Services may be subject to additional terms specific to that Cloud Service (e.g., NetApp's commitment to specific service level agreements); these are set forth at NetApp's How to Buy Site**.**

4.2. **Support.** During the Subscription Term, NetApp will provide Customer with support for the Cloud Service in accordance with the applicable Documentation.

5. WARRANTY

5.1. **Warranty and Remedy.** NetApp warrants that during the Subscription Term (a) the Cloud Service will perform substantially in accordance with the applicable service level agreement; (b) these Cloud Service Terms and the Documentation accurately describe the applicable administrative, technical and physical safeguards for the protection and security of Customer Content; (c) NetApp will not materially decrease the security of the Cloud Services; and (d) NetApp will not materially decrease the functionality of the Cloud Service. If NetApp does not meet the warranty set forth in (a), then Customer's sole and exclusive remedy is as set forth in the applicable Service Level Agreement. For breach of any of the other warranties in this Section that continue for 30 days after Customer provides written notice of such breach, as Customer's sole and exclusive remedy and NetApp's sole liability, Customer may terminate the affected Cloud Service, and NetApp will refund any prepaid subscription fees received by NetApp covering that part of the Subscription Term for the affected Cloud Service after the effective date of termination. Notwithstanding the foregoing, this warranty will not apply to any breach due to a modification of or defect in the Cloud Service made or caused by any party other than NetApp or a person acting at NetApp's direction.

5.2. **Disclaimer**. TO THE EXTENT PERMITTED BY APPLICABLE LAWS, THE FOREGOING ARE CUSTOMER'S SOLE AND EXCLUSIVE WARRANTIES AND REMEDIES. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN THESE CLOUD SERVICES TERMS, NETAPP MAKES NO OTHER WARRANTIES AND SPECIFICALLY DISCLAIMS AND EXCLUDES ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, AND ANY WARRANTIES ARISING FROM COURSE OF DEALING, COURSE OF PERFORMANCE, OR USAGE OF TRADE RELATED TO THE CLOUD SERVICE, DOCUMENTATON AND CLOUD SERVICE ENABLING SOFTWARE. NETAPP AND ITS SUPPLIERS DO NOT WARRANT THAT CLOUD SERVICES WILL BE UNINTERRUPTED OR FREE FROM DEFECTS OR ERRORS, OR THAT CLOUD SERVICES WILL MEET OR ARE DESIGNED TO MEET CUSTOMER'S BUSINESS REQUIREMENTS.

6. SUSPENSION, EXPIRATION OR TERMINATION OF CLOUD SERVICES

6.1. **Suspension/Termination.** NetApp may suspend or terminate Customer's access to, and use of, any Cloud Service if Customer (a) fails to remit payments when due; (b) otherwise breaches these Cloud Services Terms or the General Terms, as applicable; or (c) uses the Cloud Services in a manner that violates the law. NetApp will provide reasonable notice before suspending Customer's access to a Cloud Service unless NetApp, in its sole discretion, believes an immediate suspension or termination is required.

6.2. **Refund or Payment upon Termination.** If an Order subject to these Cloud Services Terms is terminated by Customer due to NetApp's breach in accordance with the Term and Termination Section set forth in the General Terms, NetApp will refund any prepaid fees received by NetApp covering the remainder of the term of such Order after the effective date of termination. If these Cloud Services Terms are terminated by NetApp due to Customer's breach in accordance with the Term and Termination Section set forth in the General Terms, Customer will pay any unpaid fees covering the remainder of the term of all Orders to the extent permitted by applicable law. In no event will any termination relieve Customer of its obligation to pay any fees payable to NetApp for the period prior to the effective date of termination.

6.3. **Effect of Cloud Service Expiration or Termination.** In the event of expiration or termination of the Cloud Service, NetApp will use commercially reasonable efforts to notify Customer that its access to the Cloud Service will be discontinued and that all Customer Content will be deleted, at a time to be determined by NetApp, without the option of recovery. NetApp expressly disclaims all liability if Customer does not receive or act in accordance with this notice, or if any Customer Content is deleted.

[REMAINDER OF PAGE LEFT INTENTIONALLY BLANK]

NetApp

NetApp® Instaclustr Services Specific Terms
January 2025

These Service Specific Terms ("Service Specific Terms") for **NetApp® Instaclustr** Support Service ("Instaclustr Support Service") and Platform Service ("Instaclustr Platform Service") are part of the NetApp Cloud Services-Terms of Service ("Terms"). Capitalized terms used, but not defined in these Service Specific Terms, will have the meaning assigned to them in the Terms.

1. **Service Level Agreement (Instaclustr Support Services)**

If the Service does not achieve the service levels described in this Service Level Agreement (SLA), then you may be eligible for a service credit.

We reserve the right to change the terms of this SLA or discontinue the SLA at our discretion. We will honor the SLA in effect at the outset of your subscription for the duration of your initial Subscription Term. However, if you renew your subscription, the version of this SLA that is in effect the time of renewal will apply throughout your renewal term.

Availability Service Level

NetApp will use commercially reasonable efforts to make support available 24 hours a day, seven days a week, during any monthly billing cycle.

Response Time Service Level

NetApp will use commercially reasonable efforts to respond to support requests no later than 20 minutes from which the support request is received from an authorized customer support contact by NetApp via one of the support channels until acknowledgement by a NetApp Technical Operations Engineer to the Customer and incident resolution commenced according to the defined incident severities.

Service Credits

For each breach of the response time SLA beyond the second in any month, 10% of the monthly contract support subscription fees as a service credit to a maximum of 50% of the monthly contracted support subscription. The service credit will apply to future use of the Instaclustr Support Services and will be deducted from your next billing cycle/invoice.

2. Service Level Agreement (Instaclustr Platform Services)

If the Service does not achieve the service levels described in this Service Level Agreement (SLA), then you may be eligible for a service credit.

We reserve the right to change the terms of this SLA or discontinue the SLA at our discretion. We will honor the SLA in effect at the outset of your subscription for the duration of your initial Subscription Term. However, if you renew your subscription, the version of this SLA that is in effect the time of renewal will apply throughout your renewal term.

