For agreements completed from March 31, 2019 to November 20, 2019:

EXHIBIT

DATA PRIVACY AGREEMENT

1. **DEFINITIONS**

    1. **Adequacy Decision.** “Adequacy Decision” means a decision issued by the European Commission that a country or region or a category of recipients in such country or region is deemed to provide an “adequate” level of data protection.

    2. **Affiliate.** An “Affiliate” means any entity which controls, is controlled by, or is under common control with the subject party.

    3. **Data Privacy Breach.** A “Data Privacy Breach” means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, access to, acquisition of Seagate Personal Information, or any other unauthorised Processing of Seagate Personal Information.

    4. **Data Protection Laws.** “Data Protection Laws” means (a) the General Data Protection Regulation 2016/679 (“GDPR”) and all applicable data protection laws and regulations of a country that is a member of the European Union (“**EU**”) or the European Economic Area (“**EEA**”) and (b) any applicable laws or regulations of any other jurisdiction governing the Processing or protection of personal data

    5. **Data Subject.** “Data Subject” is an identified or identifiable natural person about whom Seagate Personal Information may be Processed under this DPA.

    6. **Seagate Personal Information.** “Seagate Personal Information” means any information that relates to an identified or identifiable natural person, which is created, owned, or provided by Seagate or for Seagate, that Supplier has access to, obtains, uses, maintains, or Processes in connection with any agreement(s) between the parties and/or their Affiliates.

    7. **Processing.** “Process” or “Processing” means, without limitation, operations performed on Seagate Personal Information, whether or not by automated means, such as collecting, recording, organising, structuring, altering, using, accessing, disclosing, disseminating, copying, transferring, storing, deleting, aligning, combining, restricting, adapting, retrieving, consulting, destroying, or disposing Seagate Personal Information.

8. **Privacy Shield.** “Privacy Shield” means the E.U.-U.S. Privacy Shield Framework developed by the U.S. Department of Commerce and the European Commission and the Swiss-U.S. Privacy Shield Framework developed by the U.S. Department of Commerce and Switzerland, including the Privacy Shield Principles and Supplemental Principles available at: https://www.privacyshield.gov/EU-US-Framework.

9. **Sensitive Information** means any of the following types of Seagate Personal Information: (i) national insurance number, taxpayer identification number, passport number, driving licence number or other government-issued identification number; (ii) credit or debit card details or financial account number, with or without any code or password that would permit access to the account or credit history; or (iii) information on race, religion, ethnicity, sex life or practices or sexual orientation, medical or health information, genetic or biometric information, biometric templates, political or philosophical beliefs, political party or trade union membership, background check information or judicial data such as criminal records or information on other judicial or administrative proceedings.

10. **Standard Clauses.** “Standard Clauses” means the standard contractual clauses for the transfer of personal information to Processors established in third countries which do not ensure an adequate level of data protection (Commission Decision 2010/87/EU or any successor version), with optional clauses removed.

11. **Sub-processor.** A “Sub-processor” means any third party engaged by Supplier or by any other Sub-processor who will have access to, receive, or otherwise Process any Seagate Personal Information.

12. **Supplier Personnel.** “Supplier Personnel” means any Supplier employee, contractor, Sub-processor or agent whom Supplier authorises to Process Seagate Personal Information.

13. The terms **“Controller”**, **“Processor”** and **“Supervisory Authority”** shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

14. The word **“include”** shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. **DATA SECURITY AND PROTECTION**

    1. **Status of the Parties.** The parties hereby acknowledge and agree that Seagate is the Controller and Supplier is the Processor with respect to the Seagate Personal Information.

    2. **Non-disclosure of Seagate Personal Information.** Supplier shall not disclose Seagate Personal Information in any manner for any purpose to any third party without obtaining prior written authorisation from Seagate, except as otherwise provided in Section 2.5 below.

    3. **Limitations on Processing.** Supplier shall not Process or permit the Processing of Seagate Personal Information except as necessary to provide services to Seagate in accordance with any agreement(s) between the parties and/or their Affiliates or other written instructions of Seagate.

