Data Processing Agreement

PURPOSE & ORDER OF PRECEDENCE

This Data Processing Agreement, together with its annexes and any document expressly cross-referenced (the "**DPA**"), is deemed part of the services agreement between Iron Mountain and the Customer (the "**Agreement**"). The terms and conditions of the Agreement apply to, and govern, the rights and obligations of the parties under this DPA.

If any terms and conditions contained in this DPA are in conflict with the terms and conditions set forth in the Agreement, the terms and conditions set forth in this DPA shall be the controlling terms and conditions with respect to the subject matter of this DPA. This DPA supersedes and replaces any and all previous data processing agreements or data protection or privacy clauses between the parties in relation to the Services provided under the Agreement.

GENERAL TERMS

1. DEFINITIONS

Unless specifically defined herein, all capitalized terms shall have the same meanings as are given to them in the Agreement.

"**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data;

"**Customer Personal Data**" means Personal Data belonging to or collected by the Customer or its affiliates Processed as part of the Services;

"**Data Subject**" means an identified or identifiable natural person;

"Data Protection Legislation" means all applicable laws and regulations relating to the Processing of Personal Data that may exist in the relevant jurisdictions, including but not limited to, the EU GDPR (Regulation (EU) 2016/679), the UK GDPR (the GDPR as applicable as part of UK domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (as amended)), Data Protection Act 2018, FADP (the Swiss Federal Act on Data Protection), U.S. State Privacy Laws, LGPD (Brazilian General Data Protection Law), PIPL (Personal Information Protection Law of the People's Republic of China) and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them, including, where applicable, the guidance and codes of practice issued by supervisory authorities;

"**Personal Data**" means any information relating to a Data Subject;

"**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller;

"**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

"**Security Breach**" means any accidental or unlawful damage, destruction, loss, alteration, or unauthorised disclosure of, or access to the Customer Personal Data that Iron Mountain, its staff or subcontractors Process in the course of providing the Services;

"**Services**" means any services provided by Iron Mountain or its affiliates to the Customer or its affiliates under the Agreement;

"**U.S. State Privacy Laws**" means all United States state privacy and data protection laws that are applicable to the Processing of Personal Data under the Agreement, including without limitation, and as may be amended, superseded or replaced from time to time: (1) the California Consumer Privacy Act, as amended by the California

Privacy Rights Act, and any implementing regulations relating to the same (together, the "**CCPA**"); (2) the Colorado Privacy Act ("**CPA**"), (3) the Virginia Consumer Data Protection Act ("**CDPA**"); (4) the Utah Consumer Privacy Act ("**UCPA**"); and (5) the Connecticut Data Privacy Act ("**CTDPA**").

2. SCOPE AND DETAILS OF DATA PROCESSING

2.1 This DPA shall apply to the Customer Personal Data Processed by Iron Mountain as a Processor in the course of providing the Services pursuant to the Agreement on behalf of the Customer.

2.2 Iron Mountain may collect and Process Personal Data of the Customer's and its affiliates' employees as a Controller for legitimate business purposes, such as contract and customer relationship management, and in accordance with Data Protection Legislation and Iron Mountain's privacy notice available at Iron Mountain websites and other applicable privacy policies. Iron Mountain's obligations set out in this DPA shall not apply to the processing of such Personal Data.

2.3 The subject matter of the Personal Data Processing is the performance of the Services. The rights and obligations of the Customer and Iron Mountain are as set out in this DPA. Annex 1 of this DPA sets out the nature, duration and purpose of the Processing, the types of Customer Personal Data Iron Mountain Processes and the categories of Data Subjects whose Personal Data is Processed.

2.4 When Iron Mountain Processes Customer Personal Data in the course of providing the Services, Iron Mountain will:

2.4.1 Process the Customer Personal Data only in accordance with documented instructions from the Customer. If Iron Mountain is required to Process the Customer Personal Data for any other purpose by legislation to which Iron Mountain is subject, Iron Mountain will inform the Customer of this requirement first, unless such law(s) prohibit this on important grounds of public interest; and

2.4.2 At all times comply with applicable Data Protection Legislation and notify the Customer immediately if, in Iron Mountain's opinion, an instruction for the Processing of Customer Personal Data given by the Customer infringes applicable Data Protection Legislation.

2.5 Customer's instructions will be binding on Iron Mountain unless the completion of the instructions requires the provision of a service under the Agreement and the Customer does not agree to pay the service fees for such services.

2.6 Iron Mountain shall ensure that personnel required to access the Customer Personal Data are subject to a binding duty of confidentiality in respect of such Customer Personal Data and take reasonable steps to ensure the reliability and competence of Iron Mountain's personnel who have access to the Customer Personal Data.

3. PROVIDING CUSTOMER ASSISTANCE

3.1 Iron Mountain shall provide assistance to the Customer, always taking into account the nature of the Processing:

3.1.1 by appropriate technical and organisational measures and in so far as is possible, in fulfilling the Customer's obligations to respond to requests from Data Subjects exercising their rights;

3.1.2 in ensuring compliance with the Customer's obligations (such as security of Processing, notification of a Personal Data breach to the supervisory authority, communication of a Personal Data breach to the Data Subject, data protection impact assessment and prior consultation with supervisory authorities where the Processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk), taking into account the information available to Iron Mountain; and

3.1.3 by making available to the Customer all information which the Customer reasonably requests to allow the Customer to demonstrate that its obligations in selecting and appointing Iron Mountain have been met.

4. SECURITY MEASURES

4.1 Taking into account customary operational procedures, the costs of implementation and the nature, scope, context and purposes of Processing, Iron Mountain shall implement appropriate and reasonable technical and organizational measures designed to protect the confidentiality, integrity, and availability of the Customer Personal Data and to protect the Customer Personal Data against unauthorized or unlawful Processing and against accidental loss, destruction, damage, alteration, or disclosure. Iron Mountain's security standards are set forth in Annex 2 to this DPA.

4.2 It is the sole responsibility of the Customer to assess whether these technical and organizational measures meet the Customer's requirements.

5. COMPLIANCE WITH LAWS

The Customer and its affiliates shall: (i) Process Customer Personal Data in compliance with Data Protection Legislation; (ii) be authorized to give written instructions to Iron Mountain on the Processing of the Customer Personal Data in connection with the Services (including on behalf of any third party entity which is a Controller of the Customer Personal Data); and (iii) at all times retain the control and authority over the Customer Personal Data in relation to the Processing.

6. SUB-PROCESSING

6.1 The Customer acknowledges and agrees that Iron Mountain may engage its parent company, its affiliates and other third-party sub-Processors (including third-party sub-Processors engaged by Iron Mountain's affiliates or parent company) for the purposes of Processing Customer Personal Data under this DPA subject to clause 6.2 below.