The SLA is tiered based on the technology, size, number and/or class of the cluster that the Customer is running. The tiers recognize that larger clusters can support more consistent levels of performance and availability and is as follows:

Instaclustr Platform Services supporting Apache Cassandra®

Tier[1]	Service Standards[2]	Customer Requirements
Starter (Developer nodes)	○ No guaranteed availability[4] (99.9% target) ○ No latency[3] SLAs	○ Minimum replication of 2 on all topics ○ Add capacity or adjust retention settings when requested by the NetApp Instaclustr product team to maintain disk usage in normal operations as less than 80% ○ Comply with reasonable requests from NetApp to modify application for best practice Cassandra usage
Small (5 or less production nodes)	○ 99.95% availability for LOCAL_QUORUM ○ No latency SLAs ○ 20% monthly fees at risk in total; 10% credit for each breach	○ Minimum replication factor of 3 on all keyspaces (please ensure that cluster is initially configured with target RF of 3) ○ Add capacity or remove data when requested by NetApp to maintain disk usage in normal operations at less than 70% ○ Comply with reasonable requests to modify the application for best practice Cassandra usage

Enterprise (6+ production nodes)	○ 99.99% availability for LOCAL_QUORUM consistency operations ○ 99% of read/write transactions to NetApp-maintained table in the cluster within specified latency threshold[3] ○ 30% of monthly fees at risk in total; 15% credit for each incident causing breach of availability SLA and 10% credit for each incident causing breach of latency SLA	○ Minimum replication factor of 3 on all keyspaces (please ensure that cluster is initially configured with target RF of 3) ○ Add capacity or remove data when requested by NetApp to maintain disk usage in normal operations at less than 70% ○ Comply with reasonable requests to modify the application for best practice Cassandra usage
Critical (12+ production nodes)	○ 100% availability for LOCAL_QUORUM consistency operations ○ Custom latency SLA negotiable (or use medium SLA)[3] ○ 100% of monthly fees at risk in total; 30% credit for each incident causing breach of availability SLA and 10% credit for each incident causing breach of latency SLA	○ Minimum replication factor of 5 on all keyspaces (please ensure that cluster is initially configured with target RF of 5) ○ Separate testing and production clusters ○ Customer notifies that they wish to receive this SLA, commissions NetApp to review their application for best practice alignment and actions finding from that review. ○ NetApp review prior to deploying changes that may impact latency SLA ○ Add capacity or remove data when requested by the NetApp Instaclustr product team to maintain disk usage in normal operations at less than 70% ○ Comply with reasonable requests to modify the application for best practice Cassandra usage

**For Enterprise and Critical level Cassandra clusters, we also provide Recovery Point Objective SLA: The native replication of data in Cassandra means restoration of data from backups is rarely required. However, we will maintain backups to allow restoration of data with less than 24 hours data loss for standard backups and less than 5 minutes data loss for our Continuous Back-ups option. Should we fail to meet this recovery point objective, you will be eligible for SLA credits at 100% of monthly fees for the relevant cluster. If you have undertaken to restore testing of your cluster in the last 6 months (using our automated restore functionality) and can demonstrate that data loss during an emergency restore is outside target RPO and your verification testing, then you will be eligible for SLA credits at 500% of monthly fees.

Instaclustr Platform Services supporting Debezium® Change Data Capture Services

Tier[1]	Service Standards[2]	Customer Requirements
Starter (Developer nodes)	○ No guaranteed availability[4] (99.9% target) ○ No latency[3] SLAs	○ Add capacity when requested by NetApp to maintain disk usage in normal operations as less than 70% ○ Comply with reasonable requests from NetApp to modify the application for best practice Debezium usage
Enterprise (3+ production nodes)	○ 99.95% availability for get data into Kafka within <5 minutes ○ 10% monthly fees at risk in total; 5% credit for each breach	○ Add capacity or remove data when requested by NetApp to maintain disk usage in normal operations at less than 70% ○ Comply with reasonable requests to modify the application for best practice Debezium usage

**Service Level Objective is for delivery of at least 1 replica to Debezium. Duplicate writes may be delivered.

Instaclustr Platform Services supporting Apache Kafka® Services

Tier[1]	Service Standards[2]	Customer Requirements
Starter[11,18] (Developer nodes)	○ No guaranteed availability[4] (99.9% target) ○ No latency[3] SLAs	○ Minimum replication of 2 on all topics ○ Add capacity or adjust retention settings when requested by the NetApp Instaclustr product team to maintain disk usage in normal operations as less than 80% ○ Comply with reasonable requests to modify application for best practice Kafka usage
Small[17] (5 or less production nodes)	○ 99.95% availability for writes with 2 replica consistency requirement and all reads ○ No latency SLAs	○ Minimum replication of 3 on all topics ○ Add capacity or adjust retention settings when requested by NetApp to maintain disk usage in normal operations as less than 80%

	○ 20% monthly fees at risk in total; 10% credit for each breach ○ PrivateLink availability of 99.99%	○ Comply with reasonable requests to modify application for best practice Kafka usage
Enterprise[17] (6+ production nodes)	○ 99.99% availability for writes with 2 replica consistency requirement and all reads ○ Availability SLA is increased to 99.999% when dedicated ZooKeeper/KRaft nodes are used ○ 99% of read/write transactions to NetApp-maintained topic in the cluster within specified latency threshold[3] ○ 30% of monthly fees at risk in total; 15% credit for each incident causing breach of availability SLA and 10% credit for each incident causing breach of latency SLA ○ PrivateLink availability of 99.99%	○ Minimum replication factor of 3 on all topics ○ Add capacity or adjust retention settings when requested by NetApp to maintain disk usage in normal operations at less than 80% ○ Comply with reasonable requests to modify the application for best practice Kafka usage
Critical[17] (12+ production nodes)	○ 99.999% availability for writes with 2 replica consistency requirement and all reads ○ 99% of read/write transactions to NetApp-maintained topic in the cluster within specified latency threshold[3] ○ 100% of monthly fees at risk in total; 30% credit for each incident causing breach of availability SLA and 10% credit for each incident causing breach of latency SLA ○ PrivateLink availability of 99.99%	○ Minimum replication factor of 3 on all topics ○ Separate testing and production clusters ○ Must use dedicated ZooKeeper/KRaft nodes for production ○ Customer notifies that they wish to receive this SLA, commissions NetApp to review their application for best practice alignment and actions findings from that review ○ NetApp review prior to deploying changes that may impact latency SLA ○ Add capacity or remove data when requested by NetApp to maintain disk usage in normal operations at less than 80% ○ Comply with reasonable requests to modify application for best practice Kafka usage

