NetApp

INFORMATION SECURITY ADDENDUM

THIS NETAPP INFORMATION SECURITY ADDENDUM (THE "SECURITY ADDENDUM") SETS FORTH THE ORGANIZATIONAL, TECHNICAL, PHYSICAL, AND ADMINISTRATIVE, SAFEGUARDS THAT NETAPP, INC., NETAPP IRELAND, LTD. AND/OR A NETAPP AFFILIATE (COLLECTIVELY "NETAPP") TAKE TO PROTECT CUSTOMER CONTENT. THIS SECURITY ADDENDUM IS APPLICABLE TO ALL NETAPP HARDWARE, SOFTWARE AND CLOUD SERVICES PURCHASED OR LICENSED, INCLUDING ANY RELATED SUPPORT OR PROFESSIONAL SERVICES (AS APPLICABLE) DIRECTLY FROM NETAPP OR INDIRECTLY FROM A NETAPP PARTNER OR, WHERE APPLICABLE, A NETAPP CLOUD PROVIDER. NETAPP RESERVES THE RIGHT TO UPDATE THIS SECURITY ADDENDUM TO REFLECT CHANGES IN NETAPP'S SECURITY POSTURE, PROVIDED SUCH CHANGES DO NOT MATERIALLY DIMINISH THE LEVEL OF SECURITY DELINEATED HEREIN. THIS SECURITY ADDENDUM IS MADE A PART OF THE TERMS IN PLACE BETWEEN THE PARTIES AND ANY CAPITALIZED TERMS USED BUT NOT DEFINED WILL HAVE THE MEANING SET FORTH IN THOSE TERMS. IN THE EVENT OF ANY CONFLICT BETWEEN THOSE TERMS AND THIS SECURITY ADDENDUM, THIS SECURITY ADDENDUM WILL CONTROL.

1. NETAPP INFORMATION SECURITY PROGRAM

1.1 Information Security Program Overview. The NetApp Information Security Program ("Security Program") will: (a) comply with industry-recognized information security standards; (b) incorporate technical, physical, and organizational safeguards to prevent unauthorized loss, destruction, alteration, access, or disclosure of Customer Content under NetApp's possession or control; (c) be tailored to the nature, size, and complexity of NetApp's business operations; and (d) be suitable for the type of Customer Content that NetApp processes. These standards are approved by the NetApp Chief Security Officer (CISO) and undergo a formal review annually.

1.2 Information Security Program Governance and Training. NetApp maintains an organizational information security governance structure that contains: (a) training on the Security Program, on at least an annual basis for all employees and relevant subcontractors involved in processing Customer Content; and (b) appropriate disciplinary measures for any non-compliance with the Security Program

1.3 Information Security Program Self-Assessments. NetApp performs regular internal control assessments using a risk-based methodology to verify the effectiveness of its controls in terms of design and operation. Identified issues from these assessments are properly documented, tracked, and addressed through appropriate remediation measures.

1.4 Information Security Program Third-Party Assessments. NetApp maintains a third-party audit program as an integral component of its certification process to validate the ongoing governance and effectiveness of the NetApp Security Program. Any issues identified during these audits are diligently documented, tracked, and remediated in a timely manner. The NetApp corporate network environment is certified under ISO/IEC 27001. NetApp has, and will maintain, ISO and SOC certifications for specific Cloud Services, as outlined in detail in the NetApp Trust Center (www.netapp.com/esg/trust-center/).

2. SECURITY CONTROLS – NETAPP CORPORATE NETWORK

2.1 Logical and Technical Controls. NetApp implements appropriate logical and technical controls within its corporate network environment to ensure the segregation of data, systems, and network access in accordance with the principles of least privilege and need to know. NetApp actively monitors demarcation points, such as firewalls and security group enforcement points, to enforce access restrictions within its corporate environment. Industry-standard technologies are employed to promptly detect and remediate any unauthorized access or compromise of NetApp's network, servers, or applications. The NetApp corporate network environment is designed and managed to ensure network availability and reliability by utilizing network segmentation. NetApp employs industry-standard encryption techniques to ensure the encryption of Customer Content at rest. Additional security features include but are not limited to: (a) activity logging that includes suspicious activity; (b) monitoring of protected logs; (c) procedures for an emergency shutdown to prevent data leakage; (c) antivirus/anti-malware protection with automated workstation compliance; and (d) vulnerability scanning and intrusion prevention.

2.2 User Authentication. NetApp maintains an accurate and up-to-date record of authorized users, including employees and subcontractors, within the NetApp corporate environment ("User" or "Users"). Each User will be assigned a unique individual identification (ID) that, when used in combination with a compliant password, is required for user authentication across applications, operating systems, databases, and network devices. This unique User ID shall enable

the identification and tracking of individual activities on the network, including any access to Customer Content. The assignment of access rights and levels are based on the specific job function and role of each User. NetApp enforces two-factor authentication for all Users as a security measure before granting remote access to the NetApp corporate network environment.