6.2 A list of sub-Processors approved by the Customer as of the date of this DPA is made available here[1]. Iron Mountain can at any time replace or appoint a new sub-Processor provided that the Customer is given fifteen (15) days prior written notice and Customer does not object to such changes on demonstrable grounds related to data protection within that time frame. In order to receive these email notifications, the Customer shall subscribe and manage any existing subscription to Iron Mountain's notification service via this web page[2].

6.3 If the Customer fails to subscribe to this notification service, Iron Mountain shall not be liable for the lack of sub-Processor notification and all such appointments shall be deemed to be authorised by the Customer**.** If Customer objects in writing on demonstrable grounds related to data protection to the appointment of a replacement or new sub-Processor within the fifteen (15) days prior written notice, then Iron Mountain shall use reasonable efforts to make available to Customer a change in the Services or recommend a change to Customer's configuration or use of the Services, in each case to avoid the Processing of Customer Personal Data by the objected-to sub-Processor for Customer's consideration and approval. If the Customer does not approve any such changes proposed by Iron Mountain within fifteen (15) days, Iron Mountain may, by providing written notice to Customer, immediately terminate the Service or part of the Service which cannot be provided by Iron Mountain without the use of the objected-to sub-Processor. Such termination shall be without prejudice to any accrued rights and liabilities of the parties, provided that no termination fees, expenses or other compensation will be payable by Iron Mountain or Iron Mountain's affiliates in connection with such termination and the Customer shall promptly take possession of assets it provided to Iron Mountain as part of the terminated Services, subject to the terms of the Agreement and at the Customer's own cost and expense.

6.4 Iron Mountain shall ensure that any contract with sub-Processors in scope of this DPA contains provisions which are in all material respects the same as those in this DPA and are as required by applicable Data Protection Legislation. Where an Iron Mountain sub-Processor causes Iron Mountain to be in breach of its obligations under this DPA or any applicable Data Protection Legislation, Iron Mountain will remain fully liable to the Customer for the fulfilment of Iron Mountain's obligations under these terms.

7. SECURITY BREACHES

7.1 In the event of a suspected Security Breach, Iron Mountain will:

7.1.1 take action promptly to investigate the suspected Security Breach and to identify, prevent and mitigate the effects of the suspected Security Breach and to remedy the Security Breach;

7.1.2 notify the Customer without undue delay once it has a reasonable degree of certainty that a Security Breach has occurred and provide the Customer with a detailed description of the Security Breach including information reasonably necessary for Customer to meet reporting obligations under Data Protection Legislation.

7.2 Customer agrees that Iron Mountain may provide the information under clause 7.1.2 in phases. In such cases when Iron Mountain does not have access to or cannot provide certain information listed in clause 7.1.2 to the Customer, Iron Mountain will inform the Customer accordingly and Iron Mountain shall have no liability for failure to provide such information.

---

[1] https://www.ironmountain.com/-/media/files/Utility/Legal/GLOBAL-Personal-Data-Subprocessors-List.xlsx?la=en

[2] https://urldefense.proofpoint.com/v2/url?u=https-3A__reach.ironmountain.com_LegalSubprocessorSubscription&d=DwMFaQ&c=jxhwBfk-KSV6FFIot0PGng&r=JTlzF2zjl-gYEq5GmWmZcbgd--hgyVuIeEIP9Eu7Nvw&m=NB4wIISphmYGgqvrtYNU-28S8AaU6-YibdZ3Yg_2F68&s=xNzeKlzw6XbGZ_loyLbqEap2144HRDTflVtNiXKr6M4&e=

8. AUDITS

Iron Mountain will allow the Customer and its respective auditors or authorised agents, upon providing at least ten (10) business days' notice to Iron Mountain, to conduct audits or inspections during the term of the Agreement, provided that Iron Mountain shall not be required to provide or permit access to information concerning: (i) other customers of Iron Mountain; (ii) any of Iron Mountain's non-public external reports; and (iii) any internal reports prepared by Iron Mountain's internal audit or compliance function. The purposes of an audit or inspection pursuant to this clause shall be limited to verifying that Iron Mountain is Processing Customer Personal Data in accordance with its obligations under this DPA. Except where a Security Breach has occurred, no more than one such audit shall be conducted in any twelve (12) month period.

9. INTERNATIONAL DATA TRANSFERS (RESTRICTED TRANSFERS)

9.1 To the extent applicable, Customer hereby consents to and authorises international transfers of Customer Personal Data to entities as set out in Section 6.2 and in accordance with Annex 3 for the provision of the Services and the Customer and Iron Mountain agree:

9.1.1 to comply with applicable Data Protection Legislation with regards to such transfers;

9.1.2 that they have, taking into account, without limitation, i) the categories of the Customer Personal Data, ii) the countries whose national laws may not provide a level of protection for Personal Data that is comparable to those of EU/UK law ("**Third Country**") in scope, iii) the relevant technical and organisational measures set out under Section 7 and iv) the relevant parties participating in the processing of such Customer Personal Data, conducted an assessment of the appropriateness of the relevant transfer mechanism adopted hereunder where required by law and have determined that such transfer mechanism is appropriately designed to ensure Personal Data transferred in accordance with this DPA is afforded a level of protection in the destination country that is essentially equivalent to that guaranteed under the Data Protection Legislation.

10. LIABILITY AND INDEMNIFICATION

10.1 Notwithstanding anything to the contrary in the Agreement, in the event of a Security Breach caused directly by Iron Mountain's breach of its obligations under this DPA, Iron Mountain shall reimburse the Customer to the extent permitted by the applicable law for the direct, verifiable, necessary and reasonably incurred third-party costs of the Customer in the (a) investigation of such Security Breach, (b) preparation and mailing of notices to such Data Subjects and regulatory authorities as required by the Data Protection Legislation, (c) the provision of credit monitoring services to such individuals as required by law for a period not exceeding twelve (12) months, and (d) payment of the portion of regulatory fines, penalties, or sanctions imposed by a supervisory authority for which the supervisory authority states that Iron Mountain is directly responsible.

10.2 In the event a Data Subject brings a claim against either or both parties for alleged infringement of the Data Protection Legislation ("**Data Subject Claims**") where this is permitted, each party shall control its own defence of any such claim (or its portion of the defence) and remain solely responsible for its own costs, expenses and liabilities related thereto, including legal fees or any amounts awarded against it by a court or made by it in settlement, provided however, that where each party is responsible for a portion or either party is responsible for the full amount of the damages suffered by a Data Subject for the same incident or series of incidents and the Data Subject has recovered full compensation from only one party (the "**Compensating Party**"), then the Compensating Party shall be entitled to claim back from the other party that part of the compensation corresponding to the damage caused by such other party. The Compensating Party can only raise its claim towards the other party within 12 months after the incident, to the extent permitted by the applicable law.