Instaclustr Platform Services supporting Kafka® Connect Services

Tier[1]	Service Standards[2]	Customer Requirements
Starter[11] (Developer nodes)	○ No guaranteed availability[8] (99.9% target)	○ Add capacity as reasonably requested by NetApp to manage operational loads ○ Comply with reasonable requests to modify the application for best practice Kafka Connect usage
Production Nodes	○ 99.99% availability[8] to NetApp maintained synthetic transaction connector ○ 20% monthly fees at risk in total; 10% credit for each breach	○ Minimum of 3 nodes ○ Add capacity as reasonably requested by NetApp to manage operational loads ○ Comply with reasonable requests to modify the application for best practice Kafka Connect usage

Instaclustr Platform Services supporting Redis® Services

Tier[1]	Service Standards[2]	Customer Requirements
Starter (Developer nodes)	○ No guaranteed availability (99.9% target) ○ No latency[3] SLAs	○ Add capacity as reasonably requested by NetApp to manage operational loads ○ Comply with reasonable requests to modify the application for best practice Redis usage
Enterprise (6+ production nodes)	○ 99.99% availability[9] to NetApp maintained synthetic transaction ○ 30% of monthly fees at risk in total; 15% credit for each incident causing breach of availability SLA and 10% credit for each incident causing breach of latency SLA	○ The number of Redis Replica Nodes is greater than or equal to the number of Redis Master Nodes ○ Add capacity as reasonably requested by NetApp to manage operational loads ○ Comply with reasonable requests to modify the application for best practice Redis usage

Instaclustr Platform Services supporting Valkey™ Services

Tier[1]	Service Standards[2]	Customer Requirements
Starter (Developer nodes)	○ No guaranteed availability (99.9% target) ○ No latency[3] SLAs	○ Add capacity as reasonably requested by NetApp to manage operational loads ○ Comply with reasonable requests to modify the application for best practice Valkey usage
Enterprise (6+ production nodes)	○ 99.99% availability[9] to NetApp maintained synthetic transaction ○ 30% of monthly fees at risk in total; 15% credit for each incident causing breach of availability SLA and 10% credit for each incident causing breach of latency SLA	○ The number of Valkey Replica Nodes is greater than or equal to the number of Valkey Master Nodes ○ Add capacity as reasonably requested by NetApp to manage operational loads ○ Comply with reasonable requests to modify the application for best practice Valkey usage

Instaclustr Platform Services supporting Apache ZooKeeper™ Services

Tier[1]	Service Standards[2]	Customer Requirements
Starter (Developer nodes)	○ No guaranteed availability (99.9% target) ○ No latency[3] SLAs	○ Add capacity as reasonably requested by NetApp to manage operational loads ○ Comply with reasonable requests to modify the application for best practice ZooKeeper usage
Enterprise (3+ production nodes)	○ 99.99% availability[10] ○ No latency[3] SLAs ○ 30% of monthly fees at risk in total; 15% credit for each incident causing breach of availability SLA and 10% credit for each incident causing breach of latency SLA	○ Add capacity as reasonably requested by the NetApp Instaclustr product team to manage operational loads. ○ Comply with reasonable to modify the application for best practice ZooKeeper usage

Instaclustr Platform Services supporting PostgreSQL® Services

Tier	Service Standards	Customer Requirements
Starter (Developer nodes)	○ No guaranteed availability (targeting 99.95%[12]) ○ No latency SLAs	○ Add capacity as reasonably requested by NetApp to manage operational loads. ○ Configure cluster replication and query settings which are appropriate for their data loss tolerance[13] ○ Comply with reasonable requests from the NetApp Instaclustr product team to modify the application for best practice PostgreSQL usage ○ Add capacity or remove data when requested to maintain disk usage in normal operations at less than 70%
Enterprise (2+ production nodes, or 3+ if utilizing synchronous mode strict)	○ 99.99%[12] availability for read and write operations ○ 99.9%[3] of read/write transactions to NetApp-maintained table in the cluster within specified latency threshold ○ 30% of monthly fees at risk in total; 15% credit for each incident causing breach of availability SLA and 10% credit for each incident causing breach of latency SLA	○ Add capacity as reasonably requested by NetApp to manage operational loads ○ Comply with reasonable requests from the NetApp Instaclustr product team to modify the application for best practice PostgreSQL usage ○ Configure cluster replication and query settings which are appropriate for their data loss tolerance[13] ○ Add capacity or remove data when requested to maintain disk usage in normal operations at less than 70%

**Availability uptime is not inclusive of one 60-minute scheduled maintenance window per month. During the maintenance window database connectivity may be interrupted for short periods during switchover to secondary nodes. Customers will be notified of scheduled maintenance at least 7 days in advance.

Instaclustr Platform Services supporting OpenSearch Services[14]

Tier[1]	Service Standards[2]	Customer Requirements

Starter (Developer nodes)	○ No guaranteed availability (99.9% target) ○ No latency[3] SLAs	○ Minimum of one replica shard on all indices ○ Add capacity or adjust retention settings when requested by NetApp to maintain disk usage in normal operations at less than 70% ○ Comply with reasonable requests to modify application and index settings for best practice OpenSearch usage
Small (5 or less production nodes)	○ 99.95% availability[15] for search and index operations, where wait_for_active_shards is 2 or less. ○ No latency SLAs ○ 20% monthly fees at risk in total; 10% credit for each breach	○ Minimum of 2 replica shards on all indices ○ Add capacity or adjust retention settings when requested by NetApp to maintain disk usage in normal operations at less than 70% ○ Comply with reasonable requests to modify the application and index settings for best practice OpenSearch usage
Enterprise (6+ production nodes)	○ 99.99% availability[15] for search and index operations, where wait_for_active_shards is 2 or less ○ 95% of index/search operations to NetApp-maintained Index in the cluster within specified latency threshold[3] ○ 30% of monthly fees at risk in total; 15% credit for each incident causing breach of availability SLA and 10% credit for each incident causing breach of latency SLA	○ Minimum of 2 replica shards on all indices ○ Use dedicated masters ○ Add capacity or adjust retention settings when requested by NetApp to maintain disk usage in normal operations at less than 70% ○ Comply with reasonable requests to modify the application and index settings for best practice OpenSearch usage
Critical (12+ production nodes)	○ 99.999% availability[15] for search and index operations, where wait_for_active_shards is 2 or less ○ 99% of index/search operations to NetApp-maintained index in the cluster within specified latency threshold[3] ○ 30% of monthly fees at risk in total; 15% credit for each incident causing breach of availability SLA and 10% credit for each incident causing a breach of latency SLA	○ Minimum of 2 replica shards on all indices ○ Use dedicated masters ○ Separate testing and production clusters ○ Customer notifies that they wish to receive this SLA, commissions NetApp to review their application and index settings for best practice alignment and actions findings from that review ○ NetApp Instaclustr product team review prior to deploying changes that may impact latency SLA ○ Add capacity or remove data when requested by NetApp to maintain disk usage in normal operations at less than 70% ○ Comply with reasonable requests to modify the application for best practice OpenSearch usage