2.3 Password Policy. NetApp requires Users to configure complex passwords at least ten (10) alphanumeric characters long. All passwords are converted to an obfuscated, hashed form to prevent those with access to the authentication systems from deriving the actual passwords of other users. User passwords must be changed periodically to comply with NetApp password management policies, or they will expire and become unusable. NetApp limits invalid login attempts to gain access to the corporate network environment. NetApp maintains procedures to deactivate passwords that have been compromised or inadvertently disclosed.

2.4 Vulnerability Management. NetApp has a vulnerability management program to continuously monitor for vulnerabilities to the corporate network environment utilizing scans, offensive exercises, reports by employees, or external reports from vendors or others. NetApp documents vulnerabilities and ranks them according to industry best practices. NetApp assigns appropriate teams to conduct remediation and track progress to resolution. This includes patch prioritization and expedited installation of newly issued critical patches. NetApp implements patch management procedures and tracking of deferred applications along with any additional mitigating controls.

2.5 Penetration Testing. NetApp conducts a third-party penetration test on its corporate network environment at least once every twelve (12) months. If vulnerabilities are identified during these penetration tests, then the findings will be thoroughly evaluated, documented, and assigned to the relevant internal teams for remediation based on their severity level. Upon receiving a written request, NetApp may provide a Customer with a penetration testing attestation letter.

3. SECURITY CONTROLS – NETAPP FACILITIES

3.1 Employee Facility Access. NetApp provides physical access to NetApp facilities in accordance with the individuals' roles and responsibilities. Access privileges are granted based on the specific requirements of each role. NetApp's policy is to promptly revoke physical access when it is no longer necessary, including instances of employee termination or when access is no longer relevant to an individual's role or responsibilities. NetApp subcontractors are subject to the same physical access requirements as NetApp employees.

3.2 Visitor Facility Access. NetApp maintains a visitor access policy that mandates all visitors to obtain prior approval before accessing NetApp facilities. Additionally, all visitors must always be accompanied by an authorized individual from NetApp during their visit. To ensure proper documentation, NetApp logs and reviews access of all visitors to its facilities.

3.3 Additional Facility Security Measures. NetApp employees and visitors must visibly display and wear identity badges when in NetApp facilities. NetApp employs additional measures to protect its employees and assets, including video surveillance systems, onsite security personnel, and other industry-standard technologies and practices.

3.4 Facility Construction. The construction of the facilities and systems where Customer Content is stored by NetApp is intentionally designed to prevent, discourage, and identify unauthorized access or activity. NetApp's physical security measures employ a combination of building design, environmental controls, and electronic, physical security systems to effectively safeguard NetApp staff and assets.

4. SECURITY CONTROLS – NETAPP HARDWARE, SOFTWARE, AND CLOUD SERVICES

4.1 Secure Development Lifecycle. NetApp has established and implemented a Secure Development Life Cycle ("SDLC") methodology that governs the entire development lifecycle of its Software and Cloud Services.

4.2 Secure Development Lifecycle Methodology. NetApp uses a risk-based approach when applying its standard SDLC methodology. This includes, but is not limited to, the following practices: (a) performing static application security testing; (b) security architecture reviews; (c) open-source and other third-party software security scans; (d) secure code review; and (e) dynamic application security testing.

4.3 Code Versioning and Access. NetApp utilizes code versioning control systems to maintain the integrity and security of its Software and Cloud Service application source code. Access privileges to source code repositories will be subject to periodic review and will be strictly limited to authorized Users.

4.4 Segregation of Development Environments. NetApp policy requires that test and production environments for its Software and Cloud Services be appropriately segregated.

4.5 Code Signing. NetApp cryptographically signs its binary code to protect against tampering and to serve as proof of authenticity and ownership.

4.6 Vulnerability Management. NetApp has a vulnerability management program to continuously monitor for vulnerabilities to the Software or Cloud Services through scans, offensive exercises, reports by employees, or external reports from vendors or others. NetApp documents vulnerabilities and ranks them based on severity level as determined by the likelihood and impact ratings determined by CVSS scores. NetApp assigns appropriate internal teams to conduct remediation and track progress to resolution as needed, including patch prioritization and expedited installation of newly issued critical patches. NetApp implements patch management procedures that document the risk a patch mitigates, the approvals provided prior to patch application, and tracking of any exceptions.

4.7 Penetration Testing. NetApp conducts penetration testing on NetApp Software and Cloud Services. If vulnerabilities are identified during these penetration tests, then the findings will be thoroughly evaluated, documented, and assigned to the relevant internal teams for remediation based on their severity level. Upon receiving a written request, NetApp may provide a Customer with a penetration testing attestation letter.

4.8 Encryption in Transit. NetApp offers, if applicable, industry standard encryption techniques to encrypt Customer Content which is managed by the Software or Cloud Service in transit. NetApp uses encryption at rest with a minimum encryption protocol of Advanced Encryption Standard ("AES") 128-bit encryption. NetApp also uses encryption key management processes to help ensure the secure generation, storage, distribution, and destruction of encryption keys.