    4. **Information Security Program.** Supplier will implement, maintain, monitor and, where necessary, update a comprehensive written information security programme that contains appropriate administrative, technical, and physical safeguards to protect Seagate Personal Information against anticipated threats or hazards to its security, confidentiality or integrity (such as unauthorised access, collection, use, copying, modification, disposal or disclosure, unauthorised, unlawful, or accidental loss, destruction, acquisition, or damage or any other unauthorised form of Processing) ('**Information Security Program**'). The Information Security Program will include the measures listed in the Security Standards attached as Schedule 2.

    5. **Restrictions on Sub-processors.** Supplier may disclose Seagate Personal Information to Sub-processors as necessary to perform its services for Seagate, subject to the conditions set forth in this Section 2.5. Supplier shall maintain a list of the Sub-processors to which it discloses Seagate Personal Information, and will provide this list to Seagate upon Seagate's request. Supplier will provide Seagate a current list of Supplier's Sub-processor(s) as of the effective date of this DPA. The Supplier shall notify Seagate at data.protection.contracts@seagate.com at least **30 business days** before adding any Sub-processor to the list. If Seagate does not object to the proposed Sub-processor within **30 business days** of receipt of notice, the Sub-processor is deemed to have been approved. If Seagate objects to any Sub-processor having access to Seagate Personal Information, then Supplier shall not disclose Seagate Personal Information to

the Sub-processor. If at any time either party finds a Sub-processor is not providing sufficient guarantees of security appropriate to the risk associated with the Seagate Personal Information being Processed, Seagate may in its sole discretion, remove the Sub-processor from the list. In the event a Supplier is objected to or removed by Seagate, the Supplier will be provided a reasonable amount of time to replace the Sub-processor. If Supplier cannot provide the Services without disclosing Seagate Personal Information to the objected Sub-processor, then Seagate may terminate any applicable agreement(s) between the parties and/or their Affiliates without cost or liability owed to Supplier.

6. **Sub-processor Compliance and Breach.** The Supplier's use of Sub-processors does not reduce the Supplier's obligation to comply with this DPA or applicable Data Protection Laws. Supplier will be liable to Seagate for performance of the services, Data Privacy Breaches and breaches of this DPA and applicable Data Protection Laws by its Sub-processors to the same extent as if Supplier breached.

7. **Obligations of Supplier Personnel and Sub-processors.** The Supplier shall ensure that any person or Sub-processor who has access to Seagate Personal Information is (are) bound by written privacy and data protection terms at least as restrictive as those in this DPA. The Supplier shall ensure that all privacy and data protection obligations continue after their Processing for Seagate ends. This obligation continues in perpetuity, or alternatively, at least until Supplier has certified that all Seagate Personal Information has been deleted, destroyed, and irretrievable.

8. **Limited Access.** Supplier shall limit access to Seagate Personal Information to Supplier Personnel or Sub-processors who require access for Supplier to perform its obligations under any agreement(s) between the parties and/or their Affiliates or Seagate's written instruction, who have (a) been trained on data protection and security requirements, and (b) agreed to comply with data confidentiality requirements at least as restrictive as those required by Seagate during and after their Processing for Seagate.

9. **Notice of Requests or Complaints.** Unless prohibited by law, Supplier shall notify Seagate at data.protection.officer@seagate.com within **2 business days** after receiving any request or complaint relating to the Processing of Seagate Personal Information, including:

1. requests from a Data Subject for data portability, requests to access, change, delete, or restrict, and similar requests; or
2. complaints or allegations that the Processing infringes on a Data Subject's rights.

10. **Supplier Responses.** The Supplier shall not respond to any request or complaint under Section 2.9 unless expressly authorised to do so by Seagate. The Supplier shall cooperate with Seagate with respect to any action taken relating to any request or complaint. Supplier shall seek to implement appropriate processes (including technical and organizational measures) to assist Seagate in responding to requests or complaints, unless prohibited by law.