10.3 To the maximum extent allowed by applicable laws, the limitations of liability and any exclusions of damages set forth in the Agreement govern the aggregate liability for all Customer claims arising out of or related to this DPA, and/or the Agreement against Iron Mountain. These limitations of liability and exclusions of damages apply to all claims, whether arising under contract, tort or any other theory of liability, and any reference to the liability of Iron Mountain means the aggregate liability of Iron Mountain and all Iron Mountain affiliates together for claims by Customer and all other Customer affiliates. To the extent required by applicable laws, this section is not intended to (i) modify or limit the parties' liability for Data Subject Claims made against a party where there is joint and several liability, or (ii) limit either party's responsibility to pay penalties imposed on such party by a regulatory authority.

10.4 Clauses 10.1 to 10.3 state each party's sole and exclusive remedy and each party's sole liability for any loss, damage, expense or liability in connection with this DPA.

11. PUBLIC AUTHORITY REQUESTS

11.1 To the extent legally permissible and subject to clauses 11.2 to 11.5 below, Iron Mountain agrees to notify the Customer if it:

11.1.1 receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of Customer Personal Data transferred pursuant to the Agreement; or

11.1.2 becomes aware of any direct access by public authorities to Customer Personal Data transferred pursuant to the Agreement in accordance with the laws of the country of destination.

11.2 If Iron Mountain is prohibited from notifying the Customer under the laws of the country of destination, Iron Mountain agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible.

11.3 Iron Mountain agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination. It shall not disclose the Customer Personal Data requested until required to do so under the applicable procedural rules.

11.4 Iron Mountain agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

11.5 Iron Mountain agrees to preserve the information pursuant to this clause for the duration of the Agreement and make it available to the competent supervisory authority on request.

12. MISCELLANEOUS

12.1 Subject to the nature of the Services provided by Iron Mountain, upon termination/expiry of the Agreement, based on the Customer's specific instruction and subject to the terms of the Agreement, Iron Mountain shall either delete/destroy or return to the Customer or to a third party designated by the Customer all Customer Personal Data. Any Customer Personal Data contained within the Customer's asset stored by Iron Mountain on behalf of the Customer will be returned to the Customer in accordance with an agreed exit or transition plan, and subject to agreed-upon costs, as stipulated in the Agreement or other applicable contractual document. In all other cases if the Agreement is silent on the deletion/destruction or return of Customer Personal Data and the Customer fails to give any instructions regarding the deletion/destruction or return of Customer Personal Data within fifteen (15) days of the termination/expiry of the Agreement, Iron Mountain shall send a written notice to the Customer requesting to receive within 15 (fifteen) days specific instructions whether to delete/destroy or to return the Customer Personal Data and informing the Customer about all applicable secure destruction or other fees payable by the Customer. Should the Customer fail to provide written instructions within such fifteen (15) days' timeframe and pay the applicable fees within this same period, then the Customer hereby authorizes Iron Mountain to further Process, delete, destroy all Customer Personal Data after the termination of the Agreement at the option of Iron Mountain and the expense of Customer.

12.2 Notwithstanding Clause 12.1, Iron Mountain shall not be in breach of its obligations with respect to the deletion of Customer Personal Data retained on back-up tapes as long as such back-up tapes are overridden (and thereby the Customer Personal Data deleted) in the normal course of business.

12.3 Except for the Standard Contractual Clauses (as defined in Annex 3 to this DPA), this DPA, and any dispute, claim or controversy arising out of or relating to this DPA, or the breach, termination or validity thereof, are governed by the choice of law provision of the Agreement; and any dispute, controversy or claim arising out of or in connection with this DPA will be primarily sought to be resolved through any defined dispute resolution process contained within the Agreement.

12.4 Each party may notify the other party in writing from time to time of any modifications to this DPA which the party reasonably considers to be necessary to address the requirements of the Data Protection Legislation or any decision of a supervisory authority or competent court. Any such modifications shall only take effect if and to the extent set forth in a mutually agreed amendment to this DPA executed by both parties, except where one party informs the other party about any new legal requirement and sends such an amendment that includes the necessary changes only and which can be accepted without formally agreeing to it, i.e., by way of not raising any objection within a certain deadline, are considered as mutually agreed amendments to this DPA.

ANNEX 1

Details of Processing and Data Transfer (if applicable)

A. LIST OF PARTIES:

The parties to this DPA and the roles of Data Exporter and Data Importer are set out in the Agreement and Annex 3 (International Data Transfers), if applicable.

B. DESCRIPTION OF PROCESSING/TRANSFER (if applicable):

Categories of Data Subjects whose Personal Data is processed/transferred:

Depending on the nature of Iron Mountain's Services and the Customer's business, the Customer may submit Personal Data belonging to various categories of Data Subjects to Iron Mountain, the extent of which is determined and controlled by the Customer in its sole discretion. As such, categories of Data Subjects may include: past and present employees; past and present contractors or consultants; agency-supplied contractors or consultants and external secondees; job applicants and candidates; students and volunteers; individuals identified by employees or retirees as beneficiaries, spouse, domestic/civil partner, dependents and emergency contacts; retirees; past and present directors and officers; shareholders; bondholders; account holders; end-users / consumers (adults, children); patients (adults, children); by-passers (CCTV cameras); and website users.

Categories of Personal Data processed/transferred:

Depending on the nature of Iron Mountain's Services and the Customer's business, the Customer may submit Personal Data belonging to various categories of Personal Data to Iron Mountain, the extent of which is determined and controlled by the Customer in its sole discretion. As such, categories may include personal data relating to the Customer and/or the Customer's own clients, employees, etc.

Sensitive data transferred (if applicable):

Depending on the nature of Iron Mountain's services and the Customer's business, the Customer may submit sensitive data to Iron Mountain, the extent of which is determined and controlled by the Customer in its sole discretion.

If applicable, the frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis):

The transfer takes place on a continuous basis.

Nature of the Processing:

Collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Purpose(s) of the data processing/transfer (if applicable) and further Processing:

The provision of Services as set out in the Agreement.

Data retention:

The Personal Data will be retained by Iron Mountain for the duration of the Services offered to Customer and until such time the Personal Data is returned or destroyed as determined in accordance with clause 12.1 of this DPA.

If applicable, for transfers to (sub) Processors, also specify subject matter, nature and duration of the Processing:

For the duration of the Agreement with Customer, sub-Processors provide among others Information Technology (IT) and consulting services, including global IT support, event reporting and management services.

C. COMPETENT SUPERVISORY AUTHORITY

As set out in Annex 3 (International Data Transfers), if applicable.