Instaclustr Platform Services supporting Cadence Services

Tier	Service Standards	Customer Requirements
Starter (Developer Size Nodes)	○ No guaranteed availability (99.9% target) ○ No latency SLAs	○ Add capacity as reasonably requested by NetApp to manage operational loads ○ Comply with reasonable requests to modify the application for best practice Cadence usage. ○ Comply with requirements for Starter level SLAs for dependency services (Cassandra, Kafka, OpenSearch)
Production (3+ Production size nodes for each of Cadence and its dependency service clusters)	○ 99.95% availability as measured by NetApp Instaclustr synthetic transaction monitoring ○ 30% of monthly fees at risk in total; 15% credit for each incident causing breach of availability SLA and 10% credit for each incident causing a breach of latency SLA	○ Add capacity as reasonably requested by NetApp to manage operational loads ○ Comply with reasonable requests to modify the application for best practice Cadence usage ○ Comply with requirements for at least Small level SLAs for dependency services (Cassandra, Kafka, OpenSearch)

Instaclustr Platform Services supporting ClickHouse® Services

Tier	**Service Standards**	**Customer Requirements**
Starter (Developer Nodes)	• No guaranteed availability[4]	• Comply with reasonable requests to modify the

	(99.5% target)	application for best practice ClickHouse usage,
Production – Small (production nodes)	• 99.95% guaranteed availability[4] as measured by NetApp Instaclustr synthetic transaction monitoring • 30% of monthly fees at risk in total; 15% credit for each incident causing breach of availability SLA.	• At least 2 replicas per shard per cluster. • Minimum of 3 nodes per cluster • Add capacity or remove data when requested by NetApp to maintain disk usage in normal operations at less than 70% • Comply with reasonable requests to modify the application for best practice ClickHouse usage.
Production – Enterprise (production nodes)	• 99.99% guaranteed availability[4] as measured by NetApp Instaclustr synthetic transaction monitoring • 30% of monthly fees at risk in total; 15% credit for each incident causing breach of availability SLA.	• At least 3 replicas per shard per cluster. • All clusters must use dedicated ClickHouse Keeper nodes. • Add capacity or remove data when requested by NetApp to maintain disk usage in normal operations at less than 70% • Comply with reasonable requests to modify the application for best practice ClickHouse usage.

Claims Process

If at any time during your Subscription Term, you determine that you are not receiving the Availability Service Level, contact support@instaclustr.com and include the following information in your email:

- Calculated Downtime
- Description in incident of issue
- Cluster ID of impacted cluster(s)

[1]SLA tier is per-cluster and based on the number of nodes in the cluster. Customer credits are calculated based on the fees payable for the cluster or clusters impacted by the incident. SLAs credits apply to production clusters only.

[2]Service levels are measured on a monthly basis based on NetApp Instaclustr's monitoring systems. All service levels exclude outages caused by non-availability of service at the underlying cloud provide region level or availability zone level in regions which only support two availability zones.

[3]Latency is measured at a minimum rate of one read/write pair per node per 20 second period. Latency SLA excludes incidents where the cause is determined to be changes to a customer's application or unusually high loads on the cluster.

[4]Availability is measured by NetApp Instaclustr's synthetic monitoring at a minimum rate of one read/write pair per node per 20 second period. A cluster is considered to be unavailable where read/write operations fail for a majority of nodes in the cluster in a given check-in period.

[5]Where a customer meets requirements for a tier based on cluster size but does not meet other requirements for a tier, the highest level of SLA where all requirements are met will apply.

[6]All SLAs exclude issues caused by customer actions including but not limited to attempting to operate a cluster beyond available processing or storage capacity.

[7]SLA credits must be claimed by customers within 14 days of the end of the relevant calendar month.

[8]For Kafka Connect, availability is measured by NetApp Instaclustr's synthetic monitoring at a minimum rate of one Connector read or write operation per cluster per 20 second period. Excludes issues caused by BYO Kafka Connect Connectors due to the potential impact of user code on the availability of these environments.

[9]For Valkey, availability is measured by NetApp Instaclustr's synthetic monitoring at a minimum rate of one read or write operation per cluster per 20 second period. Excludes latency issues caused by the use of integrated Lua scripting (EVAL and EVALSHA). Excludes issues caused by customers executing commands marked as "dangerous" by the Valkey project (turning on authentication will restrict access to these commands). Details of these commands can be found here.

[10]For ZooKeeper, availability is measured by establishing a connection with the ZooKeeper server on each node using a local ZooKeeper client, on a per node per 20 second basis.

[11]For preview versions of Kafka and Kafka Connect, only their respective "Starter" tier SLAs are valid. Production usage may be brought under an agreed SLA for the GA version after joint testing. Please contact us if you wish to discuss this option.

[12]PostgreSQL availability is measured by NetApp Instaclustr's synthetic monitoring at a minimum rate of one read/write pair per node per 20 second period. A cluster is considered to be unavailable where read/write operations fail for all nodes in the cluster in a given check-in period. PostgreSQL SLAs exclude issues caused by customer actions including but not limited to; attempting to operate a cluster beyond available processing or storage capacity, modifications to application configuration, or customer initiated reloads or resizes. PostgreSQL uptime is not inclusive of one 30-minute scheduled maintenance window per month. Customers will be notified of scheduled maintenance at least 7 days in advance, and the NetApp Instaclustr product team will make all reasonable attempts to minimize the impact to your availability.