11. **Requests for Disclosure.** Unless prohibited by law, the Supplier shall immediately notify Seagate if the Supplier receives any document requesting or purporting to compel the disclosure of Seagate Personal Information (such as oral questions, interrogatories, requests for information or documents in legal proceedings, subpoenas, civil investigative demands, or other similar requests or processes; collectively, **'Disclosure Requests'**). If a Disclosure Request is not binding, the Supplier will not respond. If a Disclosure Request is binding, the Supplier shall, unless prohibited by applicable law, notify Seagate at least **48 hours** before responding so that Seagate may exercise such rights as it may have to prevent or limit the disclosure. The Supplier shall exercise reasonable efforts to prevent and limit any disclosure and to preserve the confidentiality of Seagate Personal Information. Supplier shall cooperate with Seagate with respect to any action taken in response to Disclosure Request, including cooperating to obtain an appropriate protective order or other assurance to protect the confidentiality of the Seagate Personal Information.

12. **Cooperation.** Supplier shall assist Seagate in meeting its obligations under Data Protection Laws regarding (a) registration and notification; (b) accountability; (c) ensuring the security of Seagate Personal Information; and (d) fulfilling privacy and data protection impact assessments and related consultations of Supervisory Authorities.

13. **Participation in Regulatory Investigations.** Supplier shall assist and support Seagate in any investigation by any Supervisory Authority to the extent the investigation relates to Seagate Personal Information Processed by Supplier or Supplier's Sub-processor.

14. **Notice of Potential Violations or Inability to Comply.** Supplier shall immediately notify Seagate if:
    1. The Supplier has reason to believe that any instructions from Seagate regarding Processing of Seagate Personal Information would violate applicable law;
    2. Supplier has reason to believe that it is unable to comply with any of its obligations under this DPA or Data Protection Laws and it cannot cure this inability to comply within a reasonable timeframe; or
    3. The Supplier becomes aware of any circumstances or changes in applicable law that are likely to prevent it from fulfilling its obligations under this DPA.
15. **Suspension or Adjustments for Compliance.** Seagate may suspend the Supplier's or Sub-processors' Processing of Seagate Personal Information to prevent potential violations of or non-compliance with applicable law, this DPA, or any applicable agreement(s) between the parties and/or their Affiliates related to privacy or data protection. The Supplier shall cooperate with Seagate to adjust the Processing to remedy any potential violation or noncompliance. If adjustment is not possible, Seagate may terminate any applicable agreement(s) between the parties and/or their Affiliates, without cost or liability owed to Supplier.

3. **DATA TRANSFERS**

1. **European Economic Area Standard Clauses.** If the Supplier transfers Personal Information received from within the EEA to a recipient outside the EEA that is not covered by an Adequacy Decision, then the Supplier shall enter into Standard Clauses, provided separately. Supplier shall ensure that any Sub-processors also execute the Standard Clauses, where applicable.
2. **Privacy Shield Certification.** If the Supplier has certified to the Privacy Shield, the Supplier shall maintain its certification to the Privacy Shield for the duration of any agreement(s) between the parties and/or their Affiliates. The Supplier shall enter into an appropriate onward transfer agreement with any Sub-processor before any disclosure. If Supplier determines that it can no longer meet its obligation to provide the level of protection required by the Privacy Shield, Supplier shall immediately notify Seagate in writing and shall return or destroy all Seagate Personal Information received pursuant to its Privacy Shield certification.

3. **Other Jurisdiction Provisions.** Where applicable, Supplier shall comply with the Requirements for Specific Jurisdictions, attached as Schedule 1.

4. **COMPLIANCE AND ACCOUNTABILITY**

    1. **Compliance.** The Supplier shall ensure that Supplier's and Sub-processors' Processing of Seagate Personal Information complies with all applicable laws, self-regulatory frameworks, and contract requirements applicable to the Supplier and Sub-processor. The Supplier shall annually review the Supplier's and Sub-processors' practices to ensure they comply with this DPA and with all applicable laws. Supplier shall cooperate, at its own expense, with Seagate's requests that Supplier demonstrate compliance with the data protection and security terms referenced in this DPA.