ANNEX 2

TECHNICAL AND ORGANISATIONAL MEASURES ("SECURITY MEASURES")

1. INFORMATION SECURITY PROGRAM AND POLICY

Iron Mountain shall maintain an information security program with appropriate physical, technical and administrative controls that are designed to meet industry standards. The information security program shall include:

1.1 Documentation, internal publication, and communication of Iron Mountain information security policies, standards, and procedures;

1.2. Documented, clear assignment of responsibility and authority for establishment and maintenance of the information security program;

1.3 Regular testing of the key controls, systems and procedures of the information security program;

1.4 Administrative, technical and operational measures designed to protect all Customer Personal Data utilizing the practices, procedures and processes described in this Security Annex, to the extent they are relevant and applicable to the format in which the Customer Personal Data is maintained.

2. RISK ASSESSMENT

Iron Mountain shall maintain an information security risk assessment program designed to identify and assess reasonably foreseeable internal and external risks and vulnerabilities that could affect the security, confidentiality, and/or integrity of Customer Personal Data. Iron Mountain shall evaluate and update, where necessary, reasonable and appropriate, the effectiveness of the current information security program for limiting such risks, on an annual basis, or whenever there is a material change in risk or vulnerabilities to Customer Personal Data.

3. MANAGEMENT OF INFORMATION PROCESSING ASSETS AND PHYSICAL MEDIA

3.1 Management of Information Processing Assets. Iron Mountain maintains an asset inventory management program to manage the physical, technical and administrative controls regarding Iron Mountain's information processing assets (such as computers, servers, storage devices, communications networks, personal computers, laptops and peripheral devices).

The asset inventory management program includes the following:

3.1.1 Documented assignment of asset ownership to Iron Mountain personnel to ensure appropriate classification of information, determination of access restrictions, and review of access controls.

3.1.2 Sanitization of assets prior to their disposal in accordance with NIST 800-88.

3.1.3 Requirement of management authorization prior to removal of equipment or software that is not assigned to a specific individual from Iron Mountain premises.

3.2 Controls. Iron Mountain controls include the following:

3.2.1 Operating procedures and technical controls designed to protect documents, computer media, input/output/backup data, and system documentation from unauthorized disclosure, modification and destruction.

3.2.2 Procedures for the secure disposal of electronic or physical media containing Customer Personal Data.

3.2.3 An established process to track all of Customer's physical media from initial Iron Mountain custody through permanent withdrawal or destruction.

4. WORKFORCE SECURITY MEASURES

4.1 Confidentiality. Iron Mountain shall reasonably require that all Iron Mountain employees, including temporary and contract employees, agree to maintain the confidentiality of Customer Personal Data and comply with Iron Mountain's internal information security and acceptable use requirements.

4.2 Background Investigation Policy. Iron Mountain has a background investigation policy and drug testing policy (U.S. only) in effect for its employees. Iron Mountain will continue to maintain such policies for the term of the Agreement. The policy requirements include, but are not limited to, drug screening (U.S. only), personnel identity verification, criminal record searches, employment verifications, government/terrorist watch list searches, as well as education verifications for certain employees, and driver licensing and violation history for driver candidates and existing drivers. When derogatory information is identified on a background check, Iron Mountain conducts an individualized assessment, in accordance with applicable labor laws and best practices.

4.3 Work with Subcontractors. Iron Mountain shall require any subcontractor performing Services under the Agreement to comply with similar restrictions to those set forth in this Section with respect to any subcontractor personnel who will be performing Services under the Agreement that involve Processing Customer Personal Data.

4.4 Security Awareness Training. At least annually, Iron Mountain shall conduct general security awareness training and specific role-applicable security training for all Iron Mountain employees with access to Customer Personal Data. Iron Mountain shall maintain records showing the names of such Iron

Mountain employees in attendance and the date of each security awareness training. Iron Mountain shall routinely review and update its security awareness training program.

4.5 Removal of Iron Mountain Personnel. Iron Mountain maintains a disciplinary process that is applied to Iron Mountain employees who violate the security requirements herein.

4.6 Termination of Access upon Termination/Reassignment. Upon termination or reassignment to a role not requiring access to Customer Personal Data, an Iron Mountain employee's access to Customer Personal Data shall be revoked promptly.

5. PHYSICAL AND ENVIRONMENTAL SECURITY

5.1 Physical Security Controls. Iron Mountain's facilities utilise physical controls that reasonably restrict access to Customer Personal Data, including, as Iron Mountain deems appropriate, access control protocols, physical barriers such as locked facilities and areas, employee access badges, visitor logs, visitor access badges, card readers, video surveillance cameras, and intrusion detection alarms. All visitors must sign in and be escorted at all times.

5.2 Supporting Utilities. Iron Mountain shall employ measures designed to protect its facilities containing Customer Personal Data and systems from failures of power, telecommunications, water supply, sewage, heating, ventilation and air-conditioning, as applicable,.

5.3 Transmission System Security. Iron Mountain shall employ measures designed to protect the physical security of its network infrastructure and telecommunication systems from transmission interception and damage.

5.4 Offsite Equipment. In the event that Iron Mountain outsources functions that require use of offsite equipment in support of services, any offsite equipment storing Customer Personal Data shall be protected by security equivalent to that used for on-site equipment used for the same purpose.

5.5 Physical Access to Information Processing Assets. Iron Mountain shall retain records of Iron Mountain employees authorized to have physical access to Iron Mountain-controlled computer environment(s) used by Iron Mountain to provide Services for one year and, upon Customer's request related to a Security Breach, and subject to Iron Mountain's security policies, provide access to Customer to view auditable records of such Iron Mountain employees.

5.6 Physical Access Restricted. Iron Mountain shall limit physical access to Iron Mountain-controlled facilities that Process Customer Personal Data to those Iron Mountain employees and authorized individuals who have a business need for such access. Iron Mountain shall have an approval process for authorising and tracking requests for physical access to such facilities.

5.7 Repairs and Modifications. Iron Mountain shall record all security-related repairs and modifications to any physical components, including hardware, walls, doors and locks of secure areas within facilities where Customer Personal Data is stored.

5.8 Records. Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

6. COMMUNICATIONS AND INFORMATION PROCESSING OPERATIONS MANAGEMENT

6.1 Device Configuration Standards. Iron Mountain shall create, implement and maintain system administration procedures that meet industry standards, including without limitation, system hardening, system and device patching (operating system and applications) and proper anti-virus installation and updates.

6.2 Information Processing Systems Change Control. Iron Mountain shall have an internal formal change management request process in place for information processing and communications network systems, and Iron Mountain's change requests shall be documented, tested, and approved prior to implementation of any new information processing or network communications capabilities, system patches or changes to existing systems.

6.3 Segregation of Duties. Iron Mountain shall segregate duties and areas of responsibility so that no one person has sole ability to modify information processing systems that access Customer Personal Data.

6.4 Separation of Development and Production Environments. Iron Mountain's development, test and production environments for information processing systems must be logically or physically separated.

