Sharecare Vendor Data Processing Addendum

[Date last updated: January 1, 2023]

This Vendor Data Processing Addendum ("DPA") forms an integral part of the services agreement ("Agreement") between Sharecare Operating Company, Inc. ("**Sharecare**") and the vendor identified in the Agreement ("**Vendor**") and applies to the extent that Vendor processes Personal Data on behalf of Sharecare in the course of providing Services under the Agreement.

Recitals

(1) As part of its privacy policy and its contractual arrangements, Sharecare is committed to ensuring the appropriate protection of Personal Data of persons protected by Applicable Privacy Law(s) whose data is processed by Sharecare ("Data Subjects").

(2) Sharecare's commitment to Personal Data protection continues when Sharecare engages third party vendors, including but not limited to, Service Providers as defined by the CCPA.

(3) Accordingly, the parties desire to amend and supplement the Agreement as set forth herein.

(4) Sharecare's engagement of Vendor is conditioned upon Vendor's agreement to the terms and conditions of this DPA.

Agreement

1. Definitions

1.1 "**Affiliate(s)**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity;

1.2 "**Applicable Privacy Law(s)**" means all worldwide data protection and privacy laws and regulations applicable to the Processing of Personal Data pursuant to the Agreement, including, where applicable, local, state, national and/or foreign laws including, but not limited to, CCPA and EU Data Protection Law and implementations of EU Data Protection Law into national law.

1.3 "**Authorized Persons**" means any person who processes Personal Data on Vendor's behalf, including Vendor's employees, officers, partners, principals, contractors and Subcontractors.

1.4 **"Controller"** means an entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. For purposes of this DPA, Sharecare is the Controller.

1.5 **"CCPA"** means the California Consumer Privacy Act, Cal. Civ. Code 1798.100 *et seq.,* including any amendments and any implementing regulations thereto that become effective before, on or after the effective date of this Data Processing Addendum.

1.6 **"CCPA Consumer"** means a "consumer" as such term is defined in the CCPA.

1.7 **"Data Processor" or "Processor" or "Subprocessor"** means the entity which Processes Personal Data on behalf of the Controller, including as applicable but not limited to any "Service Provider" as that term is defined by the CCPA. For purposes of this DPA, Vendor is a Processor.

1.8 "**EEA**" means, the European Economic Area.

1.9 "**EU Data Protection Law**" means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the Processing of Personal Data and on the free movement of such data ("**Directive**") and all applicable member state implementations thereof; and (ii) on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**") and all applicable member state implementations thereof.

1.10 **"EU Model Clauses"** means the standard contractual clauses for Processors as approved by the European Commission pursuant to Decision C (2010) 593, as they may be amended or replaced from time to time.

1.11 "**Personal Data**" means any information and data, including but not limited to Personal Information as defined by the CCPA, submitted to Vendor by Sharecare relating to i) an identified or identifiable natural person ("Data Subject"); or ii) an identified or identifiable legal entity, where such information is protected similarly as personal data under Applicable Privacy Laws. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity. For the avoidance of doubt, Personal Data includes personally identifiable information.

1.12 "**Personal Information**" shall have the meaning set forth in the CCPA.

1.13 Reserved.

1.14 Reserved.

1.15 "**Processing" or "Process**" or **"Data Processing"** means any operation or set of operations performed on Personal Data or sets of Personal Data as defined in Art. 2(b) Data Protection Directive and Art. 4(2) GDPR or any operation or set of operations that are performed on Personal Information as defined by Cal. Civ. Code § 1798.140(o), such as but not limited to collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying.

1.17 "**Security Incident**" means any breach of security leading to, or reasonably believed to have led to, the accidental or unlawful destruction, loss, or alteration of, or unauthorized disclosure or access to, Personal Data.

1.18 **"Service(s)"** means work that Vendor performs for Sharecare as described in the Agreement.

1.19 **"Service Provider"** is defined by Cal. Civ. Code § 1798.140(v) and means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of Sharecare and to which Sharecare discloses a CCPA Consumer's Personal Information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the Personal Information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the Personal Information for a commercial purpose other than providing the services specified in the contract with the business.

1.20 "**Subcontractor**" means any third party (including but not limited to any Vendor affiliates) engaged directly or indirectly by Vendor as a subprocessor to process any Personal Data relating to this DPA and/or the Agreement. The term "Subcontractor" shall also include any third party appointed by a Subcontractor to process any Personal Data relating to this DPA and/or the Agreement.