    2. **Records of Processing Activities.** Supplier will maintain an up-to-date record of the details of the Supplier's representative and data protection officer, categories of Processing activities performed, information regarding cross-border data transfer, a general description of the security measures implemented in respect of the Processed data, the name, contact and Processing details of each Sub-processor of Seagate Personal Information, and, where applicable, any Sub-processors' representative and data protection officer. Upon request, Supplier will provide an historical and current copy of this record to Seagate.

    3. **Audit.** The Supplier shall make available to Seagate, upon written request, all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including onsite inspections, by Seagate or an independent third-party auditor mandated by Seagate in relation to the Processing of Seagate Personal Information. Any such independent third-party auditor shall be required to enter into a non-disclosure agreement with the parties. The Supplier shall remedy any non-compliance within a reasonable amount of time. If remediation is not possible, Seagate may terminate any applicable agreement(s) between the parties and/or their Affiliates, without cost or liability owed to Supplier.

5. **SUPPLIER RESPONSIBILITIES AFTER A DATA PRIVACY BREACH**

    1. **Notification of Data Privacy Breach.** Supplier shall notify Seagate in writing of a known or suspected Data Privacy Breach immediately, and in any event within 24 hours after first learning of the potential Data Privacy Breach, and shall immediately:

1. notify Seagate at data.protection.officer@seagate.com of the Data Privacy Breach;
2. investigate or provide required assistance in the investigation of the Data Privacy Breach;
3. provide Seagate with detailed information about the Data Privacy Breach, including but not limited to the categories, location, and approximate number of Data Subjects concerned and the categories, location, and approximate number of Seagate Personal Information records, and continue to provide Seagate promptly with additional information about the Data Privacy Breach as it becomes available;
4. take all commercially reasonable steps to mitigate the effects of the Data Privacy Breach, or assist Seagate in doing so; and
5. implement a remediation plan, subject to Seagate's approval, and monitor the resolution of Data Privacy Breaches and vulnerabilities related to Seagate Personal Information to ensure that appropriate corrective action is taken on a timely basis.

2. **Containment and Remedy.** Supplier shall immediately contain and remedy any Data Privacy Breach and prevent any further Data Privacy Breach; and Supplier shall take all actions necessary to comply with applicable Data Protection Laws and industry standards to contain and remedy the Data Privacy Breach.
3. **Communications.** Supplier shall not issue any communications related to a Data Privacy Breach, in any manner that would identify, or is reasonably likely to identify or reveal the identity of, Seagate, without Seagate's prior approval.
4. **Preservation of Evidence.** The Supplier shall maintain an incident response plan. Following discovery of a Data Privacy Breach, Supplier shall preserve evidence related to the Data Privacy Breach and maintain a clear chain of command according to Supplier's incident response plan.
5. **Cooperation.** The Supplier shall cooperate with Seagate in any litigation, investigation, or other action Seagate requires to protect Seagate's rights relating to the use, disclosure, protection, and maintenance of Seagate Personal Information. Supplier further agrees to provide reasonable assistance and cooperation requested by Seagate and/or Seagate's designated representatives, in the furtherance of any correction, remediation, or

investigation of any Data Privacy Breach and/or the mitigation of any potential damage, including any notification that Seagate may determine appropriate to send to affected Data Subjects, regulators or third parties, and/or the provision of any credit reporting service that Seagate deems appropriate to provide to affected Data Subjects. The Supplier will be responsible for Seagate's reasonable expenses related to a Supplier Data Privacy Breach, including but not limited to investigation, remediation, and notification.

6. **RETURN AND SECURE DELETION OF SEAGATE PERSONAL INFORMATION**

    1. **Data Integrity.** Supplier shall comply with all Seagate instructions to maintain data integrity, including (a) disposing of Seagate Personal Information that is maintained by Supplier but that is no longer necessary to provide Services; (b) ensuring that any Seagate Personal Information created by Supplier on Seagate's behalf is accurate and kept up to date; and (c) upon Seagate's request, allow Seagate to access any Seagate Personal Information, all in accordance with applicable laws.