6.5 Technical Architecture Management. Iron Mountain shall establish a configuration management process to define, manage, and control the information processing system components utilized to provide the Services and the technical infrastructure of such components.

6.6 Intrusion Detection. Iron Mountain shall continually monitor computer systems and processes for attempted or actual security intrusions or violations and notify Customer of any unauthorized access to Customer Personal Data.

6.7 Network Security. Iron Mountain shall ensure the following are in place:

- 6.7.1 With regards to Iron Mountain-hosted environment(s) used to provide the Services, network intrusion detection system ("IDS") and intrusion prevention sensors ("IPS") alert events that are logged, with daily reports issued for review (collectively known as "IDS/IPS");
- 6.7.2 With regards to Iron Mountain-hosted environment(s) used to provide the Services, IDS/IPS that are updated no less frequently than weekly but as soon as reasonably possible after the updates are received, and prompt running of the latest threat signatures or rules;
- 6.7.3 High-risk ports on externally-facing systems are not accessible from the internet;
- 6.7.4 Iron Mountain's network connections are logged and recorded in log files;

6.7.5 Deployment of firewall(s) designed to protect and inspect all inbound and outbound network services traffic between defined network points;
6.7.6 Hardening policies for defining inbound and outbound network ports or service traffic for all Iron Mountain-owned or managed systems that are documented and authorized within the information security program;
6.7.7 Network and diagnostic ports that are properly secured; and
6.7.8 Policies, procedures and technical controls that are designed to prevent, detect and remove malicious code or known attacks on Iron Mountain's information systems.

6.8 Encrypted Authentication Credentials. Iron Mountain shall ensure that authentication credentials transmitted over Iron Mountain's network devices are encrypted in transit.

6.9 Secure Network Administration. Iron Mountain networks shall be reasonably managed and controlled to protect from known threats, and to maintain security for all Iron Mountain managed applications and data on the network or in transit over the network. Technical controls and secure communication protocols shall be implemented to prohibit unrestricted connections to untrusted networks or publicly accessible servers.

6.10 Virus Protection. Iron Mountain shall implement and maintain an anti-virus management program, including malware protection, up-to-date signature files or alternative protection against emerging threats, patches, and virus definitions, for Iron Mountain managed servers and workstations used to house or access Customer Personal Data.

6.11 Website – Client Encryption. Iron Mountain shall ensure that for each of its websites Secure Sockets Layering (SSL) is enabled and contains a valid SSL certificate requiring confidentiality, authentication or authorization controls.

6.12 Information Backup. Iron Mountain shall create appropriate back-up copies of system files. In addition, Iron Mountain shall develop and maintain disaster recovery procedures, please see "Disaster Recovery" section below for more details.

6.13 Electronic Information in Transit. Iron Mountain shall utilise encryption with an industry-standard algorithm with a minimum 128 bit key length to protect Customer Personal Data transmitted over public networks when originating from Iron Mountain hosted infrastructure.

6.14 Cryptographic Controls. Iron Mountain shall follow a documented policy on the use of cryptographic controls. Iron Mountain's cryptographic controls shall:
6.14.1 Be designed to reasonably protect the confidentiality and integrity of Customer Personal Data being processed, transmitted or stored by Iron Mountain in any shared network environments in accordance with the terms of the Agreement;
6.14.2 Be applied, in Iron Mountain-hosted environment(s) used to provide services, to Customer Personal Data in transit across or to "untrusted" networks (i.e., networks that Iron Mountain does not legally control), including those used for sending data to Customer's corporate network from Iron Mountain's network, subject, in each case, to Customer's cooperation in management of encryption keys necessary to de-encrypt transmissions received by Customer; and
6.14.3 Include documented encryption key management practices to support the security of cryptographic technologies.
6.14.4 Include encryption of all Customer Personal Data on laptops or other portable devices.

6.15 Logging Requirements. Iron Mountain shall ensure the following:
6.15.1 Significant security and systems events are logged and reviewed;
6.15.2 Audit logs are retained for a minimum of one year for systems in Iron Mountain-hosted environment(s) used by Iron Mountain to provide services;
6.15.3 System audit logs are reviewed for anomalies; and
6.15.4 Log facilities and systems information are reasonably protected against tampering and unauthorized access.

6.16 Network Time Synchronization. Iron Mountain shall synchronize the system clocks of all information processing systems using a common authoritative time source.

6.17 Segregation on Networks. Iron Mountain shall appropriately segregate related groups of information services, users, and information systems on networks.

7. ACCESS CONTROL

7.1 Access Control Policy. Iron Mountain maintains access control policies with respect to information processing assets that Iron Mountain formally approves, publishes and implements.

7.2 Logical Access Authorization. Iron Mountain shall have an approval process for logical access requests to Customer Personal Data and requests for access to Iron Mountain systems dedicated for use in the Services.

7.3 Access Control and Access Review. Iron Mountain shall grant access to Customer Personal Data only to active Iron Mountain employees, including temporary and contract employees, and active users accounts who need such access in order to perform their job function. All privileged access must be reviewed and confirmed to be consistent with current job role and documented on, at least, a quarterly basis.

7.4 Control of Third Party Access. Prior to granting access to external parties to Iron Mountain's information systems that access Customer Personal Data, Iron Mountain shall ensure that appropriate controls are in place.

7.5 Operating Systems Access Control. Iron Mountain shall control access to operating systems (both software and hardware based operating systems) by requiring a secure log-on process that uniquely identifies the individual who is accessing the operating system.

7.6 Mobile Computing Devices. Iron Mountain will have a policy or procedure in place designed to protect Iron Mountain's mobile computing devices from unauthorized access. Such policies or procedures shall address physical protection, access control and security controls such as encryption, virus protection and device backup.

7.7 Customer Systems Isolation. Iron Mountain shall, within its hosted environment(s) used to provide the Services, logically separate and segregate Customer Personal Data from all other information.

7.8 Accounts. Iron Mountain shall do the following with respect to accounts:

7.8.1 Require authentication of the identity of each Iron Mountain employee who seeks access to Iron Mountain systems that Process Customer Personal Data and prohibit the use of shared user accounts, or user accounts with generic credentials (i.e., IDs), to access Customer Personal Data or systems.

7.8.2 Require that all user account IDs, including privileged accounts, be tied directly to a person (as opposed to a position).

7.8.3 If default administration accounts are not disabled or removed, require the use of temporary passwords, check out IDs, or similar controls for default administration account access.

7.8.4 Require that inactive regular accounts are locked or disabled after 90 days of inactivity.

7.8.5 Prohibit access to an account after multiple unsuccessful access attempts.

7.8.6 Require unique identifiers and strong passwords that include, at a minimum, the following: minimum number of 8 characters; must be changed every 90 days; and have complexity requirements.

