NetApp, Inc. (NetApp)
Data Protection
Binding Corporate Rules (BCRs)

NetApp obtained approval from its Lead Supervisory Authority for its Binding Corporate Rules in 2015. These Binding Corporate Rules were updated in 2019 to address the changing technology landscape and transformative business practices. This resulted in the creation of Binding Corporate Rules for its role as a Data Controller (p. 2-24) and Binding Corporate Rules for its role as a Data Processor (p.24-47). The updated Binding Corporate Rules were submitted to the Lead Supervisory Authority in April 2019 are awaiting review and approval at the time of this publication.

NetApp operates under these updated Binding Corporate Rules while it awaits the review and approval of the Lead Supervisory Authority.

NetApp, Inc. (NetApp)
Data Protection
Binding Corporate Rules (BCRs)
For Controller Activities

TABLE OF CONTENTS

1 INTRODUCTION

These NetApp, Inc. (NetApp) Data Protection Binding Corporate Rules (BCRs) for Controller Activities (these "**BCRs**") define NetApp's policy and standards in regards to NetApp's activities as a controller of Personal Data. These BCRs are binding for all NetApp Group Companies and will be communicated to all NetApp employees and applicable contingent workers on our internal legal website and published on the external NetApp website at www.netapp.com, together with a list of the NetApp Group Companies.

For avoidance of doubt, these BCRs apply only to NetApp's activities as a data controller. For the BCRs applicable to NetApp's activities as a data processor, refer to the NetApp, Inc. Data Protection Binding Corporate Rules for Processor Activities (Processor BCRs).

1.1 Introduction to BCRs

These BCRs define our approach to, and framework for, compliance with our obligations as a data controller. We believe that appropriate privacy protection is a business enabler, not a barrier. Privacy protection can be a means to develop employee and customer confidence and trust and to develop lasting and positive employment and business relationships.

All NetApp companies, employees, and applicable contingent workers must comply with these BCRs in connection with the collection, processing, storing, sharing and/or transferring of any Personal Data as a data controller. All NetApp Group Companies (as defined in Article 3) are obligated to respect and comply with these BCRs.

The BCRs apply to all Personal Data of NetApp employees, customers, clients, suppliers, partners, prospects, and any other data subjects whose Personal Data is collected and used by NetApp as a data controller.

1.2 What are BCRs?

In regards to data protection, BCRs are a tool to protect the privacy of a data subject's Personal Data while facilitating international global transfers of Personal Data within corporate groups. BCRs allow companies to transfer Personal Data from the EEA around the world using a single set of rules. This gives data subjects the confidence that their personal data is being processed using a binding and enforceable set of standards. BCRs can facilitate data flows for companies, reduce their uncertainty about compliance, and increase the confidence of data subjects.

1.3 Binding Nature of BCRs

NetApp BCRs are made binding upon all NetApp Group Companies based on unilateral declarations or undertakings made or given by the NetApp's parent company, which are binding on the other Group Companies.

These Binding Corporate Rules (BCRS) are binding for all NetApp Group Companies. All NetApp Group Companies, employees, and applicable contingent workers have a clear duty to comply with and respect our BCRs. Internally, within the NetApp Group Companies, the requirements for handling personal data are made binding through the implementation of various measures which may include:

- The BCRs
- Unilateral declarations by NetApp's Board of Directors (the "**Board**") that bind all NetApp Group Companies
- Data privacy-specific non-disclosure agreements (NDAs)
- Global data privacy policies

Employees are bound by the BCRs through various measures which may include:

- The BCRs
- Data privacy-specific NDAs
- Works Council Agreements
- Employee Code of Conduct with sanctions
- Internal policies with sanctions

1.4 Contact Information

Any questions regarding these BCRs, your rights under the BCRs, or any other privacy related questions can be directed to NetApp's Integrity and Compliance Office at the following addresses:

ng-privacy@netapp.com

NetApp, Inc.

c/o Legal Department

Attn: Global Chief Privacy Officer

1395 Crossman Avenue

Sunnyvale, CA 94089, USA

1.5 What are Privacy Laws?

Data Privacy Laws (also known as Data Protection Laws) govern how Personal Data is used, who can access it, and when and if it can be shared with a third party. The laws also define how organizations must manage and protect Personal Data, as well as the restrictions regarding the transfer of any Personal Data outside of the country of origination.

1.6 How Do Privacy Laws Impact NetApp Globally?

NetApp, Inc. and its subsidiaries transfer Personal Data internally, and to approved NetApp partners or vendors, for a variety of legitimate reasons connected to the functional, technical, and operational requirements of the global business.

For instance, employee Personal Data may be transferred for the administration of employee payroll, benefits, stock program, internal education and development programs, finance activities (e.g., expense processing, corporate credit card management), or the corporate travel program. Customer Personal Data may be transferred to provide product support, technical services, warranty and maintenance renewals, product upgrades, and relevant events of interest to our customers. Prospective customer Personal Data may be collected and transferred to provide relevant information regarding NetApp products, services, and events to interested parties.

All transfers of Personal Data are done with appropriate levels of security (taking into account the state of the art; the costs of implementation; and the nature, scope, context, and purposes of processing, as well as the risk, likelihood and severity of harm to the rights and freedoms of the data subjects) and, when required by law, with the explicit consent of the data subjects.

1.7 How Does NetApp Address Compliance with Privacy Laws?

Adherence to Data Privacy Laws and the respect for privacy are fundamental to NetApp's culture and help us maintain an environment where data subjects can trust us and our technology and feel safe that their data is protected from unauthorized access, use, or loss. Our BCRs are designed to provide a high level of protection for all Personal Data collected and processed by NetApp. The BCRs apply in all cases where NetApp collects, processes, uses, stores, shares, and/or transfers Personal Data as a data controller, whether online or offline, or by manual or automatic means.

1.8 Responsibility for Compliance

NetApp's Global Chief Privacy Officer (GCPO) is responsible for overseeing and ensuring compliance with the BCRs and establishing the global framework for data privacy compliance. The GCPO, through members of the Integrity and Compliance Office monitors compliance with the BCRs and privacy laws on a day-to-day basis. The GCPO is responsible for monitoring compliance globally and for ensuring that any changes to the BCRs are communicated within NetApp operations worldwide. The GCPO advises the Board of Directors and Audit Committee, deals with Data Protection Authorities' investigations, coordinates with the Internal Audit Department to provide reporting on compliance with the BCRs annually, ensures compliance at a global level, and manages and coordinates with the Global Data Privacy Governance Council to ensure compliance with the BCRs. The Integrity and Compliance Office is responsible for handling local complaints from data subjects, reporting major privacy issues to the GCPO, and ensuring compliance at a local level.

These BCRs bind NetApp and our Group Companies to comply with the BCRs when Personal Data is collected, processed, used, and/or transferred outside of the EEA.

1.9 Responsibility for Data Privacy Training

All NetApp employees who have access to any Personal Data, are involved in the collection of Personal Data, or who are involved in the development of products, services, or tools used to process Personal Data are required to complete the NetApp internal data privacy training course, and such other training as may be designated by the GCPO. NetApp provides various levels of training depending on the amount and type of data collected, accessed, processed, stored, shared, and/or transferred. NetApp's training program consists of online data privacy training courses, virtual and/or live data privacy classes, and data privacy videos that are short training overviews related to specific data privacy-related compliance obligations. All privacy training courses for NetApp employees with regular access to Personal Data, who are involved in the collection of Personal Data or in the development of tools used to process Personal Data, will include appropriate training on our BCRs.

2 DATA PRIVACY BINDING CORPORATE RULES

2.1 Compliance with the Privacy Laws

Nothing in these BCRs will be construed to take away any rights and remedies that individuals may have under applicable local law. These BCRs provides supplemental rights and remedies to individuals only.

In addition, where a Group Company has reasons to believe that the national legislation applicable to that Group Company prevents the company from fulfilling its obligations under the BCRs and has substantial effect on the guarantees provided by the BCRs, the Group Company will promptly inform the EU headquarters and the GCPO. The GCPO will make a responsible decision on what action to take and will consult with the competent Data Protection Authorities in case of doubt.

2.2 Transparency

NetApp will post these BCRs on its external corporate website and its internal Company intranet, and a copy of these BCRs can also be obtained by requesting a copy at privacy@netapp.com.

NetApp will notify data subjects in accordance with applicable Data Protection Law and consistent with Article 13 of GDPR regarding the processing of their Personal Data, including regarding why their personal data needs to be collected and the purposes for which their personal data will be processed, as well as their rights with respect to such processing.

If NetApp receives a request from a law enforcement authority or state security body ("**Requesting Authority**") for disclosure of Personal Data covered by these BCRs, it will first assess on a case-by-case basis whether this request is legally valid and binding on NetApp. If NetApp determines the request is not legally valid and binding on NetApp, NetApp will resist the request in accordance with applicable law. If NetApp determines the request is legally binding and valid, NetApp will promptly notify the competent DPA and will request the Requesting Authority to place the rest on hold pending this notification. If suspension and/or notification of this request is prohibited, such as in case of a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, NetApp will request that the Requesting Authority waive this prohibition and will document that it has made this request. In any event, NetApp will on an annual basis provide to the competent DPA general information on the number and type of such requests it received in the preceding 12-month period, to the fullest extent permitted by applicable law.

2.3 Use of Personal Data

NetApp will only collect, process, use, store, share, and/or transfer Personal Data for legitimate business purposes and in accordance with these BCRs.