1.21 **"Valid Transfer Mechanism"** means a data transfer mechanism permitted by EU Data Protection Laws as a lawful basis for transferring Personal Data to a recipient outside the EEA.

2. Data Processing: Role, Scope, and Instructions for Processing

2.1 **Scope and Roles.** This DPA applies when Personal Data is processed by Vendor. In this context, Vendor will act as Data Processor to Sharecare, who will act as Controller with respect to Personal Data (as each term is defined in Section 1).

2.2 **Subject-Matter. Nature, Purpose, and Duration of Data Processing.** The subject matter of the Data Processing under this DPA is Personal Data. The nature of the processing will include computing, storage, and such other Services as described in the Agreement. The purpose of the Data Processing under this DPA is the provision of the Services by Vendor pursuant to the Agreement. The type of Personal Data and categories of Data Subjects are determined by the Agreement and may include but are not limited to Sharecare's customers, employees, suppliers, and end-users. The duration of Processing Personal Data shall be for the term of the Agreement. Vendor shall not retain, use or disclose Personal Information for any purpose other than for the specific purpose of providing the Services, or as otherwise permitted by Applicable Privacy Law. Vendor acknowledges and agrees that it shall not retain, use or disclose Personal Information for a commercial purpose other than providing the Services or a purpose outside of the direct business relationship between Vendor and Sharecare. Processing Personal Data outside the scope of this DPA or the Agreement will require prior written agreement, with additional instructions for Processing, between Sharecare and the Vendor.

2.3 **Documented Instructions and Restrictions.** Vendor will at all times: (i) process the Personal Data only in accordance with Sharecare's documented instructions and in accordance with the Agreement; (ii) not disclose, release, transfer, make available or otherwise communicate any Personal Information to another business or third party without the prior written consent of Sharecare unless and to the extent that such disclosure is made to a Subprocessor for a business purpose, provided that Vendor has entered into a written agreement with the Subprocessor which imposes the same obligations on the Subprocessor with regard to their Processing of Personal Information as are imposed on the Vendor under this DPA and the Agreement; and (iii) not sell any Personal Data to another business or third party without the prior written consent of Sharecare. Notwithstanding the foregoing, nothing in this Agreement shall restrict the Vendor's ability to disclose Personal Data to comply with applicable laws. Each Party shall comply with its obligations under Applicable Privacy Law(s) in respect of any Personal Data it Processes under this DPA, providing the same level of privacy protection as required of Controllers under Applicable Privacy Law.

2.4 **Valid Transfer Mechanism.** If Vendor Processes Personal Data outside the EEA or countries formally recognized by the European Commission as providing an adequate level of data protection ("Adequate Countries") it will do so pursuant to a Valid Transfer Mechanism for all Personal Data transferred out of the EEA and/or Switzerland.

3. Personnel and Sub-processing

3.1 Vendor shall take reasonable steps to require screening of its personnel who may have access to Personal Data, and shall ensure its personnel (i) Process Personal Data in accordance with Sharecare's instructions as set forth in the Agreement and with Applicable Privacy Law(s); (ii) receive appropriate training on their responsibilities regarding the handling and safeguarding of Personal Data; and, (iii) are subject to confidentiality obligations which shall survive the termination of employment.

3.2 Vendor shall not subcontract any processing of the Personal Data to a Subcontractor without the prior written consent of Sharecare. Notwithstanding the foregoing, Sharecare consents to Vendor changing or adding to the Subcontractors listed in **Annex D**, which is incorporated by reference herein, as amended from time to time, to process the Personal Data provided that:

(a) Vendor provides Sharecare with a populated Annex D within thirty (30) days of execution of this DPA;

(b) Vendor provides prompt written notice to Sharecare of the engagement of any new Subcontractor (including details of the processing and location), and Vendor shall update the list of all Subcontractors engaged to process Personal Data under this Agreement at **Annex D** and send such updated version to Sharecare prior to the engagement of the Subcontractor;

(c) Vendor imposes the same data protection terms on any Subcontractor it engages as contained in this DPA (including but not limited to the Privacy Shield Principles and/or other Valid Transfer Mechanism provisions, where applicable), providing sufficient guarantees to implement appropriate technical and organisational measures to meet Applicable Privacy Laws and ensuring that such Subcontractor has entered into a written agreement requiring the Subcontractor to abide by terms no less protective than those provided in this DPA; and

(d) Vendor remains fully liable for any breach of this DPA or the Agreement that is caused by an act, error or omission of such Subcontractor.