7.8.7 Prohibit employees from sharing or writing down passwords.

7.9 Controls for Unattended Systems. Iron Mountain shall use a password-protected screensaver for any systems that are left unattended and have had no activity for 30 minutes.

8. INFORMATION SYSTEMS ACQUISITION DEVELOPMENT AND MAINTENANCE

8.1 Systems Development Security. Iron Mountain shall ensure that security is part of all information systems development and operations and shall publish and adhere to internal secure coding methodologies based on application development security standards.

8.2 Software Security Management. Iron Mountain's information systems (including operating systems, infrastructure, business applications, services and user-developed applications) shall be designed to be in compliance with information security standards.

8.3 Network Diagrams. Iron Mountain shall develop, document, and maintain physical and logical diagrams of networking devices and traffic.

8.4 Application Vulnerability Assessments/Ethical Hacking. Iron Mountain shall, at least annually, perform vulnerability assessments on applications in its hosted environment(s) used to provide services that Process Customer Personal Data. Detailed results are the confidential and proprietary information of Iron Mountain and will not be provided.

8.5 Change Testing and Review. Iron Mountain shall review and test changes to applications and operating systems prior to deployment to ensure there is no adverse effect on Customer Personal Data or systems.

9. DISASTER RECOVERY

Iron Mountain shall maintain a disaster recovery plan, including replication of systems and electronic data used to support the Services to a backup data center. Replication of systems and electronic data does not include Customer Personal Data that is physically stored in an Iron Mountain facility. Iron Mountain will maintain a business continuity plan for restoring critical business functions. Iron Mountain will perform disaster recovery testing no less frequently than once every twelve (12) months.

10. EXTERNAL AUDITS AND ASSESSMENTS

Iron Mountain's security protocols are designed to be consistent with industry standards. Iron Mountain will provide Customer with any third-party independent audit reports it has commissioned (e.g., PCI, ISO27001, SOC2, etc.) relevant to the Services in the region such Services are provided ("Audit Report"). Iron Mountain will provide all such reports commissioned with the intent of being customer-facing, regardless of the results of the report. Iron Mountain will not be required to provide internal audit results or results from other independent assessments which were commissioned with the intention of being confidential to Iron Mountain. Customer and its external auditors will be provided copies of the Audit Report upon request. Any Audit Report or other result generated through the tests or audits required by this section will be considered the Confidential Information of Iron Mountain. Customer shall have the right to provide a copy of such Audit Report to any applicable customers or regulators of Customer, subject to confidentiality provisions as restrictive as those herein. At Customer's request, Iron Mountain shall confirm in writing that there have been no changes in the relevant policies, procedures and internal controls since the completion of any such Audit Report, not to extend more than three months from end of reporting period of the Audit Report.

ANNEX 3

International Data Transfers

1. DEFINITIONS

"**2021 EU Standard Contractual Clauses**" means the standard contractual clauses for the transfer of Personal Data to third countries pursuant to the GDPR, adopted by the European Commission under Commission Implementing Decision (EU) 2021/914, available here[3].

"**2022 UK Addendum**" means template Addendum B.1.0 issued by the United Kingdom Information Commissioner's Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it may be revised under Section 18 thereof, available here[4].

"**EU Customer Personal Data**" means the Processing of Customer Personal Data to which data protection laws of the European Union, or of a Member State of the European Union or European Economic Area, was applicable prior to its processing by Iron Mountain;

"**Protected Area**" means:

i. in the case of EU Customer Personal Data, the members states of the European Union and the European Economic Area and any country, territory, sector or international organisation in respect of which an adequacy decision under Art.45 GDPR is in force;

ii. in the case of UK Customer Personal Data, the United Kingdom and any country, territory, sector or international organisation in respect of which an adequacy decision under United Kingdom adequacy regulations is in force;

iii. in the case of Swiss Customer Personal Data, any country, territory, sector or international organisation which is recognised as adequate under the laws of Switzerland;

iv. in the case of any other Customer Personal Data transferred out of a jurisdiction offering similar protections to those of EU, UK or Swiss Customer Personal Data, any country, territory, sector or international organisation which is recognised as adequate under the laws of such jurisdiction;

"**Standard Contractual Clauses**" means collectively 2021 EU Standard Contractual Clauses and the 2022 UK Addendum.

"**Swiss Customer Personal Data**" means the Processing of Customer Personal Data to which data protection laws of Switzerland were applicable prior to its Processing by Iron Mountain;

"**UK Customer Personal Data**" means the Processing of Customer Personal Data to which data protection laws of the United Kingdom were applicable prior to its processing by Iron Mountain;

2. MISCELLANEOUS

2.1 This Annex 3 includes the following Parts: (i) Part A – Transfers of EU Customer Personal Data; (ii) Part B – Transfers of Swiss Customer Personal Data; (iii) Part C – Transfer of UK Customer Personal Data, which shall apply as relevant for the transfer of Customer Personal Data by Iron Mountain in connection with its Services.

2.2 The Standard Contractual Clauses shall apply to Iron Mountain and its affiliates as "data importers" and to the Customer and its affiliates as "data exporters."

2.3 The signature to and dating of the Agreement shall constitute all required signatures and dates for the Standard Contractual Clauses.

2.4 In the event that the parties transfer EU, UK or Swiss Customer Personal Data outside the Protected Area and a relevant European Commission decision or other valid adequacy method under applicable Data Protection Legislation on which Iron Mountain has relied upon for the data transfer is held to be invalid, or that any supervisory authority requires transfers of Personal Data made pursuant to such decision to be suspended, then the parties shall cooperate and facilitate the use of an alternative transfer mechanism. The parties also agree that the appropriate safeguards used to facilitate international transfers in this Annex 3 are not exclusive and that the parties can pursue additional transfer mechanisms, such as the EU-U.S. Data Privacy Framework.

PART A – TRANSFERS OF EU CUSTOMER PERSONAL DATA

If and to the extent that the Customer or its Affiliates transfer EU Customer Personal Data outside the Protected Area to Iron Mountain or its Affiliates in connection with Iron Mountain's Services under the Agreement, this Part A of Annex 3 shall apply, and the Parties agree as follows:

[3] https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj
[4] https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf

1. **Standard Contractual Clauses selections.** The text from MODULE TWO of the 2021 EU Standard Contractual Clauses shall apply where the Customer or any of its Affiliates is a Controller, and Iron Mountain or any of its Affiliates is a Processor; the text from MODULE THREE of the 2021 EU Standard Contractual Clauses shall apply where the Customer or any of its Affiliates is a Processor, and Iron Mountain or any of its Affiliates is sub-Processor. The relevant provisions contained in the 2021 EU Standard Contractual Clauses are incorporated by reference into this DPA and are an integral part of this DPA. No other modules or any clauses marked as optional in the 2021 EU Standard Contractual Clauses shall apply. The information required for the purposes of the Appendices to the 2021 EU Standard Contractual Clauses are set out in Annex 1 – Description of the Processing/Transfer, Annex 2 – Technical and Organizational Measures, and Clause 6.2 of the DPA – List of sub-Processors.

