This Data Protection Addendum ("**Addendum**") forms part of the Vendor's Terms of Use available at https://gdm.services/terms-of-use as may be amended or replaced from time to time and is incorporated into all current and future agreements with Vendor ("**Principal Agreement**") between: (i) **GDMservices, Inc.** with its address at 177 Huntington Ave #179369, Boston, MA 02115 **("Vendor")** acting on its own behalf and as agent for each Vendor Affiliate; and (ii) you ("**Company**") acting on its own behalf and as agent for each Company Affiliate.

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

Company is a Controller and Vendor is a Processor under this Addendum.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Principal Agreement. Except where the context requires otherwise, references in this Addendum to the Principal Agreement are to the Principal Agreement as amended by, and including, this Addendum.

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Company Personal Data in respect of which any Company Group Member is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Company Personal Data in respect of which any Company Group Member is subject to any other Data Protection Laws;

1.1.2 "**Company Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.3 "**Company Group Member**" means Company or any Company Affiliate;

1.1.4 "**Company Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of a Company Group Member pursuant to or in connection with the Principal Agreement;

1.1.5 "**Contracted Processor**" means Vendor or a Subprocessor;

1.1.6 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.7 "**EEA**" means the European Economic Area;

1.1.8 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.9 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.10 "**Restricted Transfer**" means:

1.1.10.1 a transfer of Company Personal Data from any Company Group Member to a Contracted Processor; or

1.1.10.2 an onward transfer of Company Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under section 6.4.3 or 12 below; *For the avoidance of doubt:* (a) without limitation to the generality of the foregoing, the parties to this Addendum intend that transfers of Personal Data from the UK to the EEA or from the EEA to the UK, following any exit by the UK from the European Union shall be Restricted Transfers for such time and to such extent that such transfers would be prohibited by Data Protection Laws of the UK or EU Data Protection Laws (as the case may be) in the absence of the Standard Contractual Clauses to be established under section 6.4.3 or 12; and (b) where a transfer of Personal Data is of a type authorized by Data Protection Laws in the exporting country, for example in the case of transfers from within the European Union to a country (such as Switzerland) or scheme (such as the US Privacy Shield) which is approved by the Commission as ensuring an adequate level of protection or any transfer which falls within a permitted derogation, such transfer shall not be a Restricted Transfer;

1.1.11 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Vendor for Company Group Members pursuant to the Principal Agreement;

1.1.12 "**Subprocessor**" means any person (including any third party and any Vendor Affiliate, but excluding an employee of Vendor or any of its sub-contractors) appointed by or on behalf of Vendor or any Vendor Affiliate to Process Personal Data on behalf of any Company Group Member in connection with the Principal Agreement; and

1.1.13 "**Vendor Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Vendor, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1.3 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Authority

Vendor warrants and represents that, before any Vendor Affiliate Processes any Company Personal Data on behalf of any Company Group Member, Vendor's entry into this Addendum as agent for and on behalf of that Vendor Affiliate will have been duly and effectively authorized (or subsequently ratified) by that Vendor Affiliate.

3. Processing of Company Personal Data

3.1 Vendor and each Vendor Affiliate shall:

3.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

3.1.2 not Process Company Personal Data other than on the relevant Company Group Member's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Vendor or the relevant Vendor Affiliate shall to the extent permitted by Applicable Laws inform the relevant Company Group Member of that legal requirement before the relevant Processing of that Personal Data.

3.2 Each Company Group Member:

3.2.1 instructs Vendor and each Vendor Affiliate (and authorizes Vendor and each Vendor Affiliate to instruct each Subprocessor) to:

3.2.1.1 Process Company Personal Data; and

3.2.1.2 in particular, transfer Company Personal Data to any country or territory,

as reasonably necessary for the provision of the Services and consistent with the Principal Agreement; and

3.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorized to give the instruction set out in section 3.2.1 on behalf of each relevant Company Affiliate.

3.3 Annex 1 to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Company Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Company may make reasonable amendments to Annex 1 by written notice to Vendor from time to time as Company reasonably considers necessary to meet those requirements. Nothing in Annex 1 (including as amended pursuant to this section 3.3) confers any right or imposes any obligation on any party to this Addendum.

4. Vendor and Vendor Affiliate Personnel

Vendor and each Vendor Affiliate shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Vendor and each Vendor Affiliate shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

5.2 In assessing the appropriate level of security, Vendor and each Vendor Affiliate shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

6. **Subprocessing**

6.1 Each Company Group Member authorizes Vendor and each Vendor Affiliate to appoint (and permit each Subprocessor appointed in accordance with this section 6 to appoint) Subprocessors in accordance with this section 6 and any restrictions in the Principal Agreement.

