DATA PROTECTION AGREEMENT

This Data Protection Agreement ("DPA") governs SonicWall's processing of your Data.

1. **DEFINITIONS**

(a) "**Appropriate Safeguards**" means such legally enforceable mechanism(s) for transfers of Data as may be permitted under Data Protection Laws from time to time.

(b) "**Data**" has the meaning given to 'personal data' in Data Protection Laws and only includes that data Processed by SonicWall in the provision of hosted products or services under an agreement with SonicWall and the this DPA.

(c) "**Data Breach**" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Data.

(d) "**Data Controller**" has the meaning given to that term (or to the term 'controller') in Data Protection Laws.

(e) "**Data Processor**"has the meaning given to that term (or to the term 'processor') in Data Protection Laws.

(f) "**Data Subject**" has the meaning given to that term in Data Protection Laws.

(g) "**Data Protection Laws**" means any applicable law in the Member States of the European Union relating to the Processing, privacy and use of Data, as applicable to you, SonicWall and/or the services under this DPA, including: the EU General Data Protection Regulation 2016/679 (the Regulation) on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data, and/or any corresponding or equivalent national laws or regulations, as amended or superseded from time to time, and/or the ePrivacy Directive 2002/58/EC (the Directive), and/or any corresponding or equivalent national laws or regulations, as amended or superseded from time to time; and, any judicial or administrative interpretation of the Regulation and the Directive, any guidance, codes of practice, approved codes of conduct or approved certification mechanisms issued by any relevant data protection regulator responsible for administering Data Protection Laws.

(h) "**Processing**", "**Processed**" or "**Process**" has the meanings given to that term in Data Protection Laws (and related terms such as process have corresponding meanings).

(i) "**SonicWall Personnel**" means SonicWall and/or any employee of SonicWall, acting on behalf of SonicWall or under the apparent authority of SonicWall in providing products and/or services. References to "SonicWall" herein include SonicWall Personnel.

(j) "**SonicWall"** means SonicWall Inc. or any affiliated entity of SonicWall Inc.

(k) "**Subcontractors**" means any third person or entity, including all subcontractors, acting for or on behalf of SonicWall, providing products and/or services to you. "Subcontractors" does not include employees of SonicWall.

(l) "**Sub-Processor**" means another Data Processor engaged by SonicWall for carrying out processing activities in respect of the Data on behalf of the Customer.

2. **SONICWALL OBLIGATIONS**

(a) **Scope**. Unless required to do otherwise under Data Protection Laws or other applicable laws, you instruct and SonicWall undertakes to (and shall ensure each person acting under its authority shall) Process Data for the sole and exclusive purpose of performing SonicWall's obligations to you under and in accordance with (1) an agreement with SonicWall and this DPA; (2) your documented instructions as set out in Appendix 1 (Processing Instructions), and otherwise as instructed by you in writing from time to time. If any applicable laws require SonicWall to Process Data other than in accordance with your instructions SonicWall shall notify you of any such requirement before Processing the Data (unless any applicable laws prohibit such information on important grounds of public interest), and; (3) privacy laws. You undertake, represent and warrant to SonicWall that your instructions and actions with respect to the Data, including its appointment of SonicWall as another processor, have been authorized by the relevant controller prior to such Data being provided to or accessed by the SonicWall under this DPA. You shall comply in all respects, including in terms of its collection, storage and processing (which shall include the providing all of the required fair processing information to, and obtaining all necessary consents from data subjects, with Data Protection Laws.

(b) **Disclosure**. SonicWall shall not transfer or otherwise disclose Data to, or permit Processing by, its Personnel or Subcontractors except (1) on a need-to-know-basis related to the provision of products and/or services; (2) to the extent necessary to provide the products and/or services; (3) as permitted under an agreement with SonicWall; or (4) if required by applicable privacy law.

(c) **Destruction and Return**. Upon termination of the agreement or upon written request from you, whichever comes first, SonicWall shall, and shall ensure that its Subcontractors, immediately cease all use of and securely return to you or, at your direction, securely dispose of or destroy, or render permanently anonymous all such Data remaining in its control, in each case using the security measures set out herein;

existing copies of Data shall be securely deleted (unless storage of Data is required by any applicable laws, and if so SonicWall shall inform you of such a requirement). You are responsible for backing up data before Data is deleted. If, in SonicWall's discretion, it does not believe applicable law permits SonicWall to destroy the Data or copies of it, SonicWall shall not use the Data for any purpose other than as required by the applicable law and shall remain bound by the provisions of the applicable law.