2. **Use of Sub-Processors.** For the purposes of clause 9 of the 2021 EU Standard Contractual Clauses, option 2 (General Written Authorization) to the use of sub-Processors for the performance of the Services shall apply. The Customer acknowledges and agrees that Iron Mountain may engage new sub-Processors through the mechanism agreed in clause 6 of this DPA and that the time period for submitting requests for changes to sub-processors shall be fifteen (15) days.

3. **Governing law and choice of forum.** For the purposes of clause 17 of the 2021 EU Standard Contractual Clauses (Governing Law), option 2 governing law shall apply, and these clauses shall be governed by the law of the EU Member State in which the data exporter is established, to the extent it allows for third party beneficiary rights. For the purposes of clause 18 of the 2021 EU Standard Contractual Clauses (Choice of Forum and Jurisdiction) these shall be the courts of the EU Member State in which the data exporter is established.

4. **Certification of deletion.** For the purposes of Clause 8.5 and 16(d) of the 2021 EU Standard Contractual Clauses, a certification of deletion of Personal Data shall be provided by Iron Mountain to the Customer only upon Customer's written request.

5. **Personal data breaches.** For the purposes of clause 8.6(c) of the 2021 EU Standard Contractual Clauses, personal data breaches shall be handled in accordance with the mechanism agreed in clause 7 of the DPA.

6. **Audits.** For the purposes of clause 8.9 of the 2021 EU Standard Contractual Clauses, audits of these clauses shall be carried out in accordance with the audit mechanism agreed in the Agreement.

7. **Complaints.** For the purposes of clause 11 of the 2021 EU Standard Contractual Clauses, Iron Mountain shall inform the Customer if it receives a complaint from a Data Subject with respect to EU Customer Personal Data and shall communicate the complaint to the Customer in accordance with the mechanism agreed in the Agreement.

8. **Supervisory Authority.** For the 2022 EU Standard Contractual Clauses, the relevant competent supervisory authority shall be determined in accordance with clause 13 of the EU Standard Contractual Clauses.

PART B – TRANSFERS OF SWISS CUSTOMER PERSONAL DATA

If and to the extent that the Customer or its affiliates transfer Swiss Customer Personal Data outside the Protected Area to Iron Mountain or its affiliates in connection with Iron Mountain's Services under the Agreement, this Part B of Annex 3 shall apply, and the Parties agree as follows:

1. **Standard Contractual Clauses selections.** The 2021 EU Standard Contractual Clauses and relevant provisions under Part A shall apply where the Customer or any of its Affiliates is a Controller, and Iron Mountain or any of its Affiliates is a Processor, and/or Customer or any of its Affiliates is a Processor, and Iron Mountain or any of its Affiliates is a sub-Processor, except that:

   a. the competent supervisory authority under the Clause 13 of the 2021 EU Standard Contractual Clauses shall be the Swiss Federal Data Protection and Information Commission;

   b. the applicable law for contractual claims under clause 17 of the 2021 EU Standard Contractual Clauses shall be Swiss law and the place of jurisdiction for actions between the parties pursuant to clause 18 (b) shall be the Swiss courts.

2. References to the EU GDPR in the 2021 EU Standard Contractual Clauses are to be understood as references to the FADP.

3. The term "member state" in the 2021 EU Standard Contractual Clauses shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 (c) of the 2021 EU Standard Contractual Clauses.

PART C – TRANSFERS OF UK CUSTOMER PERSONAL DATA

If and to the extent that the Customer or its Affiliates transfer UK Personal Data outside the Protected Area to Iron Mountain or its Affiliates in connection with Iron Mountain's Services under the Agreement, this Part C of Annex 3 shall apply, and the Parties agree as follows:

1. **Standard Contractual Clauses selections.** The 2021 EU Standard Contractual Clauses, relevant provisions under Part A, and the 2022 UK Addendum shall apply where the Customer or any of its Affiliates is a Controller, and Iron Mountain or any of its affiliates is a Processor, and/or Customer or any of its Affiliates is a Processor, and Iron Mountain or any of its Affiliates is a sub-Processor.

2. **Part 1: Table 1 - 3 of the 2022 UK Addendum:** Information about the Parties - Table 1; Selected SCCs, Modules and Selected Clauses; and Appendix Information, including Annex 1A: List of Parties, Annex 1B: Description of Transfer and Annex 1C: Technical and organizational measures to ensure the security of data - Table 3, shall be considered completed by reference to this Annex 3, including Part A. Table 4 of the UK Addendum: Customer and Iron Mountain acknowledge and agree that the UK Addendum may be terminated by either Party.

3. **Part 2:** Mandatory Clauses of the UK Addendum: Customer and Iron Mountain acknowledge and agree to the Mandatory Clauses of the UK Addendum.

4. **Supervisory Authority.** The UK Information Commissioner's Office shall act as competent supervisory authority.

PART D – TRANSFERS OF OTHER CUSTOMER PERSONAL DATA

If and to the extent that the Customer or its affiliates transfer Customer Personal Data not covered under PART A-C to Iron Mountain or its affiliates in connection with Iron Mountain's Services under the Agreement, Part A of Annex 3 shall apply to the extent relevant and applicable under the applicable Data Protection Legislation. Otherwise, to the extent that any substitute or additional appropriate safeguards or transfer mechanisms under Data Protection Legislation are required to transfer Customer Personal Data to a country that does not provide adequate level of protection for Personal Data from the perspective of the data exporter, the parties agree to implement the same as soon as practicable and document such requirements for implementation in an attachment to this DPA.

ANNEX 4

HIPAA – Business Associate Agreement ("BAA")

This BAA supplements and amends any and all current or future Agreements entered into between Iron Mountain and its affiliates and Customer and its affiliates under which Iron Mountain or its affiliates is providing certain Services for Customer or its affiliates, which Services require the Business Associate to Use and/or Disclose PHI on behalf of the Covered Entity. Except to the extent modified in this BAA, all terms and conditions set forth in the Agreement shall remain in full force and effect and govern the Services provided by Iron Mountain to Customer.

Iron Mountain and Customer are entering into this BAA in order for both parties to meet their respective obligations as they become effective and binding upon the parties under the HIPAA Privacy, Security, and Breach Notification Rules along with any implementing regulations including those implemented as part of the Omnibus Rule (collectively referred to as the "HIPAA Rules"), under which Customer and its affiliates is a "Covered Entity" or "Business Associate" and Iron Mountain and its affiliates is a "Business Associate" of Customer. For purposes of this Agreement, any references hereinafter to Business Associate shall be deemed references to Iron Mountain or its applicable affiliate.