3.3 If Sharecare objects to the engagement of any Subcontractor on data protection grounds, then either Vendor will not engage the Subcontractor to process the Personal Data or Sharecare may elect to immediately suspend or terminate the processing of Personal Data under the Agreement(s) and/or immediately suspend or terminate the Agreement(s), in each case without penalty. Upon any termination by Sharecare pursuant to this Section, Vendor shall refund Sharecare any prepaid fees for the terminated portion(s) of the Services that were to be provided after the effective date of termination.

4. Cooperation

4.1 Vendor shall comply with Applicable Privacy Laws by assisting and reasonably cooperating with Sharecare to enable Sharecare (or its third party Controller) to respond to any i) Data Subject requests for access, correction, deletion or restriction of that person's Personal Data ("Data Subject Request") or CCPA Consumer requests as governed by applicable CCPA requirements; and ii) complaints or other communications from Data Subjects and governmental, regulatory or judicial bodies relating to the processing of Personal Data under the Agreement(s), including but not limited to requests from Data Subjects seeking to exercise their rights under Applicable Privacy Laws, in which case Vendor will either (i) provide Sharecare with the ability within the Services to export, correct or delete Personal Data or restrict its Processing; or (ii) make such corrections, deletions, or restrictions on Sharecare's behalf if such functionality is not available within the Services. In the event that any such Data Subject Request or CCPA Consumer request, complaint, or communication is made directly to Vendor, Vendor shall immediately notify and pass this onto Sharecare and shall not respond to such communication without Sharecare's express authorization. During the term of the Agreement, Vendor shall ensure that Sharecare can extract Personal Data from the Services in a structured, commonly used and machine-readable format such that Sharecare can provide the Personal Data to an individual who makes a data portability request under EU Data Protection Laws.

4.2 If Vendor receives a subpoena, court order, warrant or other legal demand from a third party (including law enforcement or other governmental, regulatory or judicial authorities) seeking the disclosure of Personal Data, Vendor shall not disclose any information but shall immediately notify Sharecare in writing of such request, and reasonably cooperate with Sharecare if it wishes to limit, challenge or protect against such disclosure, to the extent permitted by applicable laws.

4.3 To the extent Vendor is required under Applicable Privacy Laws, Vendor will assist Sharecare (or its third party Controller) to conduct a data protection impact assessment and, where legally required, consult with applicable data protection authorities in respect of any proposed processing activity that present a high risk to data subjects.

5. Data Access & Security Measures

5.1 Vendor shall ensure that any Authorized Person is subject to a strict duty of confidentiality (whether a contractual or statutory duty) and that they process the Personal Data only for the purpose of delivering the Services under the Agreement to Sharecare.

5.2 Vendor will implement and maintain all appropriate technical and organizational security measures to protect from Security Incidents and to preserve the security, integrity and confidentiality of Personal Data ("**Security Measures**"). Such measures shall have regard for 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. At a minimum, Vendor agrees to the Security Measures identified at **Annex C hereto**. Vendor shall, to the extent possible, use best in class encryption technologies for transmitting and storing Personal Data. Vendor shall also employ best in class network security techniques, including but not limited to, firewalls, intrusion detection, and authentication protocols.

6. Security Incidents

6.1 In the event of a Security Incident, Vendor shall promptly (and in no event later than 48 hours of becoming aware of such Security Incident) inform Sharecare and provide written details of the Security Incident, including but not limited to the type of data affected and the identity of affected person(s) or legal entities as soon as such information becomes known or available to Vendor.

6.2 Furthermore, in the event of a Security Incident, Vendor shall:

(a) Include in the notification, to the extent known at the time of notification, (i) a description of the Security Incident, including but not limited to, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned; (ii) the name and contact details of Vendor's data protection officer or other contact point where more information can be obtained; (iii) a description of the likely consequences of the Security Incident; and (iv) a description of the measures taken or proposed to be taken by Vendor to address the Security Incident, including but not limited to, where appropriate, measures to mitigate its possible adverse effects. If Vendor is unable it is to provide all of the information listed above as part of the initial notification, Vendor will provide this information to Sharecare as soon as reasonably practicable. To the extent Sharecare requires additional information from Vendor to meet its Security Incident notification obligations under applicable Data Protection Laws, Vendor shall provide reasonable assistance to provide such information to Sharecare taking into account the nature of Processing and the information available to Vendor;

(b) provide timely information and cooperation as Sharecare may require to fulfil Sharecare's data breach reporting obligations under Applicable Privacy Laws; and

(c) take such measures and actions as are appropriate to remedy or mitigate the effects of the Security Incident and shall keep Sharecare up-to-date about all developments in connection with the Security Incident.