[13]Client PostgreSQL applications should be configured in order to maintain high availability and reestablish connections in the event of a master replica failure. For more information see Replication and High Availability

[14]OpenSearch SLAs also apply to legacy OpenDistro for Elasticsearch clusters.

[15]The KNN plugin will use additional off heap memory. The default cache and selected node size may be inappropriate depending on the specific use of the plugin combined with other OpenSearch activities. This may result in cluster instability and customers need to be aware this could impact high availability of the cluster.

[16]Clusters created as "Bundled Use Only" are covered by SLAs only when used purely as a supporting service for another NetApp Instaclustr offering (i.e., no direct access).
[17]Enterprise Add-ons for Kafka (Schema Registry, REST Proxy, Karapace Schema Registry and Karapace REST Proxy) are excluded from availability and latency SLAs.
[18]For preview versions of Enterprise Features for Kafka, only the "Starter" tier SLAs are valid. Production usage may be brought under an agreed SLA for the GA version after joint testing. Please contact us if you wish to discuss this option.

3. Open-Source Software

In the event NetApp distributes or otherwise provides for Customer any software for which the original source code is made freely available to the public under a designated open source license which permits users to use, change, and improve the software, and to redistribute it in modified or unmodified form ("Open Source Software") to Customer in furtherance of the delivery of the services associated with this Order Form, then such Open Source Software is subject to the terms of the applicable open source license. To the extent there is a conflict between the terms and conditions of this Order Form and the terms and conditions of the applicable open-source licensee, the terms and conditions of the open-source license will prevail.

Bug fixes, patches and features developed for Open-Source Software (Open-Source Contribution), because of the services associated with this Order Form, may be released by NetApp to the Apache Software Foundation project or other relevant open-source project at any time (a "Open-Source Software Contribution"). The parties agree that, despite any other provision in the Order Form, neither NetApp nor Customer has any right (including IP Rights), title or interest in the Open-Source Contribution.

4. Service Use for Processing Personal Information

If personal information has not been specified in the Order Form, Customer will not use the Services for the storage and processing of personal information without NetApp's consent.

If personal information has been specified in the Order Form. NetApp acknowledges that Customer will use of the Services for the storage and processing of personal information. Where personal information is stored in the Services NetApp recommends:

- Using application encryption (as appropriate) for all personal information before storage in the Services;
- Enabling Customer to Server encryption when provisioning clusters;
- For clusters running in AWS, enabling EBS encryption within the Services when provisioning clusters;
- Meeting NetApp's published baseline security control requirements for NetApp Instaclustr services applicable to Customers;
- Meeting all Customer security responsibilities as described in the Agreement; and
- Implementing any additional security controls as are reasonably recommended by NetApp.

Customer must provide NetApp, at reasonable periods, information regarding the total number of personal records stored within the Services to enable NetApp to meet its security, insurance, and other compliance requirements.

In order to provide you with the most effective response, information submitted to NetApp via email or our support portal may be sent to any or all members of our support team, in Australia, UK, Europe, India and the US. As such, NetApp requires that you ensure that information that is considered Personal Information, Health Information, or PCI related data is NOT submitted to NetApp via email, our support portal or any chat interface. The only approved mechanism for submitting such data, is directly to a managed cluster.

NetApp will manage Customer's clusters and information as stated in NetApp's SOC-2 accreditation. NetApp will not be liable to Customer for any data breach arising from Customer's failure to implement any of the above recommendations.

5. **PCI Compliance**. If Customer wishes to run a cluster in PCI mode, Customer must comply with the requirements as set out in the PCI Responsibilities Document available at
https://www.instaclustr.com/support/documentation/useful-information/pci-compliance/

6. **Security Incident reporting**
Any incident suspected in Customer Facing Infrastructure must be reported to **support@instaclustr.com**, which will instigate the Major Incident Management process.
For the purposes of this procedure, Customer Facing Infrastructure means any customer managed environment, regardless of whether it is Run In Instaclustr's Account, Run in Your Own Account, or Run In Customer Managed Infrastructure/ On-Premise. It also includes support only customers, where we support the infrastructure that is the subject of the incident.

7. **Customer Responsibilities—Baseline Security Controls**
   At a minimum, we require you to implement and monitor the following aspects of the security of your account and cluster. You are responsible for:
   a. Configuring firewall rules via the NetApp Instaclustr Console.
   b. Configuring encryption between the client and the cluster.
   c. Approving user access to the cluster.
   d. Removing user access to the cluster on a timely basis.
   e. Providing accurate, current, and complete information in their communications with NetApp.
   f. Reading release notes published on the website www.instaclustr.com.
   g. Determining the authentication method to the console from those supported by NetApp (i.e. password rules or two-factor authentication).
   h. Cluster capacity planning and cross data center performance considerations.
   i. Defining and configuring the number of nodes and hence the layers of redundancy required.
   j. Adding, managing and removing the data stored on the NetApp Instaclustr platform.

8. **Data Protection.** NetApp will maintain commercially reasonable administrative, physical and technical safeguards to protect the security, confidentiality and integrity of Customer's Data. All NetApp Instaclustr services rely on Office365 and Zendesk for customer interactions. NetApp has reviewed and are satisfied that these services meet a reasonable level of security for information typically provided to our technical support team. Customer should review the security practices of Office365 and Zendesk to confirm that Customer is satisfied that the level of protection is appropriate for any data Customer is considering submitting to NetApp. The links to their security practices are provided below:
   Microsoft Office365 Security
   Zendesk Security

9. **Managed Services**
   (a) **Data Protection.** Cluster safeguards include the ability to enable encryption of Customer's Data at rest and in transmission to Your Environment (using TLS or similar technologies) over the Internet, except for any Third-Party Services that does not support encryption, which Customer may link to through the Services at Customer's election. Some NetApp Instaclustr instances do not support encryption. This is clear in the NetApp Instaclustr console on cluster creation, and Customer is responsible for ensuring that the protection required for Customer's Data is appropriately enabled.