    2. **Return and Deletion of Seagate Personal Information.** Upon the earlier (a) request by Seagate or (b) the expiration or earlier termination of the agreement(s) between the parties and/or their Affiliates related to the Processing of Seagate Personal Information, at Seagate's direction, the Supplier shall direct its Sub-processors to export the Seagate Personal Information or provide Seagate, or its third-party designee, with the ability to export all Seagate Personal Information in a machine-readable and interoperable format determined by Seagate. The Supplier shall maintain the Seagate Personal Information for as long as Seagate determines is reasonably necessary to allow Seagate to fully access and export Seagate Personal Information, at no cost to Seagate. Each party shall identify a contact person to migrate the Seagate Personal Information and shall work promptly, diligently, and in good faith to facilitate a timely transfer. Within 90 days after Seagate (a) confirms that Seagate Personal Information was received and migrated correctly, or (b) informs Supplier of its election to not migrate the Seagate Personal Information, Supplier and Sub-processors shall securely destroy all Seagate Personal Information, delink Seagate's workspace identifiers, and overwrite with new data or otherwise destroy the Seagate Personal Information through an approved sanitization method.

3. **Destruction of Seagate Personal Information.** If Supplier disposes of any paper, electronic or other record containing Seagate Personal Information, Supplier will do so by taking all reasonable steps (based on the sensitivity of the Seagate Personal Information) to destroy Seagate Personal Information by: (a) shredding; (b) permanently erasing and deleting; (c) degaussing; or (d) otherwise modifying the Seagate Personal Information in such records to make it unreadable, unreconstructable and indecipherable. If the Supplier decommissions or otherwise retires a hard drive that contains a copy of Seagate Personal Information then the Supplier shall securely shred or destroy the drive rendering the Seagate Personal Information unreadable and destroyed in accordance with NIST 800-88, revision 1. The Supplier shall certify in writing that the drive has been shredded or destroyed and that the Seagate Personal Information cannot be read, retrieved, or otherwise reconstructed.

4. **Notice of Any Retention.** If the Supplier has a legal obligation to retain Seagate Personal Information beyond the period otherwise permitted by this DPA, the Supplier shall notify Seagate in writing of its obligation, and shall return or destroy the Seagate Personal Information as soon as possible after the legally-required retention period ends. This DPA will remain in effect until Supplier has ceased to have custody or control of or access to any Seagate Personal Information.

5. **Documentation.** The Supplier shall document its retention and disposal of Seagate Personal Information pursuant to this DPA. Upon Seagate's request, Supplier shall provide documentation of retention and a written certification that Seagate Personal Information has been securely destroyed in accordance with this DPA.

7. **MISCELLANEOUS**

1. **Term.** This DPA will remain in effect until (i) there is no other active agreement(s) between the parties and (ii) Supplier has ceased to have custody or control of or access to any Seagate Personal Information.

2. **Order of Precedence.** In case of discrepancies between this DPA and any agreement(s) between the parties and/or their Affiliates, the provisions of this DPA will prevail except for any discrepancies involving Schedule III (Security Standards), in which case the other agreement(s) will prevail. This DPA shall not limit or restrict, but shall only be deemed to supplement the Standard Clauses

3. **Updates.** The parties will reasonably cooperate to update this DPA by mutual written agreement as needed to ensure compliance with applicable laws and regulations

4. **Third Party Beneficiaries.** Seagate's Affiliates are intended third-party beneficiaries of this DPA and may enforce the terms of this DPA as if each was a signatory to this DPA. Seagate also may enforce the provisions of this DPA on behalf of its Affiliates, instead of its Affiliates separately bringing a cause of action against Supplier.

5. **Disclosure of DPA to Supervisory Authority.** Seagate may provide a summary or a copy of this DPA to any Supervisory Authority.

6. **Severance.** If any provision in this DPA is ineffective or void, this will not affect the remaining provisions. The parties shall replace the ineffective or void provision with a lawful provision that reflects the purpose of the ineffective or void provision. In case a necessary provision is missing, the parties shall add an appropriate one in good faith.