6.3 The content and provision of any notification, public/regulatory communication, or press release concerning the Security Incident shall be solely at Sharecare's discretion, except as otherwise required by applicable laws.

7. Security Reports & Inspections

7.1 Upon request, Vendor shall provide copies of relevant external certifications, audit report summaries and/or other documentation reasonably required by Sharecare to verify Vendor's compliance with this DPA. If Vendor has used

Personal Data in a manner not consistent with Applicable Privacy Law or this DPA, Sharecare may take reasonable and appropriate steps to stop and remediate Vendor's unauthorized use of Personal Data.

7.2 While it is the parties' intention ordinarily to rely on Vendor's obligations set forth in Section 7.1 to verify Vendor's compliance with this DPA, Sharecare (or its appointed representatives) may carry out an inspection of the Vendor's operations and facilities during normal business hours and subject to reasonable prior notice where Sharecare considers it necessary or appropriate.

8. International Transfers

8.1 Vendor will at all times provide an adequate level of protection for the Personal Data, wherever processed, in accordance with the requirements of Applicable Privacy Laws.

8.2 Vendor shall not process or transfer any Personal Data in or to a territory other than the territory in which the Personal Data was first collected (nor permit the Personal Data to be so processed or transferred) unless: (i) it has first obtained Sharecare's prior written consent; and (ii) it takes all such measures as are necessary to ensure such processing or transfer is in compliance with Applicable Privacy Laws (including but not limited to such measures as may be communicated by Sharecare to Vendor) and this DPA.

8.3 Reserved.

8.4 Where Vendor processes Personal Data under this DPA that originates from the EEA, Vendor shall:

(a) comply with Annex A hereto, containing EU Model Clauses, if Personal Data is to be transferred outside the EEA;

(b) promptly notify Sharecare if it makes a determination that it can no longer meet its obligations under Section 8.2 above, and in such event, work with Sharecare and promptly take all reasonable and appropriate steps to stop and remediate (if remediable) any processing until such time as the processing meets the level of protection as is required by Applicable Privacy Laws via an alternative Valid Transfer Mechanism; and

(c) immediately cease (and require that all Subcontractors to immediately cease) processing such Personal Data if in Sharecare's sole discretion, Sharecare determines that Vendor has not or cannot correct any non-compliance with Section 8.3(a) above in accordance with Section 8.3(c) within a reasonable time frame.

9. Deletion & Return

9.1 Upon Sharecare's request, or upon termination or expiration of this DPA or the Agreement or termination of the Services for whatever reason, Vendor shall promptly destroy all Personal Data (including copies) in its possession or control (including but not limited to any Personal Data processed by its Subcontractors). This requirement shall not apply to the extent that Vendor is required by any applicable law or legal proceeding to retain some or all of the Personal Data, in which event Vendor shall isolate and protect the Personal Data from any further processing except to the extent required by such law.

10. General

10.1 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between any provision in this DPA and any provision in the Agreement, this DPA controls and takes precedence. With effect from the effective date, this DPA is part of, and incorporated into the Agreement.

10.2 The obligations placed upon the Vendor under this DPA shall survive so long as Vendor and/or its Subcontractors process Personal Data on behalf of Sharecare.

10.3 The parties acknowledge and agree that any breach by Vendor of this DPA shall constitute a material breach of the Agreement, in which event and without prejudice to any other right or remedy available to it, Sharecare may elect to immediately terminate the Agreement in accordance with the termination provisions in the Contract(s).

10.4 In the event there is any act or omission (whether grossly negligent, reckless, intentional, or otherwise) on the part of the Vendor and/or its Subcontractors in connection with the activities contemplated by this DPA which leads to Sharecare or its Subsidiaries being liable for breaches of Applicable Privacy Laws or any third party contract, then Vendor shall indemnify Sharecare, its Subsidiaries and their respective officers, directors, employees or agents for any and all damages, fines, penalties, losses, liabilities, costs, harm or expenses (including reasonable legal fees) suffered by Sharecare as a result.