(d) **Notifications and Assistance**. If SonicWall is contacted by a person with a request, inquiry or complaint regarding their Data in connection with the products and/or services, SonicWall will and your cost and expense (1) provide you with written notice of such request, inquiry or complaint using the contact information you provided for such purpose; and (2) provide you all reasonable cooperation, assistance, information and access to Data in its possession, custody or control as is necessary for you to respond to such request, inquiry or complaint promptly and within reasonable timescales and any timeframe required by Data Protection Laws or other Privacy Laws. SonicWall shall not respond to such request, inquiry or complaint unless so instructed in writing by you. SonicWall shall provide such cooperation, assistance, information and access as you may reasonably require in ensuring your obligations under Data Protection Laws, including with respect to: security of Processing; data protection impact assessments (as defined in the Regulation and Data Protection Laws); prior consultation with a data protection regulator responsible for administering Data Protection Laws regarding high risk Processing; and, any remedial action and/or notifications to be taken in response to any Data Breach and/or complaint, including (subject in each case to SonicWall's prior written authorization) regarding any notification of the Data Breach to a data protection regulator responsible for administering Data Protection Laws and/or communication to any data subjects. .

3. **YOUR OBLIGATIONS**

(a) You will comply with all Data Protection Laws in the processing of Data, the products and services you obtain from SonicWall and the exercise and performance of your respective rights and obligations under this DPA, including maintaining all relevant regulatory registrations and notifications as required under Data Protection Laws, and the provisions of this DPA. You represent, warrant, and agree that:

(1) all Data sourced by you for use in connection with this DPA, shall comply in all respects, including in terms of its collection, storage and processing (which shall include that you provide all of the required fair processing information to, and obtaining all necessary consents from, Data Subjects), with Data Protection Laws;

(2) all instructions given by you to SonicWall in respect of Data shall at all times be in accordance with Data Protection Laws; and

(3) you are satisfied that SonicWall's processing operations are suitable for the purposes for which you propose to use the products and services and engage SonicWall to process the Protected Data

(4) you will not unreasonably withhold, delay or condition your agreement to any change reasonably requested by SonicWall in order to ensure SonicWall (and each Sub-Processor) can comply with Data Protection Law.

(b) Provided you pay SonicWall's fees, calculated on a time and materials basis (Charges):

(1) SonicWall will promptly refer all Data Subject requests it receives to you, for recording and referring the Data Subject requests in accordance with this Section, and;

(2) provide such reasonable assistance as you may reasonably require (taking into account the nature of processing and the information available to SonicWall) to ensure compliance with your obligations under Data Protection Laws with respect to security of processing; data protection impact assessments (as such term is defined in Data Protection Laws), prior consultation with a supervisory authority regarding high risk processing; and notifications to the supervisory authority and/or communications to Data Subjects by you in response to any Data Breach.

4. **INFRASTRUCTURE SECURITY & CONNECTIVITY**

SonicWall shall have and maintain, at its cost and expense, Appropriate Safeguards. If (a) the products and/or services include application, website, Data or system hosting; (b) network connectivity is required to provide the products and/or services; or (c) the products and/or services are dependent on the integrity of SonicWall's environment, SonicWall shall ensure that the connection and mechanism to transmit Data between SonicWall and you shall be through a secure solution. Duration of access shall be restricted to only when access is required.

5. **DATA BREACH**

In respect of any Data Breach involving Protected Data, SonicWall shall, without undue delay:

(a) notify you of the Data Breach; and

(b) provide you with details of the Data Breach.

SonicWall shall promptly inform you if SonicWall becomes aware of a processing instruction that, in SonicWall's opinion, infringes Data Protection Laws, provided that to the maximum extent permitted by mandatory law, SonicWall shall have no liability, howsoever arising,

whether in contract, tort (including negligence) or otherwise for any losses, costs, expenses or liabilities (including any Data Protection Losses) arising from or in connection with any processing in accordance with your processing instructions following notification to you of that information using the contact information in this DPA. SonicWall shall be liable only for losses related to a Data Breach (howsoever arising, whether in contract, tort (including negligence) or otherwise) under or in connection with this DPA (a) only to the extent caused by the processing of Data under this DPA and directly resulting from the SonicWall's breach of this DPA, and (b) in no circumstances to the extent that any Data Breach losses (or the circumstances giving rise to them) are contributed to or caused by any breach of this Agreement by you. If a party receives a compensation claim from a person relating to processing of Data, it shall promptly provide the other party with notice and full details of such claim. The party with conduct of the action shall (a) make no admission of liability nor agree to any settlement or compromise of the relevant claim without the prior written consent of the other party (which shall not be unreasonably withheld or delayed), and (b) consult fully with the other party in relation to any such action, but the terms of any settlement or compromise of the claim will be exclusively the decision of the party that is responsible under this DPA for paying the compensation.

