For agreements completed prior to March 31, 2019.

DATA PROTECTION REQUIREMENTS

1. **DEFINITIONS**

    1. **Personal Information.** “Personal Information" means any information that identifies or may be used to identify a natural person or that otherwise relates to an identified or identifiable natural person. Examples of Personal Information include, but are not limited to:

        1. name, address, phone number, fax number, email address;
        2. social security number, taxpayer identification number, passport number, driver’s license number, or other government-issued identification number;
        3. credit or debit card details, financial account number, codes or passwords that would permit access to account or credit histories;
        4. race, religion, ethnicity, sex life or practices, or sexual orientation;
        5. medical or health information, genetic or biometric information, biometric templates,
        6. political or philosophical beliefs, political party membership, trade union membership;
        7. background check information or judicial data such as criminal records or information on other judicial or administrative proceedings.

    2. **Processing.** “Process” or “Processing” means, without limitation, operations performed on Seagate Data, such as collecting, recording, organizing, structuring, altering, using, accessing, disclosing, copying, transferring, storing, deleting, combining, restricting, adapting, retrieving, consulting, destroying, disposing, or using Personal Information.
    3. **Seagate Data.** “Seagate Data” means any data, including Personal Information, intellectual property, trade secrets, or other data, created, owned, or provided by Seagate or for Seagate, that Supplier has access to, obtains, uses, maintains, or Processes in connection with the Agreement.
    4. **Subcontractor.** A “Subcontractor” means any third party engaged by Supplier or by any other subcontractor who will have access to, receive, or otherwise Process any Seagate Data.

2. **DATA SECURITY AND PROTECTION**

    1. **Nondisclosure of Seagate Data.** Supplier shall not disclose Seagate Data in any manner for any purpose to any third party without obtaining prior written authorization from Seagate. Supplier shall implement appropriate technical, organizational, and physical security measures to protect Seagate Data, as specified in the Security Requirements set forth below.

    2. **Limitations on Processing.** Supplier shall only Process Seagate Data to provide the applicable services and/or deliverables to Seagate in accordance with the Agreement. Supplier shall not Process or permit the Processing of Personal Information except in accordance with the documented instructions of Seagate. Supplier shall not Process after termination or expiration of the Agreement, except as otherwise directed by Seagate.

    3. **Restrictions on Subcontractors.** Supplier shall maintain a list of the Subcontractors to which it discloses Seagate Data, and will provide this list to Seagate upon Seagate's request. Supplier shall notify Seagate at least **30 days** before adding any Subcontractor to the list. If Seagate objects to any Subcontractor having access to Seagate Data, then Supplier shall not disclose Seagate Data to the Subcontractor. If Supplier cannot provide the Services without disclosing Seagate Data to the Subcontractor, then Seagate may terminate the Agreement without cost or liability owed to Supplier.

    4. **Subcontractor Compliance and Breach.** Supplier shall ensure that its Subcontractors comply with the terms of this Exhibit. Supplier's use of Subcontractors does not reduce Supplier's obligation to comply with this Exhibit. Supplier will be liable to Seagate for breaches of this Exhibit by its Subcontractors to the same extent as if Supplier breached this Exhibit.

    5. **Obligations of Supplier Personnel and Subcontractors.** Supplier shall ensure that any person or Subcontractor who has access to Seagate Data is bound by written privacy and data protection agreements at least as restrictive as those in this Exhibit. Supplier shall ensure that the privacy and data protection obligations continue after the term of their employment or engagement.

    6. **Limited Access.** Supplier shall limit access to Seagate Data to persons or Subcontractors, who require access for Supplier to perform its obligations under the Agreement, who have been trained on data protection and security

requirements, and who have agreed to comply with data confidentiality requirements during and after their activities for Seagate.