10.5 This DPA may not be modified except by a subsequent written instrument signed by both parties. Notwithstanding the foregoing, Sharecare may amend this DPA from time to time if necessary to comply with applicable law. Any such amendments will be displayed at sharecare.com/dpa.

10.6 If any part of this DPA is held unenforceable, the validity of all remaining parts will not be affected.

Annex A - Model Clauses

I. **Incorporation of Standard Contractual Clauses ("SCCs")**

With respect to transfers of Personal Data across national borders to other countries that have not been recognized under the applicable Data Protection Legislation as an Adequate Jurisdiction, the Parties hereby agree to be bound by, where applicable:

(i) For transfers of Personal Data from the EEA to a Non-Adequate Jurisdiction and for transfers of Personal Data from Brazil, Israel, Japan, Mexico, the Philippines, Singapore, and South Korea ("Applicable Data Transfer Jurisdiction") to a Non-Adequate Jurisdiction, the Controller to Processor SCCs are deemed incorporated into this DPA in their entirety and without alteration, except as noted herein, where Sharecare is operating as a Controller, and the Processor to Processor SCCs are deemed incorporated into this DPA in their entirety and without alteration, except as noted herein, where Sharecare is operating as a Processor; in either event, Vendor will be operating as a Processor. To the extent that the data importer is subject to the extra-territorial scope of Article 3(2) of the GDPR with respect to the specific processing, the obligations imposed to the data importer by the GDPR shall prevail over its obligations under the SCCs, where the latter are less strict. For reference, the official SCCs are available at the following link:https://eurlex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en or any subsequent link published by the European Union Publications Office;

(ii) For transfers of Personal Data from the UK to a non-Adequate Jurisdiction, the UK Controller-to-Processor SCCs are deemed incorporated into this DPA in their entirety and without alteration, except as noted herein, where Sharecare is operating as a Controller, and the UK Processor-to-Processor SCCs are deemed incorporated into this DPA in their entirety and without alteration, except as noted herein, where Sharecare is operating as a Processor; in either event, Vendor will be operating as a Processor. For reference, the UK Controller-to-Processor Standard Contractual Clauses are available at the following link: https://ico.org.uk/media/for-organisations/documents/2620100/uk-sccs-c-p-202107.docx or any subsequent link published by the UK Information Commissioner's Office.

II. Annex B of this DPA is incorporated by reference into the SCCs as Annex I thereof.

III. Annex C of this DPA is incorporated by reference into the SCCs as Annex II thereof.

IV. Annex D of this DPA is incorporated by reference into the SCCs as Annex III thereof.

Annex B - Details of the Processing

Description of Controller/Data Exporter and Data Importer:

The data exporter is Sharecare Operating Company, Inc.

The data importer is the entity providing services on behalf of Sharecare as identified in the Agreement.

As between Sharecare and Vendor, Sharecare shall be the Controller of certain Personal Data provided to Vendor to provide the Services.

Type(s) and Categories of Personal Data processed:

The personal data is defined in Section 2.2 of the DPA and in the Agreement.

Sensitive Personal Data processed:

The personal data processed may include data regarding one's health, which is subject to the strict safeguards in this DPA and otherwise required by applicable law (e.g. HIPAA).

Categories of Data Subjects:

Data subjects are defined in Section 2.2 of the DPA and in the Agreement.

Scope and Purpose of the Processing:

The processing operations are defined in Section 2.2 of the DPA and in the Agreement.

Frequency of the Processing:

As needed during the Term of the Agreement.

Retention Period:

The Term of the Agreement, except as otherwise set forth in the DPA or the Agreement.

Competent Supervisory Authority:

Ireland Data Protection Commission

ANNEX C

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

For the purposes of this Information Security Addendum ("ISA"), "Vendor" shall have the same meaning as defined in the DPA, and "Customer" shall mean Sharecare Operating Company, Inc.

Purpose & Disclaimer

This Sharecare Information Security Addendum ("ISA") describes the minimum information security program requirements implemented and maintained by Vendor during the course of its performance of services for Customer. Vendor may have additional privacy and security obligations under the terms of other policies or provisions in its contractual relationship with Customer.