6. **PERSONNEL & SUBCONTRACTORS**

You consent to SonicWall's existing Sub-processors as at the date of this DPA, which are listed at www.sonicwall.com ("Sub-processor List"). SonicWall will not subcontract the processing of any Data to any additional Sub-processors (each a "New Sub-processor") without your written consent. SonicWall will provide prior written notice of additional New Sub-processor(s) (including general details of the processing it performs or will perform), by posting details to the Sub-processor List. If you do not object in writing to SonicWall's appointment of a New Sub-processor (on reasonable grounds relating to the protection of Data) within 30 days of SonicWall adding the New Sub-processor to the Sub-processor List, you agree that it will be deemed to have consented to that New Sub-processor. If you provide such a written objection to SonicWall, SonicWall will notify you within 30 days that either: (i) SonicWall will not use the New Sub-processor to process the Data; or (ii) SonicWall is unable or unwilling to do so. If the notification described in part (ii) is given, you may, within 30 days of such notification, elect to terminate this DPA and your agreement with SonicWall upon written notice to SonicWall. However, if no such notice of termination is provided within that timeframe, you will be deemed to have consented to the New Sub-processor. SonicWall shall take reasonable steps to ensure the reliability of SonicWall Personnel and Subcontractors that have access to Data. SonicWall will maintain a list of Sub-processors and will add the names of new and replacement Sub-processors to the list prior to them starting sub-processing of Data. SonicWall will ensure that all persons under the authority of SonicWall Processing Data (including SonicWall Personnel and any Subcontractors sub-Processing Data) are subject to a written binding contractual obligation with SonicWall with restrictions substantially similar to those under this DPA and appropriate confidentiality obligations (except where such disclosure is required in accordance with any applicable laws, in which case SonicWall will, where practicable and not prohibited by any applicable laws, notify you of any such requirement before such a disclosure). Written agreements with Subcontractors Processing Data will include Appropriate Safeguards. SonicWall shall have sole liability for the performance of those Subcontractors' Data protection obligations including all acts or omissions of Subcontractors.

7. **RECORDS, INFORMATION AND AUDITS**

SonicWall shall maintain, in accordance with Data Protection Laws binding on SonicWall, written records of all categories of processing activities carried out on behalf of you. SonicWall shall, in accordance with Data Protection Laws, make available to you such information as is reasonably necessary to demonstrate its compliance with its obligations under Article 28 of the GDPR (and under any Data Protection Laws equivalent to that Article 28), and allow for and contribute to audits, including inspections, by you (or another auditor mandated by the Customer) for this purpose, subject to you:

(a) giving SonicWall reasonable prior notice of such information request, audit and/or inspection being required by you;

(b) ensuring that all information obtained or generated by you or your auditor(s) related to such information requests, inspections and audits is kept strictly confidential (save for disclosure to the Supervisory Authority or as otherwise required by Applicable Law);

(c) ensuring that such audit or inspection is undertaken during normal business hours, with minimal disruption to SonicWall's business, the Subcontractor's business and the business of other customers of SonicWall; and

(d) paying SonicWall's reasonable costs for assisting with the provision of information and allowing for and contributing to inspections and audits.

8. **INTERNATIONAL TRANSFERS**

SonicWall may transfer Data from EEA countries to countries outside the EEA using Appropriate Safeguards, provided that such transfer is required in the provision of products and/or services. SonicWall shall ensure that all such transfers by SonicWall of Data are in accordance with this DPA, applicable Data Protection Laws and the provisions set forth in Appendix 1 and 2 attached to this DPA.

9. **MISCELLANEOUS**

SonicWall's obligations under this DPA shall survive the termination or expiration of the DPA. Legal notices shall be made in writing to the address provided under this DPA. You may not assign the DPA without SonicWall's consent. This DPA sets forth the entire agreement and understanding of the parties relating to the subject matter herein, and replaces all prior or contemporaneous discussions and agreements between the parties, both oral and written. In performing SonicWall's responsibilities pursuant to this DPA, it is understood and agreed that SonicWall is acting as an independent contractor and that SonicWall is not your partner, joint venturer, or employee.