6.2 Vendor and each Vendor Affiliate may continue to use those Subprocessors already engaged by Vendor or any Vendor Affiliate as at the date of this Addendum, subject to Vendor and each Vendor Affiliate in each case as soon as practicable meeting the obligations set out in section 6.4.

6.3 With respect to each Subprocessor, Vendor or the relevant Vendor Affiliate shall:

6.3.1 before the Subprocessor first Processes Company Personal Data (or, where relevant, in accordance with section 6.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Company Personal Data required by the Principal Agreement;

6.3.2 ensure that the arrangement between on the one hand (a) Vendor, or (b) the relevant Vendor Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Company Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR;
6.3.3 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) Vendor, or (b) the relevant Vendor Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, or before the Subprocessor first Processes Company Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses with the relevant Company Group Member(s) (and Company shall procure that each Company Affiliate party to any such Standard Contractual Clauses co-operates with their population and execution); and

6.4 Vendor and each Vendor Affiliate shall ensure that each Subprocessor performs the obligations under sections 3.1, 4, 5, 7.1, 8.2, 9 and 11.1, as they apply to Processing of Company Personal Data carried out by that Subprocessor, as if it were party to this Addendum in place of Vendor.

7. Data Subject Rights
7.1 Taking into account the nature of the Processing, Vendor and each Vendor Affiliate shall assist each Company Group Member by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Company Group Members' obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

7.2 Vendor shall:
7.2.1 promptly notify Company if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and
7.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of Company or the relevant Company Affiliate or as required by Applicable Laws to which the Contracted Processor is subject, in which case Vendor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

8. **Personal Data Breach**
8.1 Vendor shall notify Company without undue delay upon Vendor or any Subprocessor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow each Company Group Member to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.
Such notification shall as a minimum:
8.1.1 describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;
8.1.2 communicate the name and contact details of Vendor's data protection officer or other relevant contact from whom more information may be obtained;

8.2 Vendor shall co-operate with Company and each Company Group Member and take such reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation
Vendor and each Vendor Affiliate shall provide reasonable assistance to each Company Group Member with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required of any Company Group Member by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

10. Deletion or return of Company Personal Data
10.1 Subject to sections 10.2 and 10.3 Vendor and each Vendor Affiliate shall promptly and in any event within thirty (30) business days of the date of cessation of any Services involving the Processing of Company Personal Data (the "**Cessation Date**"), delete (for avoidance of any doubt, "*delete*" here means to remove or obliterate Personal Data such that it cannot be recovered or reconstructed) and procure the deletion of all copies of those Company Personal Data.

10.2 Subject to section 10.3, Company may in its absolute discretion by written notice to Vendor within five (5) business days of the Cessation Date require Vendor and each Vendor Affiliate to (a) return a complete copy of all Company Personal Data to Company by secure file transfer in such format as is reasonably notified by Company to Vendor; and (b) delete and procure the deletion of all other copies of Company Personal Data Processed by any Contracted Processor. Vendor and each Vendor Affiliate shall comply with any such written request within thirty (30) business days of the Cessation Date.

10.3 Each Contracted Processor may retain Company Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Vendor and each Vendor Affiliate shall ensure the confidentiality of all such Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

10.4 Vendor may provide written certification to Company that it and each Vendor Affiliate has fully complied with this section 10 within thirty (30) business days of the Cessation Date.

11. Audit rights

11.1 Subject to sections 11.2 to 11.3, Vendor and each Vendor Affiliate shall make available to each Company Group Member on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by any Company Group Member or an auditor mandated by any Company Group Member in relation to the Processing of the Company Personal Data by the Contracted Processors.

11.2 Information and audit rights of the Company Group Members only arise under section 11.1 to the extent that the Principal Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

11.3 Company or the relevant Company Affiliate undertaking an audit shall give Vendor or the relevant Vendor Affiliate reasonable notice of any audit or inspection to be conducted under section 11.1 and shall make (and ensure that each of its mandated auditors makes) all endeavors to avoid causing any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

11.3.1 to any individual unless he or she produces reasonable evidence of identity and authority;
11.3.2 outside normal business hours at those premises; or
11.3.3 for the purposes of more than one audit or inspection, in respect of each Contracted Processor, in any calendar year, except for any additional audits or inspections which:
11.3.3.1 A Company Group Member is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory,
where Company or the relevant Company Affiliate undertaking an audit has identified its concerns or the relevant requirement or request in its notice to Vendor or the relevant Vendor Affiliate of the audit or inspection.