If NetApp changes the purpose for which Personal Data is used, NetApp will make data subjects aware of the changes, unless the changes are within the data subject's expectations, and they can express their concerns, or unless there is a legitimate legal basis for not doing so. If NetApp changes the purpose for which the Personal Data is used, NetApp will not process the data in a way that is incompatible with the purposes for which they have been collected. If, however, NetApp must process the data for purposes that are incompatible, consent of the data subjects will be obtained where required by

applicable law. In seeking any such consent, NetApp will identify and clearly explain the purposes for which Personal Data will be used and who will have access to it.

NetApp may use automated tools to make decisions about data subjects, but decisions with a significant negative outcome for the data subject will not be based solely on the results provided by the automated tool. However, this restriction does not apply if (i) the use of automated tools is necessary for the performance of a task carried out to comply with a legal obligation to which NetApp is subject; (ii) the decision is made by NetApp for purposes of (a) entering into or performing a contract; or (b) managing the contract, provided the underlying request leading to a decision by NetApp was made by the data subject or suitable measures are taken to safeguard the legitimate interests of the data subject (e.g., the data subject has been provided with an opportunity to express his or her point of view).

2.4 Data Integrity and Quality

NetApp will only collect, process, use, store, share, and/or transfer Personal Data that is relevant and not excessive for the purpose. NetApp will take appropriate measures to keep personal information accurate and up to date for the intended purpose.

NetApp provides data subjects with a choice of methods to access and amend Personal Data and communication preferences, including online, in writing, or by contacting the appropriate internal NetApp contact.

NetApp collects, processes, and uses the minimum amount of Personal Data necessary to achieve a valid purpose. We retain Personal Data only for as long as it is necessary to meet the applicable purposes of processing or as required by or advisable in light of other legal requirements. We maintain a record of our processing activities in accordance with applicable legal requirements and make such information available to the supervisory authority on request, consistent with applicable law.

2.5 Data Security

NetApp has implemented appropriate technical and organizational security measures to protect all Personal Data, taking into account the state of the art; the costs of implementation; and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of the data subjects. Where NetApp companies process Personal Data on behalf of other NetApp companies, those companies will adhere to the BCRs and act only on the instructions of the NetApp Company on whose behalf the processing is carried out, as set forth in a contract entered into pursuant to Article 2.8. Where a third-party provider processes Personal Data on behalf of NetApp or a NetApp Group Company, the third-party provider will be required, through a binding contract entered into pursuant to Article 2.8, to adhere to obligations consistent with our BCRs and act only on the instructions of the NetApp Group Company on whose behalf the processing is carried out.

In the event of a breach of the security of Personal Data, NetApp will document information concerning the breach of security, including the facts relating to the breach of security, its effects, and the remedial actions taken, which documentation will be made available to the supervisory authority upon request. NetApp will provide any notification required by applicable law to the competent supervisory authority and to affected data subjects. NetApp will provide such notifications without undue delay following its determination that such a breach has occurred, unless otherwise prohibited (such as if a law enforcement official or a supervisory authority determines that notification would

impede a (criminal) investigation or cause damage to national security or the trust in the relevant industry sector). In that case, notification shall be delayed as instructed by such law enforcement official or supervisory authority. NetApp will respond promptly to inquiries of data subjects related to a breach of security of Personal Data.

2.6 Data Subject's Rights

NetApp will respond in a timely manner to inquiries or requests made by EU data subjects covered by these BCRs about their Personal Data. NetApp will reply to requests to access, rectify, delete, block, suppress, or cease processing Personal Data.

A data subject whose Personal Data is collected and used by NetApp may write to NetApp to ask for a copy of the Personal Data, including electronic and paper records, about them held by NetApp. If the Personal Data is inaccurate, the data subject may ask for that data to be corrected, deleted, or blocked and, in certain circumstances may object to the processing of their Personal Data, if allowable by applicable data privacy laws. NetApp will consider such requests and deal with them as appropriate.

Personal data covered by an access request may include Personal Data about the data subject that NetApp collects and uses, including a description of the Personal Data, the purposes for which the data is used, a description of transfers of that Personal Data to others, and the source of the Personal Data held by NetApp. A data subject making an access request can do so using the contact information set forth in Article 1.4 of the BCRs.

Data subjects can also contact the NetApp Integrity and Compliance Office, which in turn will direct privacy-related enquiries to the GCPO.

NetApp will respond to the request within one month of the date the GCPO receives the request. If the request requires additional time for response, NetApp will provide the data subject with an estimate (not to exceed a total of three months after receipt) of when a response will be provided.

2.7 Transfer of Personal Data Between NetApp Group Companies

NetApp processes and transfers Personal Data relating to the following categories of data subjects:

- NetApp employees, former employees, dependents and beneficiaries of employees, and prospective employees in connection with their working relationships or application for employment ("**Employment Data**");
- Our partners, customers, and our end-users in connection with the sale of products, provision of services, and financial transactions ("**Customer Data**"); provided that "Customer Data" does not include data we process as a data processor on behalf of a client or customer, which is governed instead by our Processor BCRs;
- Our prospects and leads who have expressed interest in obtaining information related to NetApp products, services, and events ("**Marketing Prospect Data**");
- Other persons as appropriate to conduct business, such as suppliers, partners, contractors, and contingent workers.

The processing and transfers undertaken by NetApp relating to the types of data subjects discussed above include processing for the following business purposes:

- Employee recruitment;

- Employee performance management and professional development;
- Payroll and administration of employee benefits;
- Research and development;
- Business development;
- Maintaining and building upon customer relationships;
- Business planning;
- Facilities management;
- Maintaining technology infrastructure and support;
- Database management;
- Training;
- Maintaining the security of data collected and processed;
- Fulfilling a transaction initiated by or involving a data subject;
- Fulfilling a transaction with or for our clients;
- Providing the data to agents and contractors to assist us in our business, some of which may be located outside of the collection country;
- As authorized by applicable laws;
- Fraud prevention or investigation, or other risk management purposes;
- For identification and information verification purposes;
- For protecting NetApp's legal rights or assets;
- Facilitating the acquisition of NetApp businesses;
- Enforcing our rights or the rights of other persons in a financial transaction;
- In response to a lawful request from a court or government agency or to otherwise comply with applicable law or compulsory process;
- On the written request of the data subject, where appropriate;
- In emergencies where the health or safety of a person is endangered; and
- Other purposes required or permitted by law or regulation.

NetApp processes and transfers a broad range of Personal Data between NetApp entities and third parties. Third-party transfers occur when a third party on behalf of NetApp provides services for which there is a legitimate business need. These services include benefits management, insurance providers, travel services, pension plan management, stock administration, and financial services. All third-party providers are vetted to ensure compliance with all applicable Data Protection Laws and are required to enter into appropriate contractual obligations consistent with these BCRs as described in Article 2.8.

The types of Personal Data processes and transfers include:

- Recruitment Data: This includes data related to job applicants and candidates, such as name, contact information, employment and job history, CV details, and other information provided during the application process.
- Employment Data: This includes data relating to health records, benefit information staff development records, attendance records including any days off due to illness, salary remuneration and expenses information, expatriate information, equal opportunities management, grievance and disciplinary procedures, employee share equity holdings, employment termination information, names, addresses, date of birth, work location, employee performance, trade union membership, and next of kin.
- Customer/Prospect Information: This includes the contact information of employees, customers and prospective customers; information relating to the client's account, clients' customers' contact details including name, address, and telephone numbers; and account information including other persons on the account and spend thresholds, details of clients' customers' spending and

spending patterns and details of the merchants accepting payment transactions to the extent these are individuals.

- Other Personal Data: NetApp also processes contact information of the employees of its suppliers and vendors and independent contractors including name, e-mail address, work location and telephone numbers and such other Personal Data as may be required in order for NetApp to conduct business with such suppliers, vendors, and independent contractors.

2.8 Protecting Data Transfers to Third Parties and Internal Processors

NetApp will ensure that any Personal Data transferred to third parties located within or outside of the EEA is adequately protected and processed in accordance with applicable Data Protection Laws.

Transfers of Personal Data to third parties outside of NetApp or outside of the EEA are not allowed without appropriate steps being taken to ensure there is a legal basis for the transfer and to protect the Personal Data being transferred. All transfers of Personal Data to external controllers or processors located in a country not considered to provide an adequate level of protection by the European Commission will respect the applicable EEA requirements concerning such data transfers. For example, NetApp makes use of the EU Standard Contractual Clauses approved by the EU Commission or will use other adequate contractual means in accordance with GDPR, as appropriate.

If a third-party service provider processes Personal Data on behalf of NetApp, either within the EEA or outside of the EEA, NetApp will enter into a contract with that provider which requires the third-party service provider to process the Personal Data only on NetApp's documented instructions; keep the Personal Data confidential and impose confidentiality obligations on personnel with access to the Personal Data; adopt and maintain technical and organizational security measures to safeguard the Personal Data and promptly inform NetApp of any personal data breach affecting the Personal Data; only permit subcontractors to Process Personal Data in connection with its obligations to NetApp and as authorized by its contract with NetApp; and, upon termination of the services, return or delete the Personal Data in accordance with the contract.

If a Group Company processes Personal Data as a data processor on behalf of another Group Company, the Group Company acting as the data processor must have a validly entered into written or electronic contract with the Group Company acting as the data controller of the relevant Personal Data, which contract must in any event include types of provisions required for third-party service providers as set forth above.