7. **Counterparts.** This DPA may be signed by electronic signature, and such electronic signature shall be treated as an original, including for evidentiary purposes. This DPA may be signed in two or more counterparts, none of which needs to contain the signatures of both of the parties, and each of which will be deemed to be an original, and all of which taken together will constitute one and the same instrument.

8. **Interpretation.** The headings in this DPA are for reference only and will not affect the interpretation of this agreement.

SCHEDULE 1

DATA PRIVACY REQUIREMENTS FOR SPECIFIC JURISDICTIONS

The following requirements apply to the jurisdictions specified:

1. **AUSTRALIA**

    1. **Applicability.** The provisions of this Section 1 apply where (a) Supplier receives or accesses Seagate Personal Information from a Seagate Affiliate located in Australia; or (b) Seagate notifies Supplier that Seagate Personal Information is subject to these requirements.

2. **Membership of a Professional or Trade Association.** The term “Sensitive Information” also includes Personal Information about an individual’s membership of a professional or trade association.

3. **Australian Privacy Principles.**The Supplier must comply with any applicable obligations under the Privacy Act 1988 (Cth), including the Australian Privacy Principles, when dealing with Seagate Personal Information or otherwise providing the services pursuant to this DPA.

4. **Note of use or disclosure for enforcement purposes.** If Supplier uses or discloses Personal Information for one or more enforcement activities conducted by, or on behalf of, an enforcement body, Supplier shall keep a written record of the use and disclosure and promptly provide a copy of the record to Seagate, unless prohibited by law.

5. **Australian government related identifiers.** Where the Personal Information includes Australian government related identifiers Supplier (a) shall not adopt the Australian government related identifier for an individual as its own identifier of the individual unless expressly directed to do so by Seagate; and (b) shall not use or disclose the Australian government related identifier except where reasonably necessary to verify the identity of the individual, or otherwise where directed to do so by Seagate.

6. **Collection of Personal Information.** Where Seagate’s instructions to Supplier require Supplier to collect personal information on Seagate’s behalf, Supplier must (a) seek instructions from Seagate regarding (i) any information that must be provided to the Data Subject in connection with the collection of the Data Subject’s personal information; and (ii) any opt-in consents required for direct marketing purposes; and (b) not collect any Sensitive Information or without the Data Subject’s consent.

7. **Supplier Agreements with the Australian Government.** If Seagate is a contracted service provider to an Australian government entity at federal, state or territory level, and to the extent Seagate is bound to comply with additional data protection obligations by virtue of an agreement with the relevant government entity, Seagate will impose equivalent obligations upon the Supplier, as required under applicable Australian law. Seagate and Supplier agree to enter into additional agreements, if needed, to reflect those obligations.

2. **JAPAN**

    1. **Applicability.** The provisions of this Section 2 apply to Seagate Personal Information Supplier receives or accesses from a Seagate Affiliate located in Japan

    2. **Supplier Personnel.** Supplier will be responsible for supervising its Supplier Personnel in their compliance with the DPA.
    3. **Employment Management Measures.** Supplier shall protect Seagate Personal Information relating to employment management as provided by Ministry of Health, Labor and Welfare ("MHLW") Employment Management Guidelines.

    4. **Personal Information Learned Through Employment.** Supplier shall ensure that its employees do not divulge or misappropriate the Seagate Personal Information learned through their employment.

    5. **Consent before Transfer or Disclosure.** Supplier shall obtain prior written consent from Seagate before disclosing or transferring national insurance and tax numbers to any third party (including any Affiliate) that is not a party to the DPA, including any Sub-processors.

    6. **Return or Destroy after Purpose Achieved.** Supplier shall stop Processing and return or destroy Seagate Personal Information in its possession when it has achieved the purpose for which it was collected.

    7. **Backup Purposes.** Supplier shall not copy or reproduce Seagate Personal Information except for backup purposes.

3. **SOUTH KOREA**

    1. **Applicability.** The provisions of this Section 3 apply to Seagate Personal Information Supplier receives or accesses from a Seagate Affiliate located in South Korea.

    2. **Limited Access.** Supplier shall limit access to Personal Information to Supplier Personnel who reasonably require such access for the purposes of the Processing.