SONICWALL By:_____ Printed Name:_____ Title:_____ Date:_____	Company:_____ By:_____ Printed Name:_____ Title:_____ Date:_____ Notification Address:_____ Notification E-mail:_____

Please print this document, provide the information requested, and have the DPA signed by an authorized representative of the company. Send a copy of the executed DPA to dataprivacy@sonicwall.com. SonicWall will then execute the DPA and return a copy to the email address provided in the signature line.

Appendix 1 – PROCESSING INSTRUCTIONS

1 Subject-matter of Processing:

SonicWall will process Data as necessary to perform the services pursuant to the provisions of the agreement applicable to the Services and as further specified in the documentation associated with the Services and as further instructed by you in your use of the Services. "Services" as used herein refers to Capture Advanced Threat Protection sandbox, Capture Cloud Platform and such other hosted products/services that SonicWall may make available from time to time.

2 Duration of the Processing the Processing:

The duration of the processing will be until the earliest of (i) expiration or termination of the applicable agreement with SonicWall ("Agreement") or Services, or; (ii) the date upon which processing is no longer necessary. The provisions of this DPA shall apply for as long as your Data is in SonicWall's possession and/or control.

3 Nature and purpose of the Processing:

The objective of the processing of Data by SonicWall Inc. is to provide the Service, pursuant to the Agreement.

4 Type of Data:

Data includes data as defined in the DPA.

5 Categories of Subjects:

The data subjects' Data transferred may concern the following categories of Data:

- Contact details (which may include name, address, e-mail address, phone and fax contact details and associated local time zone information) of employees, personnel, customers, business contracts, vendors, Subcontractors, advisors, and freelancers and/or or other third parties of or associated with the data exporter (who are natural persons);
- Employment details (which may include company name, job title, grade, demographic and location data);
- IT systems information (which may include but not be limited to user ID and password, computer name, domain name, IP address, customer or end user data, and software usage pattern tracking information i.e. cookies);
- Data subject's e-mail content and transmission Data;
- Details of goods or services provided to or for the benefit of data subjects;
- Financial details (e.g. credit, payment and bank details).

6 Processing instructions

Any operation with regard to Data irrespective of the means applied and procedures, in particular the obtaining, collecting, recording, organizing, storage, holding, use, amendment, adaptation, alteration, disclosure, dissemination or otherwise making available, aligning, combining, retrieval, consultation, archiving, transmission, blocking, erasing, or destruction of data, the operation and maintenance of systems, management and management reporting, financial reporting, risk management, compliance, legal and audit functions and shall include "processing" which shall have the meaning given to such term in the Data Protection Laws.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES (Data Importer Information Security Overview)

This Appendix 2 sets out a description of the technical and organizational security measures implemented by the Data Importer in accordance with Data Protection Laws. Data Importer takes information security seriously and this approach is followed through in its processing and transfers of Data. This information security overview applies to Data Importer's corporate controls for safeguarding Data which is processed and transferred amongst the data Importer's group companies. Data Importer's information security program enables the workforce to understand their responsibilities.

SECURITY PRACTICES

Data Importer has implemented corporate information security practices and standards that are designed to safeguard Data Importer's corporate environment and to address business objectives across the following areas: (1) information security, (2) system and asset management, (3) development, and (4) governance. These practices and standards are approved by the Data Importer's management and are periodically reviewed and updated where necessary. Data Importer shall maintain an appropriate data privacy and information security program, including policies and procedures for physical and logical access restrictions, data classification, access rights, credentialing programs, record retention, data privacy, information security and the treatment of Data throughout its lifecycle.

ORGANIZATIONAL SECURITY

It is the responsibility of the individuals across the Data Importer's organization to comply with these practices and standards. To facilitate the corporate adherence to these practices and standards, Data Importer's Information Security ("IS") function is responsible for the following activities:

1. Security strategy – the IS function drives Data Importer's security direction. The IS function works to ensure compliance with security related policies, standards and regulations, and to raise awareness and provide education to users. The IS function also carries out risk assessments and risk management activities, and manages contract security requirements.
2. Security engineering – the IS function manages testing, design and implementation of security solutions to enable adoption of security controls across the environment.
3. Security operations – the IS function manages support of implemented security solutions, monitors and scans the environment and assets, and manages incident response.
4. Forensic investigations – the IS function works with Legal, and Human Resources to carry out investigations, including eDiscovery and eForensics.
5. Security consulting and testing – the IS function works with software developers on developing security best practices, consults on application development and architecture for software projects, and carries out assurance testing.