2.9 Protecting and Limiting Use of Sensitive Data

Except as otherwise permitted by applicable law, NetApp will not process sensitive data unless:
- The data subject has given his explicit consent to the processing of those sensitive data, where the applicable laws require and permit such consent; or
- The processing is necessary for the purposes of carrying out the obligations and specific rights of NetApp in the field of employment law in so far as it is authorized by EU or EEA national law providing for adequate safeguards; or
- The processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

- The processing relates to sensitive data which are manifestly made public by the data subject; or
- The processing of sensitive data is necessary for the establishment, exercise or defense of legal claims by or pertaining to NetApp; or
- The processing of the sensitive data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment, or the management of health-care services, and where those sensitive data are processed by a health professional under EU or EEA national law or rules established by EU or EEA national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy; or
-The processing is necessary for complying with a legal obligation.

"**Sensitive data**" is defined as any information related to a data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying the data subject, data concerning health, sex life or sexual orientation, and criminal convictions.

2.10 Use of Personal Data for Sales and Marketing

NetApp will use Personal Data for direct marketing or sales to a consumer only if the consumer has agreed to that use or as otherwise permitted by applicable law. NetApp will give all data subjects the opportunity to opt out, free of charge, from receiving direct marketing or sales communications from NetApp, and will respect all opt out requests received. The opt-out option will be clearly visible in the marketing communication.

NetApp will provide data subjects with a choice of methods to access and amend Personal Data and communication preferences for direct marketing and sales.

2.11 Privacy by Design and Data Protection Impact Assessments

NetApp will require the completion of a privacy-by-design assessment whenever a new system or application is proposed that will impact Personal Data of any kind. The privacy-by-design assessment will help determine the type of Personal Data that will be collected, used, and processed; the purpose of the processing; access rights to the Personal Data, data storage and/or transfer; and the relevant data privacy laws that may be impacted. By using this assessment, NetApp can anticipate any potential data privacy issues and ensure compliance with all relevant data privacy laws before the start of any new project.

Where the processing is likely to result in a high risk for the rights and freedoms of data subjects, in particular where new technologies are used, NetApp also will carry out a data protection impact assessment (DPIA) in accordance with applicable legal requirements. If the DPIA indicates that the processing would result in a high risk in the absence of measures significantly affecting these BCRs (e.g., changes to their binding character), NetApp will communicate this to the competent supervisory authority.

2.12 Compliance Audits

NetApp's collection and use of Personal Data are subject to detailed oversight and evaluation through the audit process and on an on-going basis.

NetApp will perform regular audits of compliance to these BCRs in accordance with Appendix 1. NetApp will ensure these audits address all applicable aspects of the BCRs,

including NetApp's information technology systems and databases, security policies, contractual provisions, training, privacy policies, and guidelines.

NetApp will ensure that any issues or instances of non-compliance with the BCRs identified by NetApp's Internal Audit Department (IA) are brought to the attention of the GCPO and NetApp's senior company management and that appropriate corrective actions are taken to ensure compliance.

NetApp will conduct audits of compliance with the BCRs every 12-24 months, the exact frequency to be determined based on the circumstances, along with ad hoc audits at the request of the GCPO or a relevant DPA. IA will coordinate, manage, and provide quality assurance of audit work performed by internal or external auditors.

For further detailed information please refer to Appendix 1 – Audit Protocols

2.13 Interaction and Cooperation with Data Protection Authorities

NetApp will provide copies of the results of any audit of the BCRs to any EEA DPA of competent jurisdiction, upon request, subject to relevant law. The DPA will respect the confidentiality of the information provided and any trade secrets contained in the information. NetApp's GCPO will be responsible for liaising with the EEA DPAs for this purpose.

Where any NetApp Group Company subject to the BCRs is located within the jurisdiction of a DPA based in the EEA, NetApp agrees that the DPA may audit that NetApp Company for the purpose of reviewing compliance with the BCRs.

Any audit by a DPA will be carried out in accordance with the applicable law of the country in which the NetApp Company is located. In the case of a NetApp Group Company located outside of the EEA, the audit will be carried out in accordance with the applicable law of the EEA country from which the Personal Data is transferred under the BCRs.

NetApp companies will co-operate and assist each other and the NetApp GCPO when hosting audits by EU or EEA national DPAs. Where required, NetApp will make the necessary personnel available for dialogue with an EEA DPA in relation to the audit reviewing compliance with the BCRs. Audits will be conducted with full respect to the confidentiality of the information obtained and to the trade secrets of NetApp. NetApp's GCPO will also be responsible for liaising with the EU DPA for this purpose.

For additional information please refer to Appendix 4 – Co-Operation Procedure

2.14 Complaint Management

If a data subject, whose Personal Data is collected and used by NetApp, believes NetApp has not complied with the NetApp BCRs, that data subject may submit a complaint in accordance with the process detailed in Appendix 2 – Procedure for Complaint Handling and Resolution.

2.15 Enforcement and Liability

If NetApp violates these BCRs with respect to the Personal Data of a data subject covered by these BCRs, the data subject can as a third-party beneficiary enforce against

NetApp Holding BV any claim as a result of a breach of the obligations set forth in Article 2. These BCRs are governed by and interpreted in accordance with Dutch law. Any supplemental rights or remedies granted to any data subject under the BCRs are enforceable as follows:

Any data subject may report a suspected violation of the BCRs directly to the Dutch DPA or other competent DPA or to the courts in (i) the country of his/her habitual residence, place of work, or place where the infringement took place; or (ii) the Netherlands, against NetApp Holding BV.

If a data subject has a claim for violation of the BCRs related to processing that is governed by EU Data Protection Laws, the data subject shall be entitled to recover damages suffered by the data subject resulting from the violation of these BCRs to the extent provided by applicable EU Data Protection Laws. In the event of such a claim, the data subject will need to demonstrate that he or she has suffered the alleged damages and to establish facts which show it is plausible that the damage resulted from a violation of these BCRs. If the data subject demonstrates such damages, NetApp will be liable for such damages consistent with these BCRs, unless NetApp can demonstrate that the damages suffered by the individual due to a violation of these BCRs are not attributable to NetApp.

If a NetApp Group Company outside of the EU violates the BCRs, the courts or other competent authorities in the EU have jurisdiction to enforce action against NetApp Holding BV. The data subject has the rights and remedies against NetApp Holding BV as if the violation had taken place by it in the member state in which it is based instead of the Group Company outside the EU.

NetApp's EU headquarters, NetApp Holding & Manufacturing B.V located in the Netherlands (NetApp Holding BV), accepts responsibility for and agrees to take the necessary action to remedy the acts of other members linked by these BCRs outside of the EU and to pay damages resulting from the violation of these BCRs by such members of these BCRs, in accordance with this Article 2.15.

2.16 BCR Updates

NetApp will inform the lead DPA of any material changes to the BCRs as provided below. NetApp will provide that information at least once a year of the changes being made. NetApp's GCPO is responsible for communicating changes and providing a brief explanation of the reasons for any notified changes to the BCRs.

The NetApp GCPO will maintain an up-to-date list of the NetApp companies bound by the BCRs. NetApp will send an up-to-date list of companies to the relevant DPAs at least once a year.

NetApp will communicate the amended BCRs to the NetApp companies bound by the BCRs and will publish the amended BCRs on NetApp's internal and external websites.

NetApp will ensure that any new NetApp companies are considered for inclusion in the list of NetApp companies bound by the BCRs. NetApp will also ensure that any new NetApp Group Company has implemented the BCRs before a transfer of Personal Data to or from the new NetApp Group Company takes place.

For additional information please see Appendix 5 - BCRs Update Procedures

3 Definitions

"**Data Protection Law**" means the provisions of mandatory law of an EEA Country containing rules for the protection of individuals with regard to the processing of Personal Data, including security requirements for and the free movement of such Personal Information.

"**Group Companies**" means NetApp, Inc. and any wholly owned direct or indirect subsidiary of NetApp, Inc. that processes Personal Data.

"Personal Data" means personal data (as defined in GDPR) that is subject to EU Data Protection Law (or was subject to EU Data Protection Law prior to the transfer of such personal information to a Group Company outside of the EEA).

APPENDIX 1 – AUDIT PROTOCOLS

1 BACKGROUND

The purpose of the NetApp Binding Corporate Rules for Controller Activities (BCRs) is to establish NetApp's approach to compliance with privacy/data protection laws. This document defines how NetApp's compliance to the BCRs will be audited.

The NetApp Integrity and Compliance Office, and specifically the GCPO, provides guidance about the collection and use of Personal Data subject to the BCRs and analyzes Personal Data collection and use for potential privacy-related risks. The collection and use of Personal Data that could pose significant privacy impacts are subject to detailed oversight and evaluation during the audit and on an on-going basis.

2 APPROACH

2.1 Scope of Audit

NetApp will perform regular audits of compliance to the BCRs. NetApp will ensure these audits address all aspects of the BCRs, including methods of ensuring that any necessary corrective actions are taken.

NetApp will ensure that any issues or areas that do not comply with the BCRs that are discovered through our audits are immediately brought to the attention of NetApp's GCPO and NetApp senior executive management and that appropriate corrective actions are taken to ensure compliance.

2.2 Audit Timeframes

NetApp will conduct regular annual audits for compliance with the rules through our standard data privacy assessment and evaluation process. NetApp will conduct the audits of compliance with the BCRs in accordance with Article 2.12.