   (b) **Data Center Environment and Physical Security.** The Sub-processors which are utilized by NetApp, as per Customer's instructions, for hosting services in connection with NetApp's provision of the NetApp Instaclustr Service employ their own security measures. Customer is responsible for verifying that the measures of Customer's chosen provider are appropriate for Customer's use case. NetApp review each supported providers SOC2 report and are satisfied that they meet an appropriate level of protection for both NetApp and NetApp's Customer's Data. NetApp recommends that Customer obtains and review the SOC2 report of the underlying Cloud Provider(s) that Customer is considering. Where Services are within the scope of NetApp security accreditations, NetApp will review at least the SOC2 report of the service at least once per year. Any issues will be assessed in accordance with NetApp's vulnerability assessment process.

NetApp

DATA PROCESSING ADDENDUM

This NetApp Data Processing Addendum including its integral part Schedule 1 (**"Addendum"**) supplements the Agreement between NetApp, Inc. and its affiliates, including the NetApp affiliate performing the Services (**"NetApp"**), and Customer (together the **"Parties"**). To the extent there is a conflict between the Agreement and the terms of this Addendum, the terms of this Addendum will prevail unless otherwise expressly set forth herein.

1. DEFINITIONS. Capitalized terms used but not defined in this Addendum have the meanings set forth in the Agreement.

1.1. "**Agreement(s)**" means the applicable written agreement(s) between NetApp and Customer under which NetApp provides Services to Customer.

1.2. **"Clauses"** mean the standard contractual clauses (2021/914) published by the European Commission including any successor clauses.

1.3. "**Customer Content**" means any information, in any form, format or media (including paper, electronic and other records), provided by Customer that NetApp may operate on, where such operation is on the Customer's behalf as part of providing Services.

1.4. **"Customer Personal Information"** means Personal Information contained in Customer Content that NetApp Processes as a Data Processor on behalf of Customer in performing the Services.

1.5. "**Data Controller**" means an entity which, alone or jointly with others, determines the purposes and means of Processing of Personal Information.

1.6. **"Data Processor"** means an entity which Processes Personal Information on behalf of the Data Controller.

1.7. "**Data Protection Laws**" mean any applicable laws, regulations, and other legal requirements relating to (a) privacy or protection of Personal Information and / or (b) the Processing of Personal Information, including the EU General Data Protection Regulation (**"GDPR"**) and the EU Member State data protection laws implementing or supplementing GDPR, the UK General Data Protection Regulation (**"UK GDPR"**) as well as the Swiss Federal Act on Data Protection (**"FADP"**).

1.8. **"EEA"** means European Economic Area.

1.9. **"Effective Date"** means the date on which the Customer signs this Addendum.

1.10. **"Module(s)"** means the set of clauses that the EU Standard Contractual Clauses for the transfer of personal data to third countries provide for each of the following transfer scenarios: (a) Transfer controller to controller (Module 1); (b) Transfer controller to processor (Module 2); (c) Transfer processor to processor (Module 3); and (d) Transfer processor to controller (Module 4).

1.11. **"Personal Information"** means (a) any information relating to an identified or identifiable natural person; or (b) is defined as "personal data" or "personal information" by applicable laws or regulations relating to the Processing of information about an identified or identifiable person.

1.12. "**Process**" or "**Processing**" means any operation or set of operations performed on Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.13. **"Security Incident"** has the meaning assigned to it in Section 8 (Security Incident).

1.14. **"Services"** means the services provided by NetApp as set forth in the Agreement. Services may include NetApp's as a service offering which a Customer purchases as a subscription for a defined term ("**Cloud Services**"), NetApp's consulting services ("**Professional Services**") and/or NetApp's generally available technical support and maintenance services programs ("**Support Services**") which may be further specified in service descriptions or statements of work.

1.15. **"UK Addendum"** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, version B1.0 (21 March 2022).

2. APPLICABILITY; ROLES OF PARTIES. This Addendum applies to the extent that NetApp Processes Customer Personal Information as a Data Processor on behalf of Customer in performing Services. As between the parties, NetApp acts as a Data Processor and Customer acts as a Data Controller of such Customer Personal Information. NetApp will Process Customer Personal Information solely to provide Services in accordance with the Agreement or other documented instructions that Customer may provide (whether in written or electronic form) in accordance with the Agreement, or as otherwise required by applicable law. If NetApp is required by applicable law to Process Customer Personal Information other than in accordance with the Agreement or other documented instructions of Customer, NetApp will inform Customer of that legal requirement prior to such Processing, unless prohibited by applicable law.

3. CONFIDENTIALITY. NetApp will require NetApp personnel who will be provided access to, or will otherwise Process, Customer Personal Information, to protect Customer Personal Information consistent with the standards set forth in this Addendum and the Clauses.

4. COMPLIANCE WITH LAWS. NetApp will comply with all Data Protection Laws applicable to NetApp as a Data Processor Processing Customer Personal Information on Customer's behalf, to the extent NetApp engages in such Processing. Customer will comply with all Data Protection Laws applicable to Customer with respect to such Processing of Customer Personal Information.

5. SUB-PROCESSORS. Customer agrees that NetApp has Customer's general authorization to use subcontractors to Process Customer Personal Information for purposes of providing the Services to Customer ("**Sub-processors**"), provided that NetApp will impose on its Sub-processors data protection obligations that are at least as protective of Customer Personal Information as those set forth in this Addendum. NetApp will make a list of Sub-processors available to Customer by posting it to a Customer-accessible site. NetApp will notify Customer of any new Sub-processor by posting an updated list of Sub-processors at least thirty (30) days before authorizing any new Sub-processor to Process Customer Personal Information. Customer may object to such addition by written notice to NetApp. NetApp will be liable for the acts or omissions of its Sub-processors to the same extent as if the acts or omissions were performed by NetApp. NetApp will disclose Customer Personal Information only to Sub-processors or as otherwise expressly authorized under the Agreement (including this Addendum) or as required by law.

6. DATA TRANSFERS. In providing the Services, NetApp and its Sub-processors may transfer and access Customer Personal Information to and from other countries where they have operations, or as otherwise required by applicable law. NetApp will implement appropriate measures to protect Customer Personal Information in accordance with this Addendum regardless of the jurisdiction in which it is located.

7. SECURITY. NetApp will implement reasonable technical and organizational safeguards designed to protect Customer Personal Information in its possession or control against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to such data in accordance with Schedule 1.D. NetApp may modify such safeguards from time to time, provided that such modifications will not materially reduce the overall level of protection for Customer Personal Information.