12. Restricted Transfers

12.1 Subject to section 12.3, each Company Group Member (as "data exporter") and each Contracted Processor, as appropriate, (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from that Company Group Member to that Contracted Processor.

12.2 The Standard Contractual Clauses shall come into effect under section 12.1 on the later of:
12.2.1 the data exporter becoming a party to them;
12.2.2 the data importer becoming a party to them; and
12.2.3 commencement of the relevant Restricted Transfer.

12.3 Section 12.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

12.4 Vendor warrants and represents that, before the commencement of any Restricted Transfer to a Subprocessor which is not a Vendor Affiliate, Vendor's or the relevant Vendor Affiliate's entry into the Standard Contractual Clauses under section 12.1, and agreement to variations to those Standard Contractual Clauses made under section 13.4.1, as agent for and on behalf of that Subprocessor will have been duly and effectively authorized (or subsequently ratified) by that Subprocessor.

13. General Terms

Governing law and jurisdiction

13.1 Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:
13.1.1 the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and
13.1.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

Order of precedence

13.2 Nothing in this Addendum reduces Vendor's or any Vendor Affiliate's obligations under the Principal Agreement in relation to the protection of Personal Data or permits Vendor or any Vendor Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

13.3 Subject to section 13.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Principal Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

Changes in Data Protection Laws, etc.

13.4 Company may:

13.4.1 by at least 30 (thirty) calendar days' written notice to Vendor from time to time make any variations to the Standard Contractual Clauses (including any Standard Contractual Clauses entered into under section 12.1), as they apply to Restricted Transfers which are subject to a particular Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

13.4.2 propose any other variations to this Addendum which Company reasonably considers to be necessary to address the requirements of any Data Protection Law.

13.5 If Company gives notice under section 13.4.1:

13.5.1 Vendor and each Vendor Affiliate shall promptly co-operate (and ensure that any affected Subprocessors promptly co-operate) to ensure that equivalent variations are made to any agreement put in place under section 6.4.3; and

13.5.2 Company shall not unreasonably withhold or delay agreement to any consequential variations to this Addendum proposed by Vendor to protect the Contracted Processors against additional risks associated with the variations made under section 13.4.1 and/or 13.5.1.

13.6 If Company gives notice under section 13.4.2, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Company's notice as soon as is reasonably practicable.

13.7 Neither Company nor Vendor shall require the consent or approval of any Company Affiliate or Vendor Affiliate to amend this Addendum pursuant to this section 13.5 or otherwise.

Severance

13.8 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

ANNEX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

This Annex 1 includes certain details of the Processing of Company Personal Data as required by Article 28(3) GDPR.

The subject matter of this Addendum is the processing of Personal Data in connection with the Services provided to the Controller. As between parties, the duration of the data processing under this Addendum is until the termination of the Principal Agreement in accordance with its terms, except as otherwise required by applicable law or as instructed by the Controller plus for about 24 months during which Processor stores the pseudonymized data, let alone special requirement provided by GDPR (fraud, legal claim, etc.). Other than that, all personal data is deleted once the 24-month period is over.

(a) Company requires the following services from Vendor to be provided:

(i) processing bid requests with Personal Data using OpenRTB protocol or other applicable real time bidding protocols as will be required by the Company;
(ii) suggesting bid response with information on goods and services which are believed to be of interest to Data Subject;
(iii) collecting data for industry analysis, tracking ad conversions, cross-device matching, behavioral advertising or demographic, geolocation and interest-based profiling;

(b) Company warrants, that all the Personal Data which is sent to Vendor has been collected with prior Data Subject's consent for all the purposes and processing operations, defined in this Addendum. Company declares that Personal Data should be processed by Vendor for the purpose of providing personalized advertising experience to Data Subject. The following processing operations could be performed by Vendor with Personal Data in order to fulfil Company's purposes:

(i) receiving and storing of information, including, but not limited to, for creation of suppression lists;
(ii) collection and processing of information about Data Subject use of Company's services to subsequently personalize advertising for Data Subject in other contexts, such as on other websites, CTV or mobile applications over time;
(iii) combining Personal Data with additional information on Data Subject received from Vendor's partners to improve relevance of future ads suggested for Data Subject.