2.3 Auditors

IA is responsible for undertaking all compliance audits to the BCRs. IA will coordinate and engage with external auditors as needed and will manage and provide quality assurance of all audit work performed.

2.4 Audit Reports for EEA DPAs

NetApp will provide copies of the results of any audit of these BCRs to any EEA DPA of competent jurisdiction upon request, subject to applicable law. The DPA must respect the confidentiality of the information provided in the audit report and protect the confidentiality of any intellectual property or trade secrets that may be contained within the report. NetApp's GCPO is responsible for liaising with the EEA DPAs for this purpose.

2.5 EEA DPA Audits

Where any NetApp Group Company subject to the BCRs is located within the jurisdiction of a DPA based in the EEA, NetApp agrees that the DPA in that

jurisdiction may audit that NetApp Group Company for the purpose of reviewing compliance with the rules.

Any audit by a DPA will be conducted in accordance with the applicable law of the country in which the NetApp Group Company is located. If the NetApp Group Company is located outside of the EEA, the audit will be conducted in accordance with the applicable law of the EEA country from which the Personal Data is transferred under the BCRs. The lead DPA shall be informed and/or involved with the audits depending on the nature and/or the outcome of the audit.

NetApp companies will co-operate and assist each other and our GCPO when hosting audits by EU or EEA national DPAs. If required, NetApp will make the necessary personnel available for discussion with an EEA DPA in relation to the compliance audit to the rules. Audits will be conducted with full respect to the confidentiality of the information obtained and to the intellectual property and trade secrets of NetApp. NetApp's GCPO will also be responsible for liaising with the EEA DPA for this purpose.

APPENDIX 2 – PROCEDURE FOR COMPLAINT HANDLING AND RESOLUTION

1 BACKGROUND

The purpose of the NetApp Binding Corporate Rules for Controller Activities (BCRs) is to define and establish NetApp's approach to compliance with privacy/data protection laws. This appendix to our BCRs provides an overview of the steps NetApp takes when responding to complaints from individuals regarding NetApp's collection and processing of their Personal Data.

If an individual whose Personal Data is collected and processed by NetApp believes NetApp has not complied with our BCRs, that individual may raise the matter with NetApp's GCPO. The individual may also raise the matter with the relevant EU or EEA national data protection authority.

In addition, an individual whose Personal Data is collected and processed by NetApp in the EEA and transferred outside of the EEA may also make a claim against NetApp in accordance with Article 2.15 above.

Individuals entitled to these rights will be notified accordingly as part of the complaints-handling procedure described below.

2 APPROACH

2.1 Making a Complaint

An individual can bring a complaint by using the contact information set forth in Article 1.4 of the BCRs.

Individuals can also contact the NetApp Integrity and Compliance Office that, in turn, will direct privacy-related enquiries to the GCPO in a timely manner.

2.2 NetApp's Response

NetApp's Integrity and Compliance Office, and specifically the GCPO, is responsible for responding to any complaints, working closely with colleagues from the appropriate NetApp business groups and NetApp companies. NetApp will acknowledge receipt of a complaint within five working days of the complaint being received by NetApp's worldwide Data Governance Office. NetApp will use reasonable efforts to resolve complaints without undue delay and to respond to a complaint within 30 calendar days of the date the complaint is received by the Integrity and Compliance Office.

If the complaint is too complex to allow a response within one month, NetApp will provide the individual with an estimate (not exceeding a total of three months after receipt) of when a response will be provided. The complaint is considered closed on the date NetApp communicates its response to the complaint to the individual.

If a data subject whose information is collected and used by NetApp in the EEA and transferred to NetApp companies outside the EEA is not satisfied with the way a complaint has been handled, the data subject has the right to complain to an EEA DPA. The data subject may also lodge a claim with a court of competent jurisdiction in accordance with Article 2.15 of this BCR. Data subjects entitled to

such rights will be notified accordingly as part of the complaints handling procedure.

APPENDIX 3 – PROCEDURE FOR PERSONAL DATA ACCESS REQUEST

1 BACKGROUND

The purpose of the NetApp Binding Corporate Rules for Controller Activities (BCRs) is to define and establish NetApp's approach to compliance with privacy/data protection laws. This appendix to our BCRs provides an overview of the steps individuals can take to ask for a copy of the information NetApp holds on them.

Any individual whose Personal Data is collected and processed by NetApp may write to NetApp and request a copy of the Personal Data, including electronic and paper records, about them held by NetApp, to the extent provided by applicable law. This is referred to as a "Request." If the Personal Data is determined by the individual to be inaccurate, the individual may ask NetApp to correct, delete or block the Personal Data. In certain circumstances, the individual may object to the processing of their Personal Data. NetApp will consider all Requests and deal with them as appropriate and in compliance with our BCRs.

This appendix defines the procedure NetApp will follow when we receive a Request.

2 APPROACH

2.1 Scope of Requests

NetApp will respond to all individuals who make any type of Requests, whether made formally or informally, and whether or not they specifically mention data privacy/protection laws. Personal data covered by a Request may include, to the extent provided by applicable law, the Personal Data about the individual that NetApp collects and processes, including a description of the Personal Data, the purposes for which the data is used, and a description of any transfers of the Personal Data to others, both internal and external to NetApp. The right of access includes the right to know the source of the Personal Data held by NetApp, where provided by applicable law.

2.2 Making a Request

An individual who would like to make a Request can do so using the contact information set forth in Article 1.4 of the BCRs.

Any individual making a Request is required to confirm their identity and to confirm that they are only requesting their own Personal Data and not that of another person. Requests can be made at reasonable intervals, but not to exceed once per year unless there is a legal justification for asking more often. NetApp may require a small fee for Requests, but only if allowed by local law.

2.3 NetApp's Response to a Request

NetApp will make every reasonable effort to acknowledge receipt of a Request within five working days of the Request being received by NetApp's GCPO.

NetApp will explain to all individuals making a Request that it will be necessary to confirm their identity and require more detailed information in an effort to locate the requested Personal Data and to ensure that the individual requesting the data is the individual to which the data relates. NetApp will clearly articulate that attempting to obtain Personal Data about another person may be a violation of the law.

If the Request is ambiguous, unclear, imprecise, or unreasonable, NetApp will require the individual to provide clarity regarding the Personal Data they are requesting and where they expect this data to be found (if they know). NetApp will reply within 30 calendar days of the date the Request is clearly understood by NetApp. If the Request is too complex to allow a response within 30 calendar days, NetApp will inform the individual and provide a reasonable estimate as to when a response will be provided.

Exemptions and restrictions

NetApp may decline to grant the request in the following circumstances (which therefore operate as an exemption to the duty to respond to a request):

(a) The exemption constitutes a necessary measure to safeguard national security, defense, or public security;

(b) The exemption is for the prevention, investigation, detection, and prosecution of criminal offences or of breaches of ethics for regulated professions;

(c) The exemption is for the protection of the rights and freedoms of others; or

(d) The exemption is otherwise provided by applicable law.

A Request will be considered closed on the date the individual making the Request is provided with the data or is informed that that an exemption applies.

2.4 **Dispute of a Response**

If an individual disputes a response from NetApp, the individual may notify NetApp that he/she does not agree with the response and/or raise the matter with the relevant EU or EEA national data protection authority. If the individual notifies NetApp that he/she does not agree with the response, the issue will be handled in accordance with this complaint handling process.

APPENDIX 4 – CO-OPERATION PROCEDURE

1 BACKGROUND

The purpose of the NetApp Binding Corporate Rules for Controller Activities (BCRs) is to define and establish NetApp's approach to compliance with privacy/data protection laws. This appendix describes how NetApp companies will co-operate with each other and with the EEA DPAs in regards to these BCRs.

The provision of any information under this Co-operation Procedure will be subject to applicable law. The DPAs will respect the confidentiality of any data and any confidential or proprietary information and any trade secrets that may be contained in the information.
This appendix defines the procedure NetApp will follow when we receive a Request.

2 APPROACH

2.1 Co-Operation between NetApp Companies

NetApp companies will co-operate and assist each other and the NetApp GCPO when handling requests or complaints regarding our BCRs from individuals or from any EU or EEA national DPA. NetApp companies will comply with any instructions from the Dutch DPA, Dutch courts, or any relevant EU or EEA national DPA requiring the remedy of a breach of the BCRs.

2.2 Co-Operation with the EEA DPAs

Whenever and wherever required, NetApp will make the appropriate personnel available for interaction with an EEA DPA in regards to our BCRs. NetApp will actively review and take every reasonable effort to comply with:

- Any decisions made by a relevant EEA DPA on any Data Protection Law issues that may impact the BCRs; and
- The views of the European Data Protection Board, as defined in its published guidelines on Binding Corporate Rules.

NetApp will comply with any formal decision of the applicable DPA on any issues related to the interpretation and application of our BCRs where a right to appeal is not exercised.

2.3 EEA DPA Audit

NetApp will, upon request by an EEA DPA of competent jurisdiction, provide that authority with a copy of the results of any audit of our BCRs under our Audit Protocols found in Appendix 1 of this document.

Where any NetApp Group Company subject to the BCRs is located within the jurisdiction of a DPA based in the EEA, NetApp agrees to that DPA audit the NetApp Group Company for the purpose of reviewing compliance with the BCRs.