8. SECURITY INCIDENT. If NetApp discovers that a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to Customer Content or Personal Information in the possession or control of NetApp (a **"Security Incident"**) has occurred, NetApp will notify Customer promptly and without undue delay, in accordance with legal obligations and unless otherwise prohibited by law or otherwise instructed by a law enforcement or supervisory authority. Such notification will provide information about the nature and likely consequences of the Security Incident and how to request additional information if required. In addition to providing such notification, NetApp will promptly take reasonable steps to mitigate the effects of the Security Incident and to minimize any damage resulting from the Security Incident.

9. AUDIT AND INSPECTIONS. Notwithstanding anything to the contrary in the Agreement, and taking into account the nature of the Processing and the Services being provided, the following processes will be used to satisfy any audit or inspection requests by or on behalf of Customer and to demonstrate compliance with applicable obligations of NetApp as set forth in this Addendum including the Clauses:

9.1. Cloud Services. For Cloud Services, at least once per calendar year, NetApp will obtain an ISO/IEC 27001:2013 certification or retain an independent third-party auditor to prepare a Services Organization Control 2 (Type II) report or industry-standard successor report ("**Report**"). Upon Customer's written request, NetApp will provide to Customer within a reasonable time at no cost a copy of the most recent Report, up to once per year.

9.2. Professional Services and Support Services. For Professional Services and Support Services, NetApp will, upon Customer's written request, up to once per year (i) provide to Customer at no cost a copy of the most recent third-party certification or Report for such Services, if NetApp has obtained a certification or Report for such Services; or (ii) provide Customer with reasonable information concerning its data protection measures for such Services to help Customer comply with its audit obligations or a competent Supervisory Authority's request ("**Supplemental Information**").

9.3. Reports and Supplemental Information. Such Reports and Supplemental Information will be NetApp's Confidential Information under the confidentiality provisions of the Agreement.

9.4. Regulatory Access. NetApp will permit applicable regulator access as required by law and when on-site documentary and evidence review by the regulator is deemed insufficient by the regulator for their purpose of regulating the Customer or NetApp.

10. REQUESTS OR COMPLAINTS FROM INDIVIDUALS. NetApp will promptly notify Customer, unless prohibited by applicable law, if NetApp receives: (i) any requests from an individual with respect to Customer Personal Information Processed by NetApp, including but not limited to opt-out requests, requests for access and/or rectification, blocking, erasure, requests for data portability, and all similar requests; or (ii) any complaint relating to the Processing by NetApp of Customer Personal Information, including allegations that such Processing infringes on a data subject's rights. Customer is responsible for responding to such requests and complaints from individuals. Taking into account the nature of the Processing, NetApp will assist the Customer by appropriate technical and organizational measures, insofar as reasonably possible, for the fulfillment of the Customer's obligation to respond to such requests or complaints.

11. DURATION; RETURN OR DISPOSAL. The duration of the Processing will be the term of the Agreement or until all Customer Personal Information has been returned or deleted in accordance with the following. Upon termination or expiration of the Agreement for any reason, (i) for Cloud Services, Customer will be entitled to retrieve its Customer Personal Information in accordance with the Agreement, and NetApp will delete Customer Personal Information from the Services following such retrieval period unless otherwise required by applicable law, or (ii) for Professional Services or Support Services, NetApp will delete or return Customer Personal Information in its possession or control in accordance with the Agreement, unless otherwise required by applicable law.

12. ADDITIONAL PROVISIONS FOR THE EEA + UK + SWITZERLAND. The following additional provisions apply with respect to the Processing of Customer Personal Information of data subjects of the EEA:

12.1. GDPR. Taking into account the nature of the Processing and the information available to NetApp, NetApp will make reasonable efforts to assist Customer upon request in fulfilling any obligations Customer may have under GDPR to: (a) provide notification of a Security Incident to the supervisory authorities or affected individuals, or (b) perform a data protection impact assessment if required. NetApp reserves the right to charge a reasonable fee for such assistance, to the extent permitted by applicable law. NetApp shall immediately inform Customer, if in NetApp's opinion, instructions given by the Customer in relation to Customer Personal Information of data subjects of the EEA infringe GDPR or EEA member states data protection provisions.

12.2. Clauses. To the extent that Customer transfers Customer Personal Information of data subjects of the EEA or Switzerland to NetApp in a third country that is not deemed to provide an adequate level of data protection, Modules 2 and/or 3 of the Clauses will govern such transfers as determined in accordance with Schedule 1.A. To the extent that Customer transfers Customer Personal Information of data subjects of the United Kingdom to NetApp in a third country that is not deemed to provide an adequate level of data protection, the UK Addendum will govern such transfers.

12.3. Nothing in this Addendum modifies or amends the terms of the Clauses.

NetApp

SCHEDULE 1

Specific to Annex I of the Clauses:

A. LIST OF PARTIES

Customer:

The Customer who entered into the Agreement with NetApp is a controller of the Customer Personal Information; (Module 2 applies) and / or a processor of the Customer Personal Information; (Module 3 applies) The Customer is also the data exporter.

NetApp:

The NetApp entity who entered into the Agreement with Customer is a Data Processor of the Customer Personal Information on the Customer's behalf.

The data importer is NetApp, Inc. with its address at 3060 Olsen Drive, San Jose, CA 95128, United States E-mail: ng-privacy@netapp.com
Phone number: +1 408-822-6000

B. DESCRIPTION OF PROCESSING / TRANSFER

Categories of Data Subjects

Unless otherwise specified by the data exporter, transferred Customer Personal Information relates to the following categories of data subjects:

- Employees, contractors and temporary workers (current, former, prospective) of data exporter;
- NetApp's Customers' collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former);
- Users (e.g., Customers, clients, patients, visitors, etc.) and other data subjects that are users of NetApp's or its Customers' services; and
- Partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with employees of NetApp's Customer and/or use communication tools such as apps and websites provided by NetApp or its Customers.