(c) Types of Personal Data. Company may be sending the following Personal Data of Data Subject:

(i) advertising identifiers (Apple IDFA, or IFA on OTT, or Google Advertising ID (GAID), or Android ID, as applicable);
(ii) IP address;
(iii) geolocation data;
(iv) mobile / CTV device data: operating system version, device model, device ID;
(v) mobile / CTV application data: bundle ID, application store ID, language ID, software developer kit (SDK) version;
(vi) behavioral data: Data Subject's reaction to ads (impressions, clicks, installs), Data Subject's preferences on watching of the OTT content and an applicable embedded / included advertising.

(d) Vendor will take appropriate steps to ensure compliance with the Security Measures outlined in Annex 2 by its personnel to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Personal Data under this Addendum have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and that any such obligations survive the termination of that individual's engagement with Vendor.

(e) Company agrees that Vendor may transfer Personal Data from EU to US to fulfil its obligations under this Agreement, provided that Vendor complies with all applicable laws.

(f) Vendor is authorised by Company to use the following list of Subprocessors for performing specific Personal Data processing tasks:

(i) Amazon AWS (Cloud hosting services);
(ii) Datadog (Analytical and alerting services);
(iii) Bugsnag (Analytical and alerting services);
(iv) PagerDuty (Analytical and alerting services);
(v) Kochava (Click processing services);
(vi) AppsFlyer (Click processing services);
(vii) AdJust (Click processing services);
(viii) Tune (Click processing services);
(ix) Pixalate (Anti-fraud solutions).

(g) Vendor may appoint additional subprocessors with prior written consent of Company.

The categories of Data Subject to whom the Company Personal Data relates:

Internet users - anyone who's accessing or using the Website* and/or interacting with Application Marketing Service**.

Clients - authorized users of Application Marketing Service.

*Website: Client registration data includes name, e-mail, address, IP address.
Domains / pages: https://gdm.services

**Application Marketing Service:

RTB end-point domains: unity.gdm.services, bidder.gdm.services

Event tracking data includes: Advertising / Device ID, IP address, User Agent.

Pre-install event tracking domains: ev.gdm.services, pt.gdm.services, handler.gdm.services, request-tracker.gdm.services

Opt-out data includes: Advertising / Device ID.

Opt-out page: https://gdm.services/end-user-opt-out/

Other ad serving domains (with no personal data processing): cr.gdm.services

ANNEX 2: SECURITY MEASURES

The technical and organizational security measures implemented by the Vendor include:

1. Access control to premises and facilities (physical).

- The Vendor will maintain commercially reasonable physical security systems at all Vendor sites which are used to deliver services to the Company.

2. Access control to systems (virtual).

The Vendor will establish and maintain safeguards against accidental or unauthorized access to, destruction of, loss of, or alteration of the Personal Data:

- Access will be granted to employees, contractors and consultants through documented access request procedures. The employees, managers or other responsible individuals must authorize or validate access before it is given.
- Access controls are enabled at the operating system, database, or application level. Password standards for systems require at least 8 alphanumeric characters, cannot include common U.S. English dictionary words, and ensure that recent passwords are not reused.
- Users will be assigned a single account and prohibited from sharing accounts.

3. Access control to data:

Individuals will request access and justify a need to retain access as part of a documented access request process. Their managers or other responsible individuals must authorize or approve access before it is authorized.

- Access will be granted only after processing an approved “access control form”, i.e. LAN Logon ID, application access ID, or other similar identification.
- Unique User IDs and passwords will be issued to the users.
- Users, once authenticated, will be authorized for access levels based on their job functions.
- Vendor will promptly act to revoke access due to termination, a change in job function, or in observance of user inactivity or extended absence.

4. Disclosure control:

Vendor will deliver technology and processes designed to minimize access for illegitimate processing.

- Workstations will be configured with password protected screensavers.

5. Input control:

- Vendor will maintain system and database logs for access to all data under Vendor control.
- All Vendor systems must be configured to provide event logging to identify a system compromise, unauthorized access, or any other security violation. Logs must be protected from unauthorized access or modification.
- Company will maintain input controls on the Company systems.

6. Job control:

Technical and organizational measures to segregate the responsibilities between the Company and Vendor would include:

- Data processing activities will be carried out as is required by the applicable security standards.
- Workstations for data processing would be hardened to ensure that, to the extent possible, no client information in it is retained in the Vendor environment.

7. Availability control:

- For Microsoft Windows operational systems Vendor will protect data against accidental destruction or loss by ensuring workstations will be protected by commercial anti-virus and malware prevention software receiving weekly definition update.
- Upon detection of a virus or malware, Vendor will take immediate steps to arrest the spread and damage of the virus or malware and to eradicate the virus or malware.