7. **Notice of Requests or Complaints.** Unless prohibited by law, Supplier shall notify Seagate within **2 days** after receiving any request or complaint relating to Processing Personal Information, including
    1. requests from an individual for data portability, requests to access, change, delete, or restrict, and similar requests; or
    2. complaints or allegations that the Processing infringes on an individual's rights.
8. **Supplier Responses.** Supplier shall not respond to any request or complaint unless expressly authorized to do so by Seagate. 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.
9. **Requests for Disclosure.** Unless prohibited by law, Supplier shall immediately notify Seagate if Supplier receives any document requesting or purporting to compel the disclosure of 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, Supplier will not respond. If a Disclosure Request is binding, 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. Supplier shall exercise reasonable efforts to prevent and limit any disclosure and to preserve the confidentiality of 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 Personal Information.
10. **Cooperation.** Supplier shall provide relevant information and assistance requested by Seagate to demonstrate Supplier's compliance with its obligations under this Exhibit. Supplier shall assist Seagate in meeting its obligations under data protection laws regarding (a) registration and notification; (b) accountability; (c) ensuring the security of the Personal Information; and (d) the carrying out of

privacy and data protection impact assessments and related consultations of data protection authorities.

11. **Participation in Regulatory Investigations.** Supplier shall assist and support Seagate in any investigation by any regulator to the extent the investigation relates to Seagate Data handled by Supplier.

12. **Notice of Potential Violations or Inability to Comply.** Supplier shall immediately notify Seagate if:

    1. Supplier has reason to believe that any instructions from Seagate regarding Processing 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 Exhibit and it cannot cure this inability to comply within a reasonable timeframe; or

    3. Supplier becomes aware of any circumstances or changes in applicable law that are likely to prevent it from fulfilling its obligations under this Exhibit.

13. **Suspension or Adjustments for Compliance.** Seagate may suspend Supplier's Processing of Personal Information to prevent potential violations or noncompliance. Supplier shall cooperate with Seagate to adjust the Processing to remedy any potential violation or noncompliance. If adjustment is not possible, Seagate may terminate the Agreement, without cost or liability owed to Supplier.

3. **DATA TRANSFERS**

1. **European Economic Area Standard Clauses.** If Supplier transfers or Processes Personal Information received from within the European Economic Area ("EEA") to outside the EEA, then the Standard Contractual Clauses, provided separately ("Standard Clauses"), will apply in addition to the terms in this Exhibit. Supplier shall ensure that any Subcontractors also execute the Standard Clauses.

2. **Privacy Shield.** "Privacy Shield" means the EU-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.

3. **Privacy Shield Certification.** If Supplier has certified to the Privacy Shield, Supplier shall maintain its certification to the Privacy Shield for the duration of the Agreement. If Supplier is authorized by Seagate to subcontract, Supplier shall enter into an appropriate onward transfer agreement with any such Subcontractor 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 Personal Information pursuant to a Privacy Shield certification. Seagate may take any reasonable actions to stop or remediate the unauthorized Processing, including terminating the Agreement, without cost or liability owed to Supplier.

4. **Other Jurisdiction Provisions.** Supplier shall comply with the Requirements for Specific Jurisdictions provided below as Schedule 1 for requirements related to specific jurisdictions.

4. **COMPLIANCE AND ACCOUNTABILITY**

1. **Compliance.** Supplier shall annually review Supplier's and Subcontractors' practices to ensure they comply with this Exhibit and with all applicable laws. Supplier shall ensure that the Processing of Seagate Data complies with all applicable laws, self-regulatory frameworks, and contract requirements applicable to Supplier. 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 Exhibit.

2. **Audit.** Seagate may audit Supplier's practices related to this Exhibit. Supplier shall remedy any non-compliance within a reasonable amount of time. Seagate may take any reasonable actions to stop or remediate any non-compliance, including terminating the Agreement, without cost or liability owed to Supplier.

5. **SUPPLIER RESPONSIBILITIES AFTER A SECURITY BREACH**

1. **Security Breach.** A "Security Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, access to, acquisition of Seagate Data, or any other unauthorized Processing of Seagate Data, including Personal Information.