Any audit by a DPA will be conducted in accordance with the applicable law of the country in which the NetApp Group Company is located. If a NetApp Group Company is located outside of the EEA, the audit will be conducted in

accordance with the applicable law of the EEA country from which the personal information is transferred under the BCRs.

Audits will be conducted with full respect to the confidentiality of the information obtained and to the confidential and proprietary information of NetApp and its trade secrets. NetApp's GCPO will be responsible for coordinating and interacting with the EEA DPAs for this purpose.

APPENDIX 5 – BCRs UPDATE PROCEDURE

1 BACKGROUND

The purpose of the NetApp Binding Corporate Rules for Controller Activities (BCRs) is to define and establish NetApp's approach to compliance with privacy/data protection laws. This appendix describes how NetApp will communicate changes to the BCRs to the EEA DPAs, NetApp companies, and to individuals.

2 APPROACH

2.1 Notifying the DPAs of Changes to NetApp's BCRs

NetApp will inform the Dutch Data Protection Commissioner and any other relevant EEA DPAs of any material changes to the BCRs in accordance with this Appendix 5. NetApp will provide the information within a reasonable time of the changes being made. NetApp's GCPO is responsible for communicating any changes to the BCRs, along with a brief explanation of the reasons for any changes to the BCRs. However, NetApp is not obligated to communicate any changes that are administrative in nature or which have occurred as a result of a change of applicable data protection law in any EEA country through any legislative, court, or supervisory authority measure unless they result in a substantial change to the BCRs or affect the authorization of the BCRs by EEA DPAs.

NetApp's GCPO will maintain an up-to-date list of the NetApp Group Companies bound by the BCRs. If a modification to the list of Group Companies may affect the level of protection offered by the BCRs or significantly affect the BCRs (i.e., changes to their binding nature), NetApp will promptly communicate this to the competent supervisory authority. Other changes to the list of Group Companies will be notified to the competent supervisory authority on a yearly basis.

2.2 Notifying NetApp Companies of Changes to the NetApp BCRs

NetApp will notify all NetApp companies bound by the BCRs of any amendments or changes made and will publish the amended BCRs on NetApp's internal and external websites. The external website is available at www.netapp.com.

2.3 Inclusion of New NetApp Companies

NetApp will ensure that any new NetApp Group Company is considered for inclusion in the list of NetApp companies bound by the BCRs. NetApp will also ensure that the necessary legal, administrative, operational, and technical measures are in place before a transfer of Personal Data to or from a new NetApp Group Company occurs.

NetApp, Inc. (NetApp)
Data Protection
Binding Corporate Rules (BCRs)
For Processor Activities

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

Introduction

NetApp provides enterprise customers with a range of hybrid cloud data services that simplify the management of applications and data across cloud and on-premises environments. In providing its services, NetApp may process or store data that includes personal information of individuals that its customers process in the course of performing their business activities. NetApp processes such personal information as a data processor on behalf of these customers.

The NetApp Code of Conduct expresses our commitment to conduct our business in accordance with high ethical standards and in accordance with applicable laws and NetApp policies, including with respect to the protection of personal information. These Data Protection Binding Corporate Rules (BCRs) for Processor Activities indicate how NetApp will implement this commitment with respect to processing of personal information on behalf of its customers.

For the BCRs applicable to the processing of customer data by NetApp in its role as a data controller, refer to the Data Protection Binding Corporate Rules (BCRs) for Controller Activities.

Capitalized terms have the meaning set out in Appendix 1 (Definitions).

1 Scope, Applicability, and Implementation

1.1 Scope; NetApp as Data Processor

These Data Protection Binding Corporate Rules (BCRs) for Processor Activities (**Processor BCRs**) address the Processing of Personal Information of Customer Individuals by NetApp in its role as a Data Processor in the course of delivering Customer Services, where such Personal Information is:

(i) subject to EEA Data Transfer Restrictions (or was subject to EEA Data Transfer Restrictions prior to the transfer of such Personal Information to a Group Company outside of the EEA); and

(ii) Processed by NetApp in a country outside the EEA; and

(iii) Processed pursuant to a Services Contract that specifically provides that these Processor BCRs shall apply to such Personal Information.

These Processor BCRs will also apply if the Services Contract specifically states that the Processor BCRs will also apply to types of transfers of Personal Information other than those specified above (hereafter, such Personal Information collectively, **Customer Individual Information or CI Information**).

1.2 Electronic and Paper-Based Processing

These Processor BCRs apply to the Processing of CI Information by NetApp by electronic means and in any systematically accessible paper-based filing systems.

1.3 Applicability of Local Law and the Processor BCRs

Nothing in these Processor BCRs will be construed to take away any rights and remedies that Customer Individuals may have under applicable local law. These Processor BCRs provide supplemental rights and remedies to Customer Individuals only.

1.4 Policies and Guidelines

NetApp may supplement these Processor BCRs through policies and guidelines that are consistent with these Processor BCRs.

1.5 Accountability

These Processor BCRs are binding on NetApp. NetApp Staff must comply with these Processor BCRs.

1.6 Effective Date

These Processor BCRs have been adopted by NetApp, Inc. and will enter into force as of [•] (Effective Date). The Processor BCRs and a list of the NetApp Group Companies that are covered by these Processor BCRs will be published on the NetApp Internet site, except that the description of the security measures may be replaced by a summary description and will be made available to Customer Individuals upon request.

1.7 Processor BCRs Supplement Prior Policies

These Processor BCRs supplement all NetApp privacy policies, guidelines and notices that exist on the Effective Date.

1.8 Implementation

These Processor BCRs shall be implemented within NetApp based on the timeframes specified in Article 15.

2 Services Contract

2.1 Services Contract

NetApp shall Process CI Information only on the basis of a validly entered into written or electronic agreement with a Customer (**Services Contract**) which complies with Applicable Data Processor Law.

The NetApp Contracting Entity may use Sub-Processors, both NetApp Sub-Processors and Third Party Sub-Processors, in the regular performance of Services Contracts. The standard Services Contract shall authorize the use of such Sub-Processors, provided that the NetApp Contracting Entity remains liable to the Customer for the performance of the contract by the Sub-Processors in accordance with the terms of the Services Contract. The provisions of Article 7 shall further govern use of Sub-Processors.

2.2 Termination of Services Contract

Upon termination of the Services Contract, NetApp shall fulfill its obligations to the Customer in the Services Contract with regard to return of CI Information by allowing Customer to delete or retrieve CI Information in NetApp's possession or control in accordance with the Services Contract. When NetApp's obligations under the Services Contract have been fulfilled, NetApp shall delete or otherwise render unrecoverable such CI Information as set forth in the Services Contract and (upon request of the Customer) confirm to Customer that NetApp has done so, except to the extent the Services Contract or applicable law provides otherwise. In that case, NetApp shall no longer

Process the CI Information, except to the extent otherwise specified by the Services Contract or as required by applicable law.

2.3 Audit of Termination Measures

Upon termination of the Services Contract, NetApp shall, at the request of the Customer, allow its Processing facilities to be audited in accordance with Article 10.2, 10.3 and 10.4 (as applicable) to verify that NetApp has complied with its termination-related obligations under Article 2.2.

3 Compliance Obligations of NetApp

3.1 Instructions of the Data Controller

NetApp shall Process CI Information only on behalf of the Customer and in accordance with any documented instructions received from the Customer consistent with the terms of the Services Contract or as needed to comply with applicable law.

3.2 Compliance with Applicable Law

NetApp shall Process CI Information only in accordance with the Applicable Data Processor Law and shall deal promptly and appropriately with Customer's requests for assistance as reasonably required to enable Customer's compliance with the Applicable Data Controller Law in accordance with the Services Contract, and NetApp shall inform Customer if it believes that any such instruction infringes Applicable Data Controller Law.

3.3 Notification of Non-compliance, Substantial Adverse Effect

If a Group Company:

(i) Determines that it is unable for any reason to comply with its obligations under Article 3.1 and 3.2 and NetApp cannot cure this inability to comply; or

(ii) Becomes aware of any circumstance or change in the Applicable Data Processor Law of a non-EEA country, or an instruction of the Customer, except with respect to the Mandatory Requirements, that is likely to have a substantial adverse effect on NetApp's ability to meet its obligations under Article 3.1, 3.2 or 10.3.

such Group Company shall promptly notify NetApp Holding BV and the Customer thereof, in which case the Customer will have the right to temporarily suspend the relevant transfer of CI Information under these Processor BCRs to NetApp until such time the Processing is adjusted in such a manner that the non-compliance is remedied. To the extent such adjustment is not possible, the Customer shall have the right to terminate the relevant part of the Processing by NetApp in accordance with the terms of the Services Contract.

3.4 Request for Disclosure of CI Information

If NetApp receives a request for disclosure of CI Information from a law enforcement authority or state security body (**Authority**), it will first assess on a case-by-case basis whether this request (**Disclosure Request**) is legally valid and binding on NetApp. Any Disclosure Request that is not legally valid and binding on Company will be resisted in accordance with applicable law.

Subject to the following paragraph, NetApp shall promptly inform the Customer (requesting the Customer to inform the Customer DPA), the Lead DPA, and the Customer DPA of any legally valid

and binding Disclosure Requests, and will request the Authority to put such Disclosure Requests on hold for a reasonable delay in order to enable the Lead DPA to issue an opinion on the validity of the relevant disclosure.