    3. **Required Safeguards.** Supplier shall establish and maintain safeguards including:

        1. internal procedures for secure handling of Personal Information;

2. technical safeguards such as firewalls, anti-virus and anti-malware software;
3. physical access restrictions, such as locks
4. measures to prevent alteration or falsification of access logs or records of Processing;
5. measures to securely store and transmit Personal Information, such as encryption of Personal Information where required by the Personal Information Protection Act (PIPA), the Enforcement Regulations of PIPA, the Act on Promotion of Information and Communications Network Utilization and Protection of Information (PICNU), the Enforcement Regulations of PICNU ('PICNU Regulations'), the Utilisation and Protection of Credit Information Act (UPCIA) or other Korean law, as applicable.

4. **Encryption of Peculiar Identification Data.** Supplier shall encrypt resident registration numbers, driving licence numbers, and passport numbers when:
    1. transmitted through an information or communications network;
    2. stored on portable storage media or peripherals;
    3. stored on any external computer network, or in a demilitarized zone, or on any personal computer or mobile device; or
    4. stored on Supplier's internal network if Supplier's systems fail to meet Seagate-specified risk criteria.
5. **Encryption of Password and Biometric Data.** Supplier shall encrypt all passwords and biometric data stored in any form.
6. **Information before Disclosure.** Before disclosing or transferring Seagate Personal Information to a third party data processor, the Supplier shall inform Seagate reasonably in advance. Upon Seagate's request, Supplier will provide the following information: (a) the Processing activities to be subcontracted; (b) the identity of the third party data processor; and (c) any changes to (a) or (b).
7. **Training.** Supplier will participate in any training that Seagate may elect to provide to Supplier to safeguard against Seagate Personal Information being

stolen, leaked, altered, or damaged during the course of Processing such Seagate Personal Information.

4. **TAIWAN**

    1. **Applicability.** The provisions of this Section 4 apply to Seagate Personal Information Supplier receives or accesses from a Seagate Affiliate located in Taiwan.

    2. **Sub-Processors.** Notwithstanding Section 2.4 of the DPA, Supplier will not disclose or transfer Seagate Personal Information to, or allow access to Seagate Personal Information to any Sub-processor without Seagate's express written consent.

    3. **Limited Processing Time.** Supplier shall Process the Seagate Personal Information only for the period of time necessary to achieve the purposes of Processing, unless the parties have agreed on a different duration.

    4. **Preserve Access Records.** Supplier shall preserve access records for as long as necessary to ensure they are periodically reviewed for instances of unauthorised access.

SCHEDULE 2

SECURITY STANDARDS

This Schedule represents the minimum security measures that will be taken by Supplier. If any agreement(s) between the parties requires the Supplier to have a higher level or more extensive security measures, the Supplier will abide by those terms. The Supplier must maintain and enforce various policies, standards and processes designed to secure Seagate Personal Information and other data per industry standards, for example NIST Cyber Security Framework and ISO 27001 or 27002, to which Supplier employees are provided access.

1. **Information Security Policies and Standards.** Supplier must implement security requirements for staff and all subcontractors, suppliers, or agents who have access to Seagate Personal Information that are designed to:

    1. Prevent unauthorised persons from gaining access to Seagate Personal Information processing systems (physical access control);

2. Prevent Seagate Personal Information processing systems being used without authorisation (logical access control);
3. Ensure that persons entitled to use a Seagate Personal Information processing system can only gain access to such Seagate Personal Information as they are entitled to access in accordance with their approved access rights and that, in the course of processing or use and after storage Seagate Personal Information cannot be read, copied, modified or deleted without authorisation (data access control);
4. Ensure that Seagate Personal Information cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage, and that the target entities for any transfer of Seagate Personal Information by means of data transmission facilities can be established and verified (data transfer control);
5. Ensure the establishment of an audit trail to document whether and by whom Seagate Personal Information have been entered into, modified in, transferred or removed from Seagate Personal Information processing (entry control);
6. Ensure that Seagate Personal Information is processed solely in accordance with the instructions (control of instructions);
7. Ensure that Seagate Personal Information is protected against accidental destruction or loss (availability control); and
8. Ensure that Seagate Personal Information collected for different purposes can be processed separately (separation control).