4.9 User Authentication. NetApp utilizes multi-factor authentication, in collaboration with an external identity provider, to validate the identity and authenticate Users seeking access to Software or Cloud Services that host Customer Content. NetApp diligently maintains comprehensive records of security privileges granted to individuals with access to Software or Cloud Services containing Customer Content. These logs are securely protected at rest and are solely accessible to authorized support users for incident response purposes. NetApp will maintain policies and employ appropriate tools to identify any irregularities in access or usage. In the event of such irregularities, NetApp promptly detects and proposes necessary remediation efforts to address the situation.

5. SECURITY CONTROLS - PERSONNEL

5.1 Personnel Training. NetApp employees are obligated to undergo security training as a mandatory component of the new hire process. Additionally, all NetApp employees receive annual training and targeted information as necessary and appropriate to ensure ongoing compliance with NetApp's Information Security Program, as well as relevant security and confidentiality policies. These training initiatives also encompass adherence to other corporate policies, including the NetApp Code of Conduct. NetApp subcontractors receive targeted information and training as required to ensure ongoing compliance with NetApp's policies and any customer-specific requirements, if applicable.

5.2 Background Checks. NetApp conducts background verification checks on employees as part of the new employee onboarding process, in accordance with applicable laws. NetApp subcontractors are required to have passed a background check that is compliant with NetApp's background check requirements.

5.3 Subcontractors. NetApp has established a written agreement with each subcontractor engaged for the provision of services to NetApp. This agreement outlines the necessary confidentiality requirements and security controls to be implemented by the subcontractor, as applicable to the services they render. These requirements align with the obligations stated in this Security Addendum. Customer Content is only shared with subcontractors who have entered into appropriate confidentiality agreements with NetApp and possess a legitimate need to access such information for the purpose of delivering applicable services.

6. SECURITY CONTROLS - SUPPLY CHAIN

6.1 Vendor Management. NetApp's agreements with vendors incorporate risk-based security obligations, which are determined based on the specific product and/or service supplied, and the Customer Content shared with the vendor. Prior to onboarding vendors, NetApp conducts comprehensive security due diligence and risk assessments to evaluate and mitigate potential security risks associated with vendors. NetApp will ensure that suppliers engaged in the development of NetApp Hardware, Software, and Cloud Services adhere to a secure development lifecycle process.

6.2 Supply Chain Certifications. NetApp is certified to the International Organization for Standardization (ISO) 9001:2015 and ISO 14001:2015 certification standards. NetApp is Tier 2 certified under the U.S. Customs and Border Protection's (CBP) Customs Trade Partnership Against Terrorism (CTPAT) program.

7. DISASTER RECOVERY

In compliance with established industry standards and commercially reasonable practices, NetApp has implemented and maintains a comprehensive disaster recovery plan encompassing backup, security, and business continuity measures. This plan ensures that NetApp can continue providing Cloud Services, Professional Services, and Support Services or swiftly

resume their provision in the event of a disaster or any other significant occurrence that might otherwise disrupt NetApp's operations. NetApp has documented these measures and can furnish a summary of the plan to the Customer upon request.

8. SECURITY INCIDENTS

8.1 Incident Response. NetApp maintains an incident response plan and a dedicated team responsible for assessing, responding to, containing, and remedying identified security issues, irrespective of their nature (e.g., physical, cyber, product-related). The incident response plan is subject to annual review and updates to address emerging risks and incorporate lessons learned.

8.2 Incident Notification and Remediation. 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, and unless prohibited by law or instructed by a law enforcement or supervisory authority, NetApp will promptly and without undue delay: (a) notify that impacted Customer about the Security Incident; (b) conduct a thorough investigation of the Security Incident and provide any impacted Customer with relevant information and facts concerning the Incident; (c) take reasonable measures to mitigate the effects of the Security Incident and keep any impacted Customer reasonably informed about NetApp's investigation and remediation efforts, to the extent allowed by applicable law and any confidentiality obligations; and (d) if the Security Incident reveals any deficiencies, weaknesses, or areas of non-compliance, promptly take appropriate steps, at NetApp's reasonable discretion, to address significant deficiencies, weaknesses, and areas of non-compliance as soon as practicable given the circumstances. Impacted Customers must notify NetApp promptly about any possible misuse of its accounts or authentication credential of which it becomes aware. Upon request, NetApp will furnish information regarding the status of any required remedial actions, including an estimated timetable for completion. NetApp will also provide certification, as soon as practicable given the circumstances, stating that all necessary remedial actions have been duly completed. If an impacted Customer faces legal action from a third party related to a Security Incident, NetApp agrees to cooperate and provide reasonable assistance to help that Customer handle such legal proceedings effectively. If a Security Incident involves Customer Content and necessitates compliance with data breach notification laws, NetApp will offer reasonable assistance to an impacted Customer. This assistance may include aiding in the fulfillment of obligations under applicable data breach notification laws, such as notifying the relevant supervisory authority and providing a comprehensive description of the Security Incident.