If suspension and/or notification of a Disclosure Request is prohibited, such as in case of a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, NetApp will request the Authority to waive this prohibition and will document that it has made this request. In any event, NetApp will on an annual basis provide to the Lead DPA general information on the number and type of Disclosure Requests it received in the preceding 12 month period, to the fullest extent permitted by applicable law.

3.5 Inquiries of the Customer

NetApp shall deal promptly and appropriately with inquiries of the Customer related to the Processing of the CI Information pursuant to the terms of the Services Contract.

4 Processor Purposes

4.1 Legitimate Business Purposes

Where NetApp serves as a Data Processor, CI Information may be Processed by NetApp for one or more of the following purposes:

(i) Customer data management information services (Infrastructure-as-a-Service, Platform-as-a-Service, and Software-as-a-Service) such as:

  (a) Data management, including storage, migration, synchronization, backup, or data loss prevention services;

  (b) Data systems management, including management of applications, virtualized environments (e.g. virtual machines or containers), and public and private clouds; or

  (c) Data analytics, including telemetry, risk and cloud analytics;

(ii) Customer-specific professional and managed services including:

  (a) System and solution design, deployment and integration, data migration, and ongoing (local and remote) system and solution management (e.g., by engaging specialists, undertaking project management activities, modifying of systems);

  (b) The collection and analysis of Customer use data to report trends (e.g., specific status reports, management reporting, the general improvement of Customer's internal operations);

  (c) The provision of training for Customer's staff or third parties.

(iii) Customer support services including:

  (a) Providing (local and remote) assistance to Customer in the use or repair of NetApp products or services;

  (b) NetApp generation of service level reports or other reports on a Customer's use of NetApp products or services for Customer management information purposes; or

(c) Life-cycle management of NetApp products and services (e.g., planning, evaluation, demonstration, installation, calibration, training, maintenance, decommissioning) to facilitate continued and sustained use by a Customer of NetApp products and services.

(iv) **NetApp internal business process execution and management** leading to incidental Processing of Personal Information for:

(a) Internal auditing of NetApp Processor-related activities;

(b) Activities related to compliance with applicable law or regulation (e.g., data processing law);

(c) Data de-identification and aggregation of de-identified data for data minimization; and

(d) Use of de-identified, aggregate data to facilitate continuity, sustainability, and improvement of NetApp products and services.

5 Security and Confidentiality Requirements

5.1 Information Security

NetApp shall take appropriate commercially reasonable technical, physical and organizational measures to protect CI Information from misuse or accidental, unlawful or unauthorized destruction, loss, alteration, disclosure, acquisition or access during the Processing. NetApp shall in any event take the measures specified in **Appendix 2** of these Processor BCRs, which Appendix may be revised by NetApp, provided that such changes do not in any material manner diminish the level of security provided to CI Information under **Appendix 2**.

5.2 Data Access and Confidentiality

NetApp shall provide NetApp Staff access to CI Information only to the extent necessary to perform the Processing and to perform their job. NetApp shall impose confidentiality obligations on Staff with access to CI Information.

5.3 Information Security Breach Notification Requirement

NetApp shall notify the Customer of an Information Security Breach as soon as reasonably possible following its determination that an Information Security Breach has occurred to the extent such reporting is permitted by applicable law.

6 Transparency to Customer Individuals

6.1 Other Requests of Customer Individuals

NetApp shall promptly notify the Customer of requests or complaints that are received directly from a Customer Individual regarding NetApp's obligations under these Processor BCRs without responding to such requests or complaints, unless otherwise instructed by the Customer in the Services Contract.

If instructed by the Customer to respond to requests and complaints of Customer Individuals, NetApp shall ensure that the Customer Individual is provided with all information reasonably required to address the request or complaint (including about the point of contact and the procedure) in order for the Customer Individual to be able to effectively make the request or lodge the complaint.

7 Third Party Sub-Processors

7.1 Third Party Sub-Processor Contracts

Third Party Sub-Processors may Process CI Information only if the Third Party Sub-Processor has a binding contract with NetApp. The contract shall impose data protection-related Processing terms on the Third Party Sub-Processor that will be no less protective than those imposed on the NetApp Contracting Entity by the Services Contract and these Processor BCRs

7.2 Publication of Overview of Third Party Sub-Processors

NetApp shall publish on the appropriate NetApp website an overview of the Third Party Sub-Processors involved in the performance of the relevant Customer Services. This overview shall be promptly updated in case of changes.

7.3 Notification of New Third Party Sub-Processors and Right to Object

NetApp shall provide notice to the Customer before authorizing any new Third Party Sub-Processors engaged by NetApp for the delivery of the Customer Services to Process CI Information. Following such notice, the Customer may object to the involvement of such Third Party Sub-Processor in the delivery of the Customer Services by providing objective justifiable grounds related to the ability of such Third Party Sub-Processor to protect CI Information or comply with applicable data protection or security requirements. In the event the objection is not unreasonable, NetApp and the Customer will work together in good faith to find a solution to address such objection, including but not limited to reviewing additional documentation supporting the Third Party Sub-Processors' compliance or making the Customer Services available without the involvement of such Third Party Sub-Processor. To the extent the parties cannot reach a mutually acceptable solution, the Customer shall have the right to terminate the relevant Customer Services (i) in accordance with the terms of the Services Contract; (ii) without liability to NetApp or the Customer; and (iii) without relieving the Customer from its payment obligations under the Services Contract up to the date of termination.

8 Privacy Governance

NetApp's Global Chief Privacy Officer (**GCPO**) is responsible for overseeing and ensuring compliance with these Processor BCRs and establishing the global framework for data privacy compliance. The GCPO, through members of the Integrity and Compliance Office monitors compliance with the BCRs and the laws on a day-to-day basis. The GCPO is responsible for monitoring compliance globally, and for ensuring that any changes to the BCRs are communicated within NetApp operations worldwide. The GCPO advises the Board of Directors and Audit Committee, deals with DPA's investigations, coordinates with the Internal Audit Department to provide reporting on compliance with the BCRs annually, ensures compliance at a global level, and

manages and coordinates with the Global Data Privacy Governance Council to ensure compliance with the rules. The Integrity and Compliance Office is responsible for handling local complaints from data subjects, reporting major privacy issues to the GCPO, and ensuring compliance at a local level.

9 Policies, Procedures and Training

9.1 Policies and Procedures

NetApp shall develop and implement policies, procedures, and guidelines to comply with these Processor BCRs.

9.2 System Information

NetApp shall maintain readily available information regarding the structure and functioning of all systems and processes that Process CI Information (e.g., inventory of systems and processes, privacy impact assessments). A copy of this information will be provided to the Lead DPA or to a Customer DPA upon request.

9.3 Staff Training

NetApp shall provide training on the obligations and principles laid down in these Processor BCRs and related confidentiality and other privacy and data security obligations to Staff who Processes CI Information.

10 Monitoring and Auditing Compliance

10.1 Internal Audits

NetApp Internal Audit shall audit business processes and procedures that involve the Processing of CI Information for compliance with these Processor BCRs. The audits shall be carried out in the course of the regular activities of NetApp Internal Audit or at the request of the GCPO. The GCPO may request to have an audit as specified in this Article conducted by an external auditor. Applicable professional standards of independence, integrity and confidentiality shall be observed when conducting an audit. The GCPO shall be informed of the results of the audits. Any violations of these Processor BCRs identified in the audit report will be reported to the Global Data Privacy Governance Council. A copy of the audit results related to compliance with these Processor BCRs will be provided upon request to the Lead DPA, the Customer, or to any Customer DPA.

10.2 Customer Audit

NetApp shall, at its option, either

(i) Make available the facilities it uses for the Processing of CI Information for an audit by a qualified independent third party auditor selected by the Customer, provided such auditor is (a) reasonably acceptable to NetApp and (b) has executed a written confidentiality agreement reasonably acceptable to NetApp before conducting the audit. In accordance with the audit provisions of the applicable Services Contract audits shall be conducted no more than once per year per Customer and during regular business hours, and shall be subject to (a) a written request submitted to NetApp at least six weeks in advance of the

proposed audit date, (b) a detailed written audit plan reviewed and approved by NetApp's security organization and (c) NetApp's on-site security policies. Upon completion of an audit, the Customer shall provide NetApp with a copy of the audit report, which shall be treated as confidential information pursuant to the terms of the Services Contract; or

(ii) Provide to the Customer upon request a statement issued by a qualified independent third party assessor certifying that the NetApp business processes and procedures that involve the Processing of CI Information comply with the principles set forth in these Processor BCRs.

10.3 DPA Audit

The Lead DPA may request an audit of the facilities used by NetApp for the Processing of CI Information for compliance with these Processor BCRs. In addition, a DPA that has the right to audit a Customer (a **Customer DPA**) will be authorized to audit the relevant data transfer for compliance with these Processor BCRs, subject to the same conditions as would apply to an audit by that DPA of the Customer itself under the Applicable Data Controller Law.

10.4 DPA Audit Procedure

NetApp will facilitate any audit by a DPA under Article 10.3, by undertaking the following actions:

(i) Information sharing: NetApp and the Customer will collaborate in good faith to attempt to resolve the request using alternative methods of providing information to the DPA including NetApp audit reports, discussion with NetApp subject matter experts, and review of security, privacy, and operational controls in place. The Customer will have access to its CI Information in accordance with the Services Contract and may delegate such access to representatives of the DPA.

(ii) Examinations: If the information available through these mechanisms is insufficient to address the DPA's stated objectives, NetApp will provide the DPA with the opportunity to communicate with NetApp's auditor at the Customer's expense.