ASSET CLASSIFICATION AND CONTROL. Data Importer's practice is to track and manage key information and physical, software and logical assets. Examples of the assets that Data Importer might track include:

1. Information assets, such as identified databases, Data classification, archived information.
2. Software assets, such as identified applications and system software.
3. Physical assets, such as identified servers, desktops/laptops, backup/archival tapes, printers and communications equipment.

EMPLOYEE SCREENING, TRAINING AND SECURITY

1. Screening/background checks: Where reasonably practicable and appropriate, as part of the employment/recruitment process, Data Importer shall perform screening/background checks on employees (which shall vary from country to country based on local laws and regulations), where such employees will have access to Data Importer's networks, systems or facilities.
2. Identification: Data Importer shall require all employees to provide proof of identification and any additional documentation that may be required based on the country of hire or if required by other Data Importer entities or customers for whom the employee is providing services.
3. Training: Data Importer's annual compliance training program includes a requirement for employees to complete a Data protection and information security awareness course and pass an assessment at the end of the course. The security awareness course may also provide materials specific to certain job functions.
4. Confidentiality: Data Importer shall ensure its employees are legally bound to protect and maintain the confidentiality of any Data they handle pursuant to standard agreements.

PHYSICAL ACCESS CONTROLS AND ENVIRONMENTAL SECURITY

1. Physical Security Program: Data Importer shall use Appropriate Safeguards in its physical security program to mitigate security risks to the extent reasonably practicable.
2. Physical Access controls: Physical access controls/security measures at Data Importer's facilities/premises are designed to meet the following requirements:
   (a) access to Data Importer's buildings, facilities and other physical premises shall be controlled and based upon business necessity, sensitivity of assets and the individual's role and relationship to the Data Importer. Only personnel associated with Data Importer are provided access to Data Importer's facilities and physical resources in a manner consistent with their role and responsibilities in the organization;
   (b) relevant Data importer facilities are secured by an access control system.;
   (c) all persons requiring access to facilities and/or resources are issued with appropriate and unique physical access credentials (e.g. a badge or keycard assigned to one individual) by the IS function. Individuals issued with unique physical access credentials are instructed not to allow or enable other individuals to access the Data Importer's facilities or resources using their unique credentials (e.g. no "tailgating"). Temporary credentials may be issued to individuals who do not have active identities where this is necessary (i) for access to a specific facility and (ii) for valid business needs. Unique

credentials are non-transferable and if an individual cannot produce their credentials upon request they may be denied entry to Data Importer's facilities or escorted off the premises. At staffed entrances, individuals are required to present a valid photo identification or valid credentials to the security representative upon entering. Individuals who have lost or misplaced their credentials or other identification are required to enter through a staffed entrance and be issued a temporary badge by a security representative;

(d) Data Importer's employees are trained to always carry their credentials, store their laptops, portable devices and documents in a secure location (especially while traveling) and log out or shut down their computers when away from their desk;

(e) visitors who require access to Data Importer's facilities must enter through a staffed and/or main facility entrance. To prevent access to, or disclosure of, company proprietary information visitors are not allowed un-escorted access to restricted or controlled areas;

(f) select Data Importer facilities use CCTV monitoring, security guards and other physical measures where appropriate and legally permitted;

(g) locked shred bins are provided on most sites to enable secure destruction of confidential information and Data;

(h) for software development and infrastructure deployment projects, the IS function uses a risk evaluation process and a Data classification program to manage risk arising from such activities.

CHANGE MANAGEMENT. The IT organization manages changes to the corporate infrastructure, systems and applications through a centralized change management program, which may include testing, business impact analysis and management approval where appropriate. All relevant application and systems developments adhere to an approved change management process.

SECURITY INCIDENTS AND RESPONSE PLAN

1. Security incident response plan: Data Importer maintains a security incident response policy and related plan and procedures which address the measures that Data Importer will take in the event of loss of control, theft, unauthorized disclosure, unauthorized access, or unauthorized acquisition of Data. These measures may include incident analysis, containment, response, remediation, reporting and the return to normal operations.

2. Response controls: Controls are in place to protect against, and support the detection of, malicious use of assets and malicious software and to report potential incidents to the Data Importer's IS function or Service Desk for appropriate action. Controls may include, but are not limited to: information security policies and standards; restricted access; designated development and test environments; virus detection on servers, desktop and notebooks; virus email attachment scanning; system compliance scans; intrusion prevention monitoring and response; firewall rules; logging and alerting on key events; information handling procedures based on data type; e-commerce application and network security; and system and application vulnerability scanning. Additional controls may be implemented based on risk.