The Supplier will conduct periodic risk assessments and review and, as appropriate, revise its information security practices at least annually or whenever there is a material change in the Supplier's business practices that may reasonably affect the security, confidentiality or integrity of Seagate Personal Information, provided that the Supplier will not modify its information security practices in a manner that will weaken or compromise the confidentiality, availability or integrity of Seagate Personal Information.

2. **Physical Security.** The Supplier must maintain commercially reasonable security systems at all Supplier sites at which an information system that uses or houses Seagate Personal Information is located. Supplier reasonably restricts access to such Seagate Personal Information appropriately.

3. **Organisational Security.**
    1. When media are to be disposed of or reused, procedures must be implemented to prevent any subsequent retrieval of any Seagate Personal Information stored on them before they are withdrawn from the inventory. When media are to leave the premises at which the files are located as a result of maintenance operations, procedures must be implemented to prevent undue retrieval of Seagate Personal Information stored on them.
    2. The Supplier must implement security policies and procedures to classify Sensitive Information assets, clarify security responsibilities and promote awareness for employees.
    3. All Seagate Personal Information security incidents must be managed in accordance with appropriate incident response procedures.
    4. Supplier must encrypt, using industry-standard encryption tools, all Sensitive Information in transit and at rest.
4. **Network Security.** Supplier must maintain network security using commercially available equipment and industry-standard techniques, including firewalls, intrusion detection and prevention systems, access control lists and routing protocols.
5. **Access Control.**

1. Supplier must maintain appropriate access controls, including, but not limited to, restricting access to Seagate Personal Information to the minimum number of Supplier Personnel who require such access.
    1. Only authorised staff may grant, modify or revoke access to an information system that uses or houses Seagate Personal Information. Supplier must maintain proper access records, which will be presented to Seagate upon Seagate’s request
    2. User administration procedures must define user roles and their privileges and how access is granted, changed and terminated, address appropriate segregation of duties and define the logging/monitoring requirements and mechanisms.
    3. All employees of Supplier must be assigned unique user-IDs.
    4. Access rights must be implemented adhering to the “least privilege” approach.

5. Supplier must implement commercially reasonable physical and electronic security to create and protect passwords.

6. **Virus and Malware Controls.** Supplier must install and maintain the latest anti-virus and malware protection software on the system and have in place scheduled malware monitoring and system scanning to protect Seagate Personal Information from anticipated threats or hazards and protect against unauthorised access to or use of Seagate Personal Information.

7. **Personnel.** Prior to providing access to Seagate Personal Information to Supplier Personnel, the Supplier must require Supplier Personnel to comply with the Supplier's information security programme. The Supplier must implement a security awareness programme to train personnel about their security obligations. This programme will include training about data classification obligations, physical security controls, security practices, and security incident reporting. The Supplier will have clearly defined roles and responsibilities for the employees. Screening will be implemented before employment with terms and conditions of employment applied appropriately. Supplier employees must strictly follow established security policies and procedures. A disciplinary process must be applied if employees commit a Data Privacy Breach.

8. **Business Continuity.** The Supplier implements appropriate back-up and disaster recovery and business resumption plans. The Supplier reviews both business continuity plans and risk assessments regularly. Business continuity plans are being tested and updated regularly to ensure that they are up to date and effective.

9. **Primary Security Manager.** The Supplier must notify Seagate of its designated primary security manager. The security manager will be responsible for managing and coordinating the performance of Supplier's obligations set forth in Supplier's information security program and in this DPA.

10. **Audit.** Seagate reserves the right to audit Supplier commitments as stated in this Schedule 2, in accordance with section 4.4 "Audit" of this DPA

11. **Breach.** If it is determined the Supplier is in breach of this DPA, the Supplier must remediate any such breach without undue delay and in any event within 30 calendar days. Any known or suspected Data Privacy Breach shall be governed by section 5. "Supplier Responsibilities After a Data Privacy Breach" of this DPA.