Definitions

i. **Information Security** - the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.
ii. **Incident Management** – the defined process of monitoring and detection of security events on a computer or computer network and the execution of proper responses to those events.
iii. **Exception Management** – an established process to document and maintain appropriate management approvals for areas, processes or events that do not meet the company defined security policies.
iv. **Customer Confidential Data** – any Customer customer/member records or personal data in the possession of, or accessible by, Vendor or its computer or communication system(s), including personal data of any kind. Examples of this include PHI and PII data, pricing data, and Customer intellectual property.
v. **Cyber Security Insurance** - insurance designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage.
vi. **Demilitarized Zone (DMZ)** - a middle ground between an organization's trusted internal network and an untrusted, external network such as the Internet. Also called a "perimeter network," the DMZ is a subnetwork (subnet) that may sit between firewalls or off one leg of a firewall. Organizations typically place their web, mail and authentication servers in the DMZ.

Security Program and Policy

i. Consistent with applicable data security laws and regulatory requirements, Vendor shall:
   - implement, enforce, and update Information Security policies, standards, processes, and procedures;
   - develop Information Security strategy and maintain sufficient security budget to successfully implement the strategy; and
   - establish critical security processes such as Incident Management and Exceptions Management.
ii. Information Security policies must be reviewed and approved by Vendor management no less frequently than annually.
iii. Security Risk Management Program – Vendor must maintain a formal risk management function and methodically identify, analyze and mitigate security and technology risks.
iv. Sub-contractor Security Program – Vendor must require and verify that its subcontractors maintain security program standards that meet or exceed those of the Vendor.

Human Resources

i. A security training and awareness program must be in place for all Vendor employees and contractors, and training shall take place upon hire and no less frequently than annually. Upon request, Vendor shall provide Customer with written attestation that all employees and contractors have completed training.
ii. Upon hire, Vendor shall conduct background checks on all new employees and contractors.
iii. Vendor agrees that any employee or contractor who violates the security requirements of this ISA will be immediately removed and prohibited from providing services to Customer under any agreement, including statements of work or engagement letters, entered into between Customer and Vendor.
iv. All Vendor employee and contractor access must be deleted or disabled within 24 hours of termination. In the case of hostile terminations of employees or contractors, access must be deleted or disabled immediately.

Physical, Data and Environmental Security

i. Access for all persons to Vendor premises, buildings, and areas must be justified, authorized, logged and monitored. Appropriate steps must be taken by Vendor to protect documents and media containing sensitive information.
ii. Upon confirmed breach of this ISA and Customer's request, Vendor shall provide complete and auditable records of employees and contractors who may have had access to Customer Confidential Data, including at a minimum, their identity and date and time of access.
iii. All Customer Confidential Data shall be stored in a secure data center, and such data center shall provide to Customer upon request an ISO 27001 certificate or a Service Organization Control (SOC 2) report.
iv. All Customer Confidential Data must be encrypted in transit and at rest.

Audits, Assessments, Certifications and Insurance

i. **Notice of Audits and Certifications.** Upon request from Customer, Vendor shall provide Customer with data relating to the following audits of and certifications relating to Vendor's business and operations:

a. *External Network Security Assessment.* No less frequently than annually, Vendor shall engage an independent third party to complete an external network assessment that shall include in the scope the services provided to Customer. Vendor shall provide Customer with the full report or at a minimum a signed letter of attestation from this assessor and an overview of any critical or high issues noted by third party.
b. *Internal Network Security Assessment.* No less frequently than biennially, Vendor shall engage an independent third party to complete an internal network assessment (including social engineering tests) that shall include in the scope the services provided to Customer. Vendor shall provide Customer with the full report or at a minimum a letter of attestation from this assessor and an overview of any critical or high issues noted by third party.
c. *Customer Assessment.* Upon request and 60 days advanced notice, Customer or a third party on Customer's behalf may perform an audit to ensure compliance with this Document. Vendor is responsible for ensuring appropriate personnel are available for questions and ensuring audit records are provided in a timely manner. Any critical or high issues noted during audit must be remediated within mutually agreeable timeframe.

ii. Vendor must maintain Cyber Security Insurance policy that includes services provided to Customer.