2. **Notification of Security Breach.** Supplier shall notify Seagate in writing of a known or suspected Security Breach within **24 hours** after first learning of the potential Security Breach, and shall immediately:

1. notify Seagate at data.protection.officer@seagate.com of the Security Breach;
2. investigate or provide required assistance in the investigation of the Security Breach;
3. provide Seagate with detailed information about the Security Breach;
4. take all commercially reasonable steps to mitigate the effects of the Security Breach, or assist Seagate in doing so; and
5. implement a remediation plan and monitor the resolution of breaches and vulnerabilities related to Seagate Data to ensure that appropriate corrective action is taken on a timely basis.

3. **Containment and Remedy.** Supplier shall immediately contain and remedy any Security Breach and prevent any further Security Breach; and Supplier shall take all actions necessary to comply with applicable privacy rights, laws, regulations, and industry standards.
4. **Communications.** Supplier shall not issue any communications related to a Security Breach, in any manner that would identify, or is reasonably likely to identify or reveal the identity of, Seagate, without Seagate's prior approval.
5. **Preservation of Evidence.** Following discovery of a Security Breach, Supplier shall preserve evidence related to the breach and maintain a clear chain of command according to an incident response plan.
6. **Cooperation.** 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 Personal Information.
7. **Indemnification.** Supplier shall defend and indemnify Seagate against any third party claims related to a Security Breach to the extent the Security Breach resulted from an act or omission of Supplier or a Subcontractor. Supplier shall pay or reimburse Seagate for all fines, penalties, and costs, including Seagate's reasonable attorneys' fees, out-of-pocket expenses, and investigation costs, related to any Security Breach (including, without limitation, Seagate Data breaches), including any costs associated with: (a) providing notifications determined by Seagate to be reasonably necessary or required by law; (b) establishing communications procedures in response to the Security Breach; and

(c) providing individuals affected by the Security Breach with a minimum of **1 year** of credit monitoring.

6. **RETURN AND SECURE DELETION OF SEAGATE DATA**

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

    2. **Return and Deletion of Seagate Data.** Upon the earlier of (a) request by Seagate or (b) the expiration or earlier termination of the Agreement, Supplier shall export the Seagate Data or provide Seagate or its third party designee with the ability to export all Seagate Data in a machine readable and interoperable format determined by Seagate. After the termination or expiration of the Agreement, Supplier shall maintain the Seagate Data for as long as Seagate determines is reasonably necessary to allow Seagate to fully access and export the Seagate Data at no cost to Seagate. Each party shall identify a contact person to migrate the Seagate Data and shall work promptly, diligently, and in good faith to facilitate a timely transfer. Within **90 days** after Seagate confirms that Seagate Data was received and migrated correctly, Supplier shall securely destroy all Seagate Data, delink Seagate's workspace identifiers, and overwrite with new data or otherwise destroy the Seagate Data through an approved sanitization method.

    3. **Destroy Old Hard Drives.** If Supplier decommissions or otherwise retires a drive that contains a copy of Seagate Data then Supplier shall securely shred or destroy the drive rendering the Seagate Data unreadable and destroyed. Supplier shall certify in writing that the drive has been shredded or destroyed and that that the Seagate Data cannot be read, retrieved, or otherwise reconstructed.

    4. **Notice of Any Retention.** If Supplier has a legal obligation to retain Seagate Data beyond the period otherwise permitted by this Exhibit, Supplier shall notify Seagate in writing of its obligation, and shall return or destroy the Seagate Data as soon as possible after the retention period ends.

    5. **Documentation.** Supplier shall document its retention or disposal of Seagate Data pursuant to this Exhibit. Upon Seagate's request, Supplier shall provide a

written certification that Seagate Data has been returned or securely destroyed in accordance with this Exhibit.

7. **MISCELLANEOUS**

    1. **Order of Precedence.** In case of discrepancies between this Exhibit and the Agreement or any other agreement between Seagate and Supplier, the provisions of this Exhibit will prevail. If there are any discrepancies between this Exhibit and the Standard Clauses, the provisions of the Standard Clauses will prevail.

    2. **Third Party Beneficiaries.** Seagate's affiliates are intended third-party beneficiaries of this Exhibit; and may enforce the terms of this Exhibit as if each was a signatory to the Agreement. Seagate also may enforce the privacy and data security provisions on behalf of its affiliates, instead of its affiliates separately bringing a cause of action against Supplier.