(iii) If this appears insufficient, NetApp will provide the DPA with a direct right to examine NetApp's data processing facilities used to process the CI Information on giving reasonable prior notice and during business hours, with full respect to the confidentiality of the information obtained and to the trade secrets of NetApp.

(iv) Scope: The DPA can only access the CI Information belonging to the Customer. The Customer will be liable for NetApp's reasonable additional costs associated with such examination.

For clarity, NetApp and its Customers are committed to working together in good faith to resolve a DPA request through discussion and interaction among the Customer, NetApp, and the DPA. Nothing in this Article 10.4 will be construed to take away any audit rights that a DPA may have under applicable law or Services Contracts. These Processor BCRs provide supplemental audit rights to DPAs only. In the event of any conflict between this Article 10.4 and applicable law, the provisions of applicable law shall prevail.

10.5 Annual Privacy Report

The GCPO shall produce a CI Information privacy report for the Audit Committee of the Board of Directors of NetApp, Inc. on NetApp compliance with these Processor BCRs, privacy protection risks and other relevant issues. This report will be produced every 12-24 months, the exact frequency to be determined based on the circumstances.

10.6 Mitigation

NetApp shall, if so indicated, ensure that adequate steps are taken to address breaches of these Processor BCRs identified during the monitoring or auditing of compliance pursuant to this Article.

11 Legal Issues

11.1 Rights of Customer Individuals

If NetApp violates the Processor BCRs with respect to the CI Information of a Customer Individual (Affected Individual) covered by these Processor BCRs, the Affected Individual can as a third party beneficiary enforce any claim as a result of a breach of Articles 1.1, 1.5, 1.6, 2.1, 2.2, 3, 5, 6.1, 7.1, 7.3, 9.2, 10.2, 11.1-11.4, 11.8, 13.1, and 13.3.

11.2 Complaints Procedure

Customer Individuals may file a written complaint in respect of any claim they have under Article 11.1 with NetApp's Integrity and Compliance Office. Customer Individuals may also file a complaint or claim with the authorities or the courts in accordance with Article 11.3.

NetApp's Integrity and Compliance Office shall be responsible for complaint handling. Each complaint will be assigned to an appropriate Staff member (either within the Integrity and Compliance Office or within the applicable business unit or functional area). These Staff will:

(a) Promptly acknowledge receipt of the complaint;

(b) Analyze the complaint and, if needed, initiate an investigation;

(c) If the complaint is well-founded, advise the GCPO so that a remediation plan can be developed and executed; and

(d) Maintain records of all complaints received, responses given, and remedial actions taken by NetApp.

NetApp will use reasonable efforts to resolve complaints without undue delay, so that a response is given to the Customer Individual within four weeks of the date that the complaint was filed. The response will be in writing and will be sent to the Customer Individual via the means that the Customer Individual originally used to contact NetApp (e.g., via mail or email). The response will outline the steps that NetApp has taken to investigate the complaint and will indicate NetApp's decision regarding what steps (if any) it will take as a result of the complaint.

In the event that NetApp cannot reasonably complete its investigation and response within four weeks, it shall inform the Customer Individual within four weeks that the investigation is ongoing and that a response will be provided within the next eight week period.

If NetApp's response to the complaint is unsatisfactory to the Customer Individual (e.g., the request is denied) or NetApp does not observe the conditions of the complaints procedure set out in this Article 11.2, the Customer Individual can file a complaint or claim with the authorities or the courts in accordance with Article 11.3.

11.3 Jurisdiction for Claims of Customer Individuals

The Affected Individual may, at his/her choice, submit any claim under Article 11.1:

To the DPA or the courts in the EEA country of his/her habitual residence, place of work, or the place where the infringement took place, against the NetApp Contracting Entity; or

To the Lead DPA or the courts in the Netherlands, against NetApp Holding BV.

The courts, and DPAs shall apply their own substantive and procedural laws to the dispute. Any choice made by the Affected Individual will not prejudice the substantive or procedural rights he or she may have under applicable law.

11.4 Right to Claim Damages, Reversal of Burden of Proof

In case an Affected Individual has a claim under Article 11.1, the Affected Individual shall be entitled to recover damages that he or she suffered resulting from a violation of these Processor BCRs to the extent provided by Data Protection Law.

In case an Affected Individual brings a claim for damages under Article 11.1, it will be for the Affected Individual to demonstrate that he/she has suffered damage and to establish facts which show it is plausible that the damage has occurred because of a violation of these Processor BCRs. It will subsequently be for the NetApp Contracting Entity or NetApp Holding BV to prove that the damages suffered by the Affected Individual due to a violation of these Processor BCRs are not attributable to a Group Company or a Sub-Processor or to assert other applicable defenses.

The NetApp Contracting Entity or NetApp Holding BV may not rely on a breach by a Sub-Processor of its obligations to avoid liability except to the extent any defense of Sub-Processor would also constitute a defense of NetApp. NetApp may, however, assert any defenses or rights that would have been available to the Customer. NetApp also may assert any defenses that NetApp could have asserted against the Customer (such as contributory negligence), in defending against the Affected Individual's claim.

11.5 Rights of Customers

The Customer may enforce these Processor BCRs against the NetApp Contracting Entity or, if the NetApp Contracting Entity is not established in an EEA Country, against NetApp Holding BV. NetApp Holding BV shall, if so indicated, ensure that adequate steps are taken to address violations of these Processor BCRs by the NetApp Contracting Entity or any other Group Company.

The NetApp Contracting Entity or NetApp Holdings BV may not rely on a breach by another Group Company or a Sub-Processor of its obligations to avoid liability, except to the extent any defense of Sub-Processor would also constitute a defense of NetApp.

11.6 Available Remedies, Limitation of Damages

In case of a violation of these Processor BCRs, Customers shall be entitled to compensation of damages consistent with the Services Contract.

11.7 Mutual Assistance Group Companies and Redress

All Group Companies shall cooperate and assist each other to the extent reasonably possible to achieve compliance with these Processor BCRs, including an audit or inquiry by the Lead DPA, the Customer or a Customer DPA.

The NetApp Group Company receiving a request for information pursuant to Article 6.1 or a claim pursuant to Article 11.1, is responsible for promptly informing the GCPO thereof and handling any communication with the Customer Individual regarding his/her request or claim as instructed by the GCPO except where circumstances dictate otherwise.

11.8 Advice by Lead DPA

NetApp is committed to abiding by the advice of the Lead DPA and Customer DPAs issued on interpretation and application of these Processor BCRs. NetApp shall provide assistance requested by the Customer as reasonably required to enable the Customer's compliance with the Applicable Data Controller Law in accordance with the Services Contract and Articles 3.2 and 3.3.

12 Sanctions for Non-Compliance

Non-compliance of NetApp employees with these Processor BCRs may result in disciplinary action in accordance with NetApp policies and local law, up to and including termination of employment.

13 Conflicts between these Processor BCRs and Applicable Data Processor Law

13.1 Conflict between Processor BCRs and Law

Where there is a conflict between Applicable Data Processor Law and these Processor BCRs, the relevant Staff shall consult with the GCPO to determine how to comply with these Processor BCRs and resolve the conflict to the extent reasonably practicable given the legal requirements applicable to the relevant Group Company.

13.2 New Conflicting Legal Requirements

The relevant Staff, in consultation with the legal department, shall promptly inform the GCPO of any new legal requirement that may interfere with NetApp's ability to comply with these Processor BCRs.

13.3 Reporting to Lead DPA and Customer DPA

If NetApp becomes aware that Applicable Data Processor Law or any change in Applicable Data Processor Law is likely to have a substantial adverse effect on NetApp's ability to meet its obligations under 3.1, 3.2 or 10.3, NetApp will report this to the Lead DPA and the Customer DPA.

14 Changes to these Processor BCRs

14.1 Approval for Changes

Any changes to these Processor BCRs require the prior approval of the GCPO.

14.2 Effective Date Of Changes

Any change shall enter into force with immediate effect after it is approved and published on the NetApp Internet site and communicated to the Customers.

14.3 Prior Versions

Any request, complaint or claim of a Customer Individual involving these Processor BCRs shall be judged against the version of these Processor BCRs that is in force at the time the request, complaint or claim is made.

14.4 Notification to Lead DPA and Customers

The GCPO shall be responsible for informing the Lead DPA of material changes to these Processor BCRs (if any) on a yearly basis. Where a material change to these Processor BCRs has a material impact on the Processing conditions of the Customer Services, NetApp will promptly notify the Lead DPA thereof, including a brief explanation for such change, as well as provide notice of such change to the Customer. Within 30 days of receiving such notice, the Customer may object to such change by providing written notice to NetApp. In the event that the parties cannot reach a mutually acceptable solution, NetApp shall enable the Customer to terminate the relevant Customer Services in accordance with the terms of the Services Contract.

15 Transition Periods

15.1 Transition Period for New Group Companies

Except as otherwise indicated, any entity that becomes a Group Company after the Effective Date shall comply with these Processor BCRs within two years of becoming a Group Company.

15.2 Transition Period for Divested Entities

A Divested Entity (or specific parts thereof) will remain covered by these Processor BCRs after its divestment for such period as is required by NetApp to disentangle the Processing of CI Information relating to such Divested Entity.