Network Security and Other Security Controls

i. **Perimeter Defense** – Vendor must deploy a multilayered perimeter defense of its system by use of firewalls, proxies and DMZs. Vendor must implement and maintain rules for allowing inbound and outbound traffic.
ii. **Data Loss Prevention** – Vendor must monitor networks, user activities and system processes to prevent and detect unauthorized data movements.

iii. **Malware Defenses** - Vendor must monitor workstations, servers, and mobile-devices for active, up-to-date anti-malware protection with anti-virus, and procedures to ensure antivirus checking for all incoming files.

iv. **Access Control** – All access must follow the minimal necessary and "least privileged" principles. Vendor must maintain appropriate access by implementing access approval, termination and revalidation processes and procedures. This should include appropriate segregation of duties (e.g., developers do not have access to production data, etc.).

v. **Controlled Use of Administrative Privileges** – Vendor must ensure all service accounts have long and difficult-to-guess passwords that are changed on a periodic basis or is set to not allow interactive login. Passwords for all systems must be stored in a hashed or encrypted format.

vi. **Secure Configurations** – Vendor must develop, implement, and maintain secure configuration standards for hardware and software, including networking devices, operating systems, databases and applications. Vendor must enforce use of strong authentication and secure protocols.

vii. **Maintenance, Monitoring and Analysis of Audit Logs** – Vendor must log user and system activities around data, ensure integrity of log files, and implement activity review procedures and tools.

viii. **Inventory of Information Assets** – Vendor must maintain a detailed inventory of information assets complete and accurate with proper classification, ownership, location, value and criticality.

ix. **Change Management** – Vendor must use formal, documented change management procedures for any modifications to systems, infrastructure, equipment, software/applications, or other elements related to the services performed for Customer.

Vulnerability Management and Application Security Testing

i. **Application Software Security** - Both internally developed and third-party application software must be carefully tested by Vendor for security vulnerabilities. For third-party software, Vendor must verify that its suppliers have conducted detailed security testing of their products. For in-house developed applications, Vendor must conduct such testing itself or engage an outside firm to complete the testing. Findings must be remediated within an established reasonable timeframe. Vendor's developers must be trained in secure coding techniques and security testing integrated into the System Development Lifecycle.

ii. **Continuous Vulnerability Assessment and Remediation** – Vendor must maintain vulnerability and patch management processes for all software and hardware. All servers and workstations must be scanned by Vendor for vulnerabilities no less than monthly, and have defined remediation timelines to remediate any vulnerabilities that are noted.

iii. **Corrective Action**. If during an audit Vendor is found to be not compliant with the stipulations in this ISA, a corrective action plan will be put in place and reviewed yearly if not closed.

Business Continuity Management Program

i. **Business Continuity Program -** At all times during the term of its agreements with Customer, including statements of work and engagement letters, Vendor will maintain and adequately support a Business Continuity Management Program that ensures the continuous operation and, in the event of an interruption, the recovery of all material business functions needed to meet Vendor's contractual obligations to Customer.

ii. **Business Continuity Plan (which includes a Disaster Recovery (IT) Plan) -** Vendor shall develop, implement, maintain, and exercise a written Business Continuity Plan (the "Plan").

iii. **Delivery of the Plan -** Upon request from Customer and within 30 days, Vendor shall provide review to Customer of Vendor's then-current official company Plan.

iv. **Content -** The Plan must, at a minimum, describe the actions and resources required to provide for the continuous operation, and in the event of any interruption, the recovery of Vendor's contractual obligations to Customer under all agreements, including statements of work and engagement letters. Resources are defined as including, but not limited to, all people and facility resources and required systems, hardware, software and data. The recovery of systems, hardware, software and data must be within a Recovery Time Objective (RTO) sufficient to sustain contracted levels of service. Included as part of the required data, Vendor must provide Recovery Point Objective (RPO).

v. **Updates -** Vendor shall update and re-publish the Plan whenever there is a significant or material change in Vendor's systems, recovery strategies, recovery resources, actions described in the Plan or other data affecting Vendor's contractual obligations to Customer under all agreements, including statements of work and engagement letters, but no less frequently than at least once in every 12-month period.

vi. **Exercises -** Vendor shall exercise the Plan no less than annually and provide review to Customer of the exercise results.

Incident Reporting

i. In the event of a confirmed or suspected breach of Customer Confidential Data, Vendor shall notify Customer Information Security as soon as possible and within 72 hours of discovery. This notification is in addition to, but can be coordinated with, any other contractual reporting requirements.

Annex D - List of Vendor's Subcontractors

[**Vendor to list all Subcontractors here (including any and all Vendor affiliates processing Personal Data).**]

Name	Nature of Processing	Territory(ies)