    3. **Disclosure of Exhibit to Regulators.** Seagate may provide a summary or a copy of the privacy provisions in this Exhibit to any regulator.

SECURITY REQUIREMENTS

DATA SECURITY

1. **Information Security Program.** Supplier will establish, implement, and maintain an information security program that includes technical and organizational security and physical measures as well as policies and procedures to protect Seagate Data Processed by Supplier accidental, unauthorized, or unlawful destruction or loss, alteration, unauthorized disclosure or access, or other unauthorized Processing. Supplier's information security program must reasonably address the confidentiality, integrity, and availability of all Seagate Data, including the below matters and any other requirements specified in this Exhibit:

    1. Periodic risk assessments.

    2. Identify and document the security requirements of authorized users.

    3. User access, the nature of that access, and authorization of access.

    4. Prevent unauthorized access through the use of effective physical and logical access controls, including but not limited to, the physical security measures specified in this Exhibit.

5. Procedures to add new users, modify access levels of existing users, and removal of users who no longer need access.
6. Assign responsibility and accountability for security, system changes, and maintenance.
7. Implement system software upgrades and patches, including a patching interval of less than 90 days for security-impacting patches and less than 15 days for critical patches.
8. Test, evaluate, and authorize system components before implementation.
9. Resolve complaints and requests relating to security issues.
10. Handle errors and omissions, Security Breaches, and other incidents.
11. Procedures to detect actual and attempted attacks or intrusions into systems and to proactively test security procedures (for example, penetration testing).
12. Allocate training and other resources to support its security policies.
13. Provision for handling exceptions and situations not specifically addressed in its security process.
14. Processing integrity and related system security policies.
15. A requirement that users, management, and third parties confirm (initially and annually) their understanding of an agreement to comply with the applicable privacy policies and procedures related to the security of Seagate Data.
16. Procedures for proper destruction and disposal of Seagate Data.

2. **Environment.** Supplier will securely collect, host, transmit, and store the Seagate Data. Supplier will provide the Services using no less than industry standard physical and environmental security measures to prevent unauthorized access to, theft of, or unlawful disclosure of the Seagate Data. Supplier will employ technologies that are consistent with industry standards for firewalls and other security technologies. Supplier will notify Seagate of each location for storing or Processing Seagate Data. Supplier warrants that Seagate Data will not be commingled with data from other companies.
3. **Secure Data Transfers.** To protect Seagate Data during electronic transmission, Supplier will use Transport Layer Security (TLS) standards. In addition, Supplier will

maintain at a minimum the following security measures when encrypting Seagate Data: HTTP with SSL 256-bit encryption (HTTPS); the ability to transfer files via Secure File Transfer Protocol (SFTP); at least 256-bit AES encryption of files and encode data during transmission; and encrypted passwords for hosting services.

4. **Data Integrity.** Supplier will maintain the Seagate Data in a file format approved by Seagate, such as flat file, relational database management system, spreadsheet, ASCII, XML, original format. Supplier may maintain the Seagate Data in Supplier's own format, if approved by Seagate. Supplier must support tape formats or applicable media. Supplier will regularly test and validate the integrity of the Seagate Data.

5. **Recoverability.** Supplier will comply with Seagate requests to produce the Seagate Data in response to Seagate or third party audits, incident or investigation requests by Seagate, or as required by law. Supplier will cooperate with Seagate to test the recoverability of the Seagate Data from Supplier's systems and Supplier's backups, upon Seagate's request.

6. **Compliance.** Supplier will provide reports on standards and controls compliance specific to the service provided: International Standards Organization (ISO) 27001 or 27002, Certified Public Accountants (AICPA) Statements on Standards for Attestation Engagements (SSAE) 16 Type II, or other similar report. The report(s) will be provided at least annually upon request from Seagate, and must be from an audit firm reasonably acceptable to Seagate. Supplier will give Seagate a full copy of the certification and report on which the certification is based. Upon written request from Seagate, Supplier will also give Seagate a management representation letter stating that, to the knowledge of Supplier management after reasonable investigation, there have been no changes to the control environment between the date of the management representation letter and the date of the certification. No more than **ninety (90) days** may pass between the period covered by the tests of controls and the delivery of the certification report.