DATA TRANSMISSION CONTROL AND ENCRYPTION. Data Importer shall, to the extent it has control over any electronic transmission or transfer of Data, take all reasonable steps to ensure that such transmission or transfer cannot be read, copied, altered or removed without proper authority during its transmission or transfer. Data Importer will:

1. Implement industry-standard encryption practices in its transmission of Data. Industry-standard encryption methods used by Data Importer includes Secure Sockets Layer (SSL), Transport Layer Security (TLS), a secure shell program such as SSH, and/or Internet Protocol Security (IPSec);
2. If technically feasible, encrypt Data when transmitting or transferring that Data over any public network, or over any network not owned and maintained by Data Importer. The Data Importer's policy recognizes that encryption is ineffective unless the encryption key is inaccessible to unauthorized individuals and instructs personnel never to provide an encryption key via the same channel as the encrypted document; and
3. For Internet-facing applications that may handle sensitive Data and/or provide real-time integration with systems on a network that contains such information (including Data Importer's core network), a Web Application Firewall (WAF) may be used to provide an additional layer of input checking and attack mitigation. The WAF will be configured to mitigate potential vulnerabilities such as injection attacks, buffer overflows, cookie manipulation and other common attack methods.

SYSTEM ACCESS CONTROLS. Access to Data Importer's systems is restricted to authorized users. Access is granted based on formal procedures designed to ensure appropriate approvals are granted to prevent access from unauthorized individuals. Such procedures include:

1. admission controls (i.e. measures to prevent unauthorized persons from using data processing systems):
   (a) access is provided based on segregation of duties and least privileges to reduce the risk of misuse, intention or otherwise;
   (b) access to IT systems will be granted only when a user is registered under a valid username and password;
   (c) Data Importer has a password policy in place which requires strong passwords for user login to issued laptops, prohibits the sharing of passwords, prohibits the use of passwords that are also used for non-work functions, and advises users on what to do in the event their password or other login credentials are lost, stolen or compromised;
   (d) mandatory password changes on a regular basis;
   (e) automatic computer lock, renewed access to the PC only after new registration with a valid username and password;
   (f) Data and user classification determines the type of authentication that must be used by each system; and
   (g) remote access and wireless computing capabilities are restricted and require that both user and system safeguards are in place as well as user authentication.

2. access controls (i.e. measures to prevent unauthorized access to systems):
    (a) access authorization is issued in respect of the specific area of work the individual is assigned to (i.e. work role);
    (b) adjustment of access authorizations in case of changes to the working area, or in case an employee's employment is terminated for any reason;
    (c) granting, removing and reviewing administrator privileges with the appropriate additional controls and only as needed to support the system(s) in question; and
    (d) event logs from key devices and systems are centrally collected and reported on an exceptions basis to enable incident response and forensic investigations.

DATA ACCESS CONTROL. Data Importer applies the controls set out below regarding the access and use of Data:

1. personnel are instructed to only use the minimum amount of Data necessary to achieve the Data Importer's relevant business purposes;
2. personnel are instructed not to read, copy, modify or remove Data unless necessary to carry out their work duties, and;
3. third party use of Data is governed through contractual terms and conditions between the third party and Data Importer which impose limits on the third party's use of Data and restricts such use to what is necessary for the third party to provide services.

SEPARATION CONTROL. Where legally required, Data Importer will ensure that Data collected for different purposes can be processed separately. Data Importer shall also ensure there is separation between test and production systems.

AVAILABILITY CONTROL. Data Importer protects Data against accidental destruction or loss by following these controls:

1. Data is retained in accordance with this DPA or Data Importer's record management policy and practices, as well as legal retention requirements;
2. hardcopy Data is disposed of in a secure disposal bin or a crosscut shredder such that the information is no longer decipherable;
3. electronic Data is given to Data Importer's IT Asset Management team for proper disposal; and
4. appropriate technical measures are in place, including (without limitation): anti-virus software is installed on all systems; network protection is provided via firewall; network segmentation; user of content filter/proxies; interruption-free power supply; regular generation of back-ups; hard disk mirroring where required; fire safety system; water protection systems where appropriate; emergency plans; and air-conditioned server rooms.

DATA INPUT CONTROL. Data Importer has, where appropriate, measures designed to check whether and by whom Data have been input into Data processing systems, or whether such Data has been modified or removed.