Categories of Data Transferred

The transferred Personal Information may be collected and/or processed includes data in multiple formats, including email, documents and other electronic forms. Depending on the applicable use of the Services, NetApp may collect and/or process Personal Information from any of the following categories:

- **Individual Identifiers** – This includes information like an end users name, email address, physical address, telephone number, login alias, IP address or other Information that identifies you regardless of your relationship to NetApp.
- **Customer Records** – This includes information like an end user's company name, job title, account number, Customer identifier, or other Information that relates to an end user as a Customer of NetApp.
- **Commercial Information** – This includes payment card data, financial account information, account information, records of products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies of the customer, and other information necessary to collect and process payment for products and services ordered by the customer.
- **Electronic Network Information** – This includes information like browser and device data, and internet or network activity information, such as activity on our Websites and Services, data collected through cookies, pixel tags and other technologies, and other information that is generated through the end user's use of the internet to access our websites.

Frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

The transfer may occur on a continuous or one-off basis depending on the Products or Services outlined in the underlying agreement(s).

Nature of the processing

Where NetApp is the Data Processor, Processing may include the collection, use, analysis, storage, and deletion, including the sharing of data with authorized third party subprocessors for the purposes of providing, monitoring, and improving products or services where NetApp acts as the Data Processor.

The transferred Personal Information may be subject to the following basic processing activities:

- use of Personal Information to set up, operate, monitor and provide the Products or Services (including operational and technical support), including communication to Authorized Users;
- continuous improvement of Product or Service features and functionalities provided as part of the Services including automation, transaction processing and machine learning;
- provision of Professional Services;
- release, development and upload of any fixes or upgrades to the Products or Services;
- storage, back up and restoration of Personal Information stored in the Products or Services;
- computer processing of Personal Information, including data transmission, data retrieval, data access;
- network access to allow Personal Information transfer; and
- monitoring, troubleshooting and administering the underlying service infrastructure and database; security monitoring, network-based intrusion detection support, penetration testing.

Purpose(s) of the data transfer and further processing

Where NetApp is the Data Processor, the data transfer is required to provide the Products and Services, ancillary support and Support Services, monitor, develop and improve the Products and Services, and to develop new related Products and Services.

Data Retention Period

NetApp will retain Customer Personal Information for as long as needed or permitted in light of the purpose(s) for which it was obtained per the underlying Agreement and consistent with applicable law.

Transfers to Sub-processors shall be on the same basis.

C. COMPETENT SUPERVISORY AUTHORITY

In respect of Modules 2 and 3 (if applicable), the Customer's supervisory authority is the supervisory authority in accordance with Clause 13 of the Clauses.

Specific to Annex II of the Clauses:

D. TECHNICAL AND ORGANISATIONAL MEASURES

NetApp takes reasonable and appropriate measures to secure personal of data subjects, taking into account the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the Processing for the data subject. NetApp further makes available to its customers certain features and functionalities of NetApp products and services, such as support for encryption or pseudonymisation, including during transmission of Customer Personal Information, to help customers implement reasonable and appropriate measures to secure the Customer Personal Information. For those products and services that are covered under the scope of this Addendum, NetApp implements at least the following security controls and carries out regular checks that these measures continue to be in place and are functioning as designed:

D.1 Physical Security & Access Controls

NetApp maintains physical security controls at all NetApp sites that contain an information system that uses or houses personal data. These physical security controls include measures to restrict entry to non-public areas of the site and to restrict physical access to servers and other physical components of the information system and include the following:

- Identification badges automatically authenticated against lists of authorized personnel required to enter NetApp facilities;
- Emergency and contingency plans in place for NetApp facilities;
- Prior authorization required for use of removable media (e.g., USB sticks and CD ROMs); and
- Data center records of the incoming and outgoing physical media, authorized sender/recipients, date and time, and the number of media.

D.2 Technical Security & Access Controls

NetApp maintains technical security and access controls designed to restrict access to personal data to only those personnel required to access the personal data for the purposes set forth in NetApp's Privacy Policy (available at https://www.netapp.com/company/legal/privacy-policy/), including:

- Use of complex password requirements and required multifactor authentication;

- Unique administrator account IDs and passwords;
- Prohibition on shared passwords;
- Encryption requirements for Internet transmission of personal data;
- Role-based access controls on information systems containing Confidential or Restricted Confidential personal data;
- Role-based access controls to its information systems, including firewalls, intrusion detection and prevention systems, access control lists, and routing protocols; and
- Data loss prevention tools and systems implemented on company issued laptops and mobile devices.

D.3 Organizational Controls

NetApp maintains policies, procedures, and protocols designed to limit the collection, use, and sharing of Personal data to authorized individuals and entities, including:

- Security Policies in place for end users and administrators of corporate systems;
- Global Privacy Policy addressing OECD Privacy Principles;
- Global Data Governance Policy;
- Global Retention Schedule;
- Global Procurement Process to ensure vendor/supplier security standards or controls;
- Privacy by Design validation program;
- Contracting protocols to pass privacy obligations to processors and subprocessors;
- Regular testing of controls by internal audit;
- Regular reviews of Business Continuity and Disaster Recovery plans;
- Regular tabletop exercises on security incident response; and
- Annual privacy and cybersecurity training for all employees.

D.4 Deletion & Disposal Controls

NetApp maintains a data governance policy and related controls designed to ensure that personal data is not retained in records for longer than required under the lawful basis for processing, including:

- The de-identification of records containing personal data once the personal data is no longer necessary for the purpose of record keeping;
- Protocols for the sanitization and/or disposal of NetApp owned equipment and media containing personal data; and
- Protocols for the sanitization of customer equipment and media under return authorization.

Specific to Annex III to the Clauses:

E. AUTHORIZED SUB-PROCESSORS

Subject to and in accordance with Clause 9(a) in Module 2 and Module 3 (if applicable), NetApp has Customer's general authorization to engage the Sub-processors from the following Agreed List. To the extent that "NetApp" for the purposes of the Agreement does not also include affiliates, the NetApp Affiliates are also Sub-processors.

Specific to Clause 17 of the Clauses:

F. GOVERNING LAW

The Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands without regard to conflict of law principles.

Specific to Clause 18(b) of the Clauses:

G. CHOICE OF FORUM AND JURISDICTION

(b) The Parties agree that those shall be the courts of Amsterdam, the Netherlands.

Specific to the adoption of the Clauses for Switzerland:

H. SWISS AMENDMENT

It is agreed that nothing in Clause 18 of the Clauses excludes data subjects in Switzerland from the possibility of suing for their rights in the competent courts in Switzerland.

I. UK Addendum

If applicable, to be provided under separate cover.

* * *