7. **Audit and Test.** Seagate may audit or have a third party audit the processes, control, privacy, and security of the data centers, application, and network infrastructure from which Supplier provides the Services to ensure compliance with Seagate's security policies and standards. This audit right includes examining the security practices of Supplier's connection to any of its datacenters involved in providing the Services (for example, developer account security protocols). Seagate may conduct non-intrusive network audits (basic port scans, etc.) randomly without prior notice. Seagate will not attempt to access the data of another Supplier customer. Seagate may perform any

technical security integrity review, penetration test, load test, denial-of-service simulation or vulnerability scan with Supplier's prior written consent.

8. **Mitigation of Vulnerabilities.** Supplier will aggressively mitigate any critical security vulnerabilities discovered at any time. Seagate may require Supplier to disclose specific configuration files for web servers and associated support functions (such as search engines or databases). Any configuration files disclosed to Seagate are Supplier confidential information.
9. **Business Continuity Plan.** Supplier will establish, implement, test, and maintain an effective business continuity plan (including without limitation disaster recovery and crisis management procedures) to provide Seagate with continuous access to and support for the Services. Supplier will ensure that backup and disaster-recovery planning processes protect Seagate Data from unauthorized use, access, disclosure, alteration, or destruction.
10. **Backups and Archives.** On a daily basis, Supplier will backup, archive, and maintain duplicate or redundant systems that can fully recover all Seagate Data. Supplier will establish and follow procedures and frequency intervals for transmitting backup data and systems to Supplier's backup location. Supplier will maintain the backup storage and systems in a secure physical location other than the location of Supplier's primary systems. Supplier will update and test the backup storage systems at least annually. Upon written request, Supplier will provide Seagate with a summary of Supplier's business continuity plan and will permit Seagate to participate in disaster recovery exercises. Supplier will incorporate any reasonable modifications required by Seagate into the business continuity plan in a timeframe mutually agreed to by Seagate and Supplier. Supplier will backup Seagate Data with incremental backups at least daily and will complete one backup at least weekly. If the original Seagate Data is lost or corrupted, Supplier will reconstruct the Seagate Data from the backup data within 2 hours.
11. **Controlled Access.** Supplier is responsible for preventing physical access to any areas hosting the Seagate Data, except for Supplier's employees who have a need to access the physical area.
12. **Network Security.** Supplier will configure all network infrastructure to enforce the "principle of least access," including filters that allow only the minimum required traffic, anti-spoofing filters, and network ingress and egress filters.

13. **Hardening Documentation.** Upon written request, Supplier will provide Seagate with the hardening documentation used to secure Servers hosting the Seagate application and Seagate Data.

14. **Host Monitoring.** Upon written request, Supplier will disclose the processes for monitoring the integrity and availability of the hosts.

15. **Passwords.** Supplier will store any passwords within a secured database server, using industry standard security measures behind Supplier's firewall. Supplier will use Secure Hash Algorithm 2 (SHA-2) or higher to scramble or hash the database password. Supplier's system must require this password upon application startup to connect to the database.

16. **Web Security.** Supplier will provide Seagate with the process for doing security-specific quality assurance testing for the application, for example, testing of authentication, authorization, and accounting functions, as well as any other activity designed to validate the security architecture.

17. **Encryption Algorithms.** Supplier will use cryptographic algorithms that have been published and evaluated by the general cryptographic community. Supplier will use encryption algorithms that are sufficient strength to equate to 256-bit or better. Supplier may use hashing functions SHA-2 or higher. Supplier will not use any "homegrown" cryptography, such as symmetric, asymmetric, or hashing algorithm.

18. **Encryption Key Management.** Supplier will provide encryption key management. Supplier will protect private keys in storage, transit, and backup. Supplier will segregate the encryption key and encryption key management process from any hosts that store and Process the data. Supplier will provide Seagate with documentation of its security controls for the secure key management. Supplier will provide an effective key destruction technique, such as crypto shredding, to ensure that the encryption keys are destroyed and unrecoverable after the Agreement is terminated.