15.3 Transition Period for IT Systems

Where implementation of these Processor BCRs requires updates or changes to information technology systems (including replacement of systems), the transition period shall be three years from the Effective Date or from the date an entity becomes a Group Company, or any longer period as is reasonably necessary to complete the update, change or replacement process.

15.4 Transition Period for Existing Agreements Compliance During Transition Periods

Where there are existing agreements with Third Parties that are affected by these Processor BCRs, the provisions of the agreements will prevail until the agreements are renewed in the normal course of business.

During the transition periods set out in Article 15.1 – 15.4, no CI Information will be transferred under these Processor BCRs until the relevant Group Company is (i) fully compliant or (ii) an alternative data transfer mechanism has been put in place, such as standard contractual clauses.

15.5 Contact Details

Any questions regarding these Processor BCRs can be directed to NetApp's Integrity and Compliance Office at the following addresses:

Ng-Privacy@netapp.com

NetApp, Inc.

c/o Legal Department

Attn: Global Chief Privacy Officer

1395 Crossman Avenue

Sunnyvale, CA 94089, USA

APPENDIX 1 – DEFINITIONS

Affected Individual	AFFECTED INDIVIDUAL shall have the meaning set forth in Article 11.1 above.
Applicable Data Controller Law	APPLICABLE DATA CONTROLLER LAW shall mean the Data Protection Laws applicable to the Customer as the Data Controller of the CI Information.
Applicable Data Processor Law	APPLICABLE DATA PROCESSOR LAW shall mean the Data Protection Laws that are applicable to NetApp as the Data Processor of the CI Information.
Article	ARTICLE shall mean an Article in these Processor BCRs.
Authority	AUTHORITY shall have the meaning set forth in Article 3.4 above.
CI Information	CI INFORMATION shall mean Personal Information of a Customer Individual.
Customer	CUSTOMER shall mean any Third Party who has entered into a contract with NetApp for Customer Services.
Customer DPA	CUSTOMER DPA shall have the meaning set forth in Article 10.3.
Customer Individual	CUSTOMER INDIVIDUAL shall mean any individual whose Personal Information is Processed by NetApp in its role as a Data Processor in the course of delivering Customer Services to a Customer.
Customer Services	CUSTOMER SERVICES shall mean the services provided by NetApp to Customers, which may include data storage and management software, systems and services.
Data Controller	DATA CONTROLLER shall mean the entity or natural person which alone or jointly with others determines the purposes and means of the Processing of Personal Information.
Data Processor	DATA PROCESSOR shall mean the entity or natural person that Processes Personal Information on behalf of a Data Controller.
Data Protection Law	DATA PROTECTION LAW shall mean the provisions of mandatory law of an EEA Country containing rules for the protection of individuals with regard to the Processing of Personal Information including security requirements for and the free movement of such Personal Information.

Disclosure Request	DISCLOSURE REQUEST shall have the meaning set forth in Article 3.4.
Divested Entity	DIVESTED ENTITY shall mean the divestment by NetApp of a Group Company or business by means of: (i) a sale of shares that results in the divested Group Company no longer qualifying as a Group Company; and/or (ii) a demerger, sale of assets, or any other manner or form.
DPA	DPA shall mean any data protection authority of one of the EEA Countries.
EEA Countries	EEA COUNTRIES (European Economic Area Countries) shall mean all Member States of the European Union, Norway, Iceland, Liechtenstein and, for purposes of these Processor BCRs, Switzerland.
EEA Data Transfer Restriction	EEA DATA TRANSFER RESTRICTION shall mean any restriction under Data Protection Law regarding outbound transfers of Personal Information.
Effective Date	EFFECTIVE DATE shall mean the date on which these Processor BCRs become effective as set forth in Article 1.6.
Global Chief Privacy Officer	GLOBAL CHIEF PRIVACY OFFICER (or GCPO) shall mean the officer referred to in Article 8.
Group Company	GROUP COMPANY shall mean NetApp, Inc. and wholly-owned direct or indirect subsidiary of NetApp, Inc.

Information Security Breach	INFORMATION SECURITY BREACH shall mean the unauthorized acquisition, access, use or disclosure of unencrypted CI Information that compromises the security or privacy of such data to the extent the compromise poses a high risk of financial, reputational, or other harm to the Customer Individual. An Information Security Breach is deemed not to have occurred where there has been an unintentional acquisition, access or use of unencrypted CI Information by an employee of NetApp or the Customer or an individual acting under their respective authority, if (i) the acquisition, access, or use of CI Information was in good faith and within the course and scope of the employment or professional relationship of such employee or other individual; and (ii) the CI Information is not further acquired, accessed, used or disclosed by any person.
Lead DPA	LEAD DPA shall mean the DPA of the Netherlands**.**
Mandatory Requirements	MANDATORY REQUIREMENTS shall mean mandatory requirements of Applicable Data Processor Law which do not go beyond what is necessary in a democratic society i.e. which constitute a necessary measure to safeguard national security defense, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the state or the protection of a Customer Individual or the rights and freedoms of others.
NetApp	NETAPP shall mean NetApp, Inc. and its Group Companies.
NetApp Contracting Entity	NETAPP CONTRACTING ENTITY shall mean the NetApp Group Company that has entered into the Services Contract.
NetApp Holding BV	NetApp Holdings BV shall mean NetApp Holding and Manufacturing BV., having its registered seat in Schiphol-Rijk, The Netherlands.
NetApp Sub-Processor	NETAPP SUB-PROCESSOR shall mean any Group Company engaged by NetApp as a Sub-Processor.
Personal Information	Personal INFORMATION shall mean any information relating to an identified or identifiable individual.

Processing	PROCESSING shall mean any operation that is performed on CI Information, whether or not by automatic means, such as collection, recording, storage, organization, alteration, use, disclosure (including the granting of remote access), transmission or deletion of CI Information.
Processor BCRs	PROCESSOR BCRs shall mean these Data Protection Binding Corporate Rules (BCRs) for Processor Activities.
Services Contract	SERVICES CONTRACT shall mean the contract for delivery of NetApp Services entered into between a NetApp Group Company and the Customer pursuant to Article 2.1.
Staff	STAFF shall mean all employees and other persons under the direct authority of NetApp who Process CI Information as part of their respective duties or responsibilities towards NetApp using NetApp information technology systems or working primarily from NetApp's premises.
Sub-Processor	SUB-PROCESSOR shall mean any Group Company or Third Party engaged by NetApp to Process CI Information as a sub-processor.
Third Party	THIRD PARTY shall mean any person or entity (e.g., an organization or public authority) outside NetApp.
Third Party Sub-Processor	THIRD PARTY SUB-PROCESSOR shall mean any Third Party engaged by NetApp as a Sub-Processor.
Third Party Sub-Processor Contract	THIRD PARTY SUB-PROCESSOR CONTRACT shall mean the validly entered into written or electronic agreement between the NetApp Contracting Entity and the Third party Sub-Processor pursuant to Article 7.2.

Interpretations

INTERPRETATION OF THIS PROCESSOR CODE:

(i) Unless the context requires otherwise, all references to a particular Article or Appendix are references to that Article or Appendix in or to this document, as they may be amended from time to time;

(ii) headings are included for convenience only and are not to be used in construing any provision of these Processor BCRs;

(iii) if a word or phrase is defined, its other grammatical forms have a corresponding meaning;

(iv) the male form shall include the female form(v) the words “include”, “includes” and “including” and any words following them shall be construed without limitation to the generality of any preceding words or concepts and vice versa ;

(v) a reference to a document (including, without limitation, a reference to these Processor BCRs) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by these Processor BCRs or that other document, and

(vi) a reference to law includes any regulatory requirement, sectorial recommendation, and best practice issued by relevant national and international supervisory authorities or other bodies.

APPENDIX 2 – SECURITY

NetApp maintains an information security program that contains physical, technical, and organizational measures designed to protect Personal Information in NetApp's possession or control. This Exhibit describes core measures that NetApp has in place to protect the security of Personal Information. NetApp may modify these security measures from time to time, provided that such modifications will not materially reduce the overall level of protection for Personal Information.

1. Information Security Policies and Procedures

NetApp's information security program includes policies and procedures designed to:

- Maintain the confidentiality, integrity, and availability of Personal Information in NetApp's possession or control;
- Protect such Personal Information against unauthorized access, use, disclosure, alteration, or destruction; and
- Identify and mitigate potential threats or hazards to the security of the Personal Information.

2. Physical Security

NetApp maintains physical security controls at all NetApp sites that contain an information system that uses or houses Personal Information. 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.

3. Technical Security

NetApp maintains technical security controls designed to:

- Restrict access to its information systems, including firewalls, intrusion detection and prevention systems, access control lists, and routing protocols;
- Safeguard data on NetApp laptops or other mobile devices or removable storage devices; and
- Protect Personal Information from unauthorized access during electronic transmission, transport or storage by NetApp.

4. Organizational Security

NetApp maintains policies, procedures, and technical controls to limit access to Personal Information to authorized persons, and to remove access rights promptly in the event of a change in job status.

NetApp requires NetApp personnel to comply with its information security program. NetApp maintains a security awareness program to train personnel about their security obligations.

5. Business Continuity

NetApp maintains disaster recovery and business continuity plans to mitigate the effects of natural disasters, emergencies, or similar events on NetApp's information systems and the sites that house them. NetApp regularly reviews and updates these plans to keep them up-to-date.

6. Disposal

NetApp maintains protocols for the disposal of equipment and media containing Personal Information, to guard against unauthorized access to Personal Information during or after the disposal process.