19. **Identity Provisioning and Deprovisioning.** Supplier will provide a secure and timely management of on-boarding and off-boarding of cloud service users. Supplier will use standard APIs, such as Simple Cloud Identity Management.

20. **Federation.** Supplier will use Seagate's Single Sign-on mechanisms which include the SAML v2 federation standard.

21. **Strong Authentication.** Supplier will use two-factor authentication and certificates to authenticate their remote administrators who manage their cloud services, or an alternative strong authentication method provided it has received prior approval from Seagate.

22. **Authorization and Access Controls.** Supplier will maintain a policy and role-based access controls to log user access information for compliance, audit, and incident investigation purposes. Supplier will use standards such as OAUTH v2 to avoid becoming locked into one authorization method.

DATA BREACH

23. **Supplier Responsibilities.** Refer to Data Protection Requirements above for Supplier responsibilities and following a breach of Seagate Data.

BACKGROUND CHECKS AND SITE/SYSTEM ACCESS

24. **Background Checks.** Supplier certifies in writing, certification attachment to be provided separately, that it performs background checks on all personnel who will have access to Seagate Data, which, as of the date of this Agreement, includes criminal history, reference verification, work, and education validation and OFAC. Seagate reserves the right to review Supplier practices and audit completed pre-employment screening processes to ensure these standards are met. Additionally, personnel onsite at a Seagate location shall comply with Seagate's policies, procedures and guidelines.

25. **Access Restrictions.** Supplier shall not allow any person with conviction for theft, violence, or narcotics related offenses to have access to Seagate Data, systems, or networks used to provide the Services, or to have unescorted access to the physical sites used to provide the Services, unless otherwise prohibited by applicable law or regulations. Seagate may conduct, at its option and cost, all background screenings for Supplier personnel who need access to Seagate's systems, network, or physical site through a licensed Credit Reporting Agency in compliance with all applicable laws and regulations, including to the Fair Credit Reporting Act and data protection and privacy regulations, when acting pursuant to this section. Seagate shall maintain the confidentiality of the reports it reviews.

SCHEDULE 1

DATA PROTECTION REQUIREMENTS FOR SPECIFIC JURISDICTIONS

The following requirements apply to the jurisdictions specified:

1. **AUSTRALIA**

    1. **Membership of a Professional or Trade Association.** The term "Personal Information" also includes Personal Information about an individual's membership of a professional or trade association.

    2. **Anonymity/Pseudonymity.** Where the Supplier is informed that the Data Subject wishes to be dealt with on an anonymous or pseudonymous basis, Supplier shall handle the request in accordance with applicable law.

    3. **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.

    4. **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.

2. **JAPAN**

    1. **Employment Management Measures.** Supplier shall protect Personal Information relating to employment management as provided by Ministry of Health, Labor and Welfare ("MHLW") Employment Management Guidelines.

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

    3. **Consent before Transfer or Disclosure.** Supplier shall obtain prior written consent from Seagate before disclosing or transferring Personal Information to any third party (including any Affiliate) that is not a party to this Agreement.

4. **Return or Destroy after Purpose Achieved.** Supplier shall stop processing and return or destroy Personal Information in its possession when it has achieved the purpose for which it was collected.
5. **Backup Purposes.** Supplier shall not copy or reproduce Personal Information except for backup purposes.

3. **SOUTH KOREA**
    1. **Limited Access.** Supplier shall limit access to Personal Information to Supplier personnel who reasonably require such access for the purposes of the Processing.
    2. **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 Utilization and Protection of Credit Information Act (UPCIA) or other Korean Law.
    3. **Encryption of Peculiar Identification Data.** Supplier shall encrypt resident registration numbers, driver's license 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

4. stored on Supplier's internal network if Supplier's systems fail to meet Seagate-specified risk criteria.

4. **Encryption of Password and Biometric Data.** Supplier shall encrypt all passwords and biometric data stored in any form.

5. **Information before Disclosure.** Before disclosing or transferring Personal Information to a third party data processor, 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).

4. **TAIWAN**

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

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