1. DEFINITIONS

Capitalized terms used but not otherwise defined in this BAA shall have the same meaning as ascribed to those terms in HIPAA Rules or in the Agreement, as applicable.

"**Breach Notification Rule**" shall mean the rule for Breach Notification for Unsecured Protected Health Information at 45 CFR §164 Subpart D.

"**Business Associate**" shall mean the Business Associate entity identified above to the extent it receives, maintains, or transmits Protected Health Information in delivering Services to Customers.

"**HIPAA**" shall mean the Health Insurance Portability and Accountability Act of 1996.

"**HITECH Act**" shall mean the applicable provisions of the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009, and including any implementing regulations.

"**Privacy Rule**" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR §160 and §164, Subparts A and E.

"**Protected Health Information**" or "**PHI**" shall have the same meaning as the term 'protected health information' in 45 CFR §160.103 and shall be limited to the PHI created by Business Associate on behalf of Customer or received from or on behalf of Customer pursuant to the Agreement.

"**Security Rule**" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR §160 and §164, Subparts A and C.

2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

2.1. Business Associate agrees to not Use or further Disclose PHI other than as permitted or required by this BAA or as required by law.

2.2. Business Associate agrees to use appropriate safeguards, and comply, as applicable, with Subpart C of 45 CFR §164 with respect to electronic PHI, to prevent Uses or Disclosures of the PHI other than as provided for by this BAA or the Agreement; however, the parties acknowledge and agree it shall be the responsibility of Customer and not Business Associate to comply with requirements under 45 CFR §164.312 to implement encryption or decryption mechanisms for electronic PHI maintained on physical media (e.g., tapes) stored by Customer with Business Associate.

2.3. Business Associate agrees to promptly report to Customer any Security Incident, Breach, or other Use or Disclosure of PHI of which it becomes aware that is not permitted or required by this BAA or the Agreement. In the event of a Breach, such notification shall be made in accordance with and as required of a business associate by the HIPAA Rules, including without limitation pursuant to 45 CFR 164.410, but in no event more than three (3) business days after Business Associate has completed its internal investigation and confirmed a Breach as occurred. Business Associate will provide reasonable assistance and cooperation in the investigation of any such Breach and shall document the specific Deposits which have been compromised, the identity of any unauthorized third party who may have accessed or received the PHI, if known, and any actions that have been taken by Business Associate to mitigate the effects of such Breach.

2.4. Business Associate shall, in accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), as applicable, ensure that any business associate that is a subcontractor that creates, receives, maintains, or transmits PHI on behalf of Business Associate for the purpose of assisting in providing Services pursuant to the Agreement, agrees to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such PHI through this BAA.

2.5. If Business Associate has custody of PHI in a Designated Record Set with respect to Individuals, and if Customer so requests, Business Associate agrees to provide access to such PHI to Customer by retrieving and delivering such PHI in accordance with the terms and conditions of the Agreement, so Customer may respond to an Individual in order to meet the requirements of 45 CFR §164.524.

2.6. Business Associate agrees that if an amendment to PHI in a Designated Record Set in the custody of Business Associate is required, and if Customer instructs Business Associate to retrieve such PHI in accordance with the Agreement, Business Associate shall perform such service so that Customer may make any amendment to such PHI as may be required by either Customer or an Individual pursuant to 45 CFR §164.526.

2.7. Business Associate agrees to document and make available to Customer the information required to provide an accounting of Disclosures of PHI, provided that Customer has provided Business Associate with information sufficient to enable Business Associate to determine which records or data received from or on behalf of Customer by Business Associate contain PHI. The documentation of Disclosures shall contain such information as would be required for Customer to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR §164.528 or other provisions of the HIPAA Rules.

2.8. Unless otherwise expressly agreed in the Agreement, Business Associate shall promptly notify Customer of any requests by Individuals for access to or knowledge or correction of PHI, without responding to such requests, and Customer shall be responsible for receiving and responding to any such Individual requests.

2.9. To the extent the Business Associate is to carry out one or more of Customer's obligation(s) under Subpart E of 45 CFR §164, Business Associate shall comply with the requirements of Subpart E that apply to Customer in the performance of such obligation(s).

2.10. Business Associate agrees to make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

3. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

3.1. Business Associate may Use or Disclose PHI as necessary to perform the Services set forth in the Agreement.

3.2. Business Associate may Use or Disclose PHI as required by law.

3.3. Business Associate agrees to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the Use, Disclosure, or request.

3.4. Business Associate may not Use or Disclose PHI in a manner that would violate Subpart E of 45 CFR §164 if done by Customer.

3.5. Business Associate may Disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of the Business Associate, provided the Disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

4. OBLIGATIONS OF CUSTOMER

4.1. Customer shall not direct Business Associate to act in a manner that would not be compliant with the HIPAA Rules.

4.2. Customer shall notify Business Associate of any limitation(s) in its notice of privacy practices of Customer in accordance with 45 CFR §164.520, to the extent that such limitation may affect Business Associate's Use or Disclosure of PHI.

4.3. Customer shall notify Business Associate of any changes in, or revocation of, the permission by an Individual to Use or Disclose their PHI, to the extent that such changes may affect Business Associate's Use or Disclosure of PHI.

4.4. Customer shall notify Business Associate in writing of any restriction to the Use or Disclosure of PHI that Customer has agreed to in accordance with 45 CFR §164.522, to the extent that such restriction may affect Business Associate's Use or Disclosure of PHI.

5. TERM AND TERMINATION

5.1. The term of this BAA shall commence as of the Effective Date and shall terminate automatically upon the later to occur of (i) the expiration of the Agreement, or (ii) when all PHI provided by Customer to Business Associate is destroyed or returned to Customer.

5.2. Upon a party's knowledge of a material breach of the BAA by the other party, the non-breaching party shall provide an opportunity for the breaching party to cure the breach. If the breaching party does not cure the breach within thirty (30) days, following the breaching party's receipt of a written notice from the non-breaching party setting forth the details of such material breach, then the non-breaching party shall have the right to terminate this BAA and the Agreement according to the terms of the Agreement, or, if termination is not feasible, shall report the problem to the Secretary or any other competent authority.

5.3. Effect of Termination:

5.3.1.1. Except as provided in 5.3.2 below, upon termination of this BAA for any reason, Business Associate shall return or destroy all PHI received from Customer in accordance with the Agreement. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.

5.3.1.2. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Customer notification of the conditions that make return or destruction infeasible. Upon notice to Customer, Business Associate shall extend the protections of this BAA to such PHI and limit further Uses and Disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI pursuant to the terms of the Agreement.

6. MISCELLANEOUS

6.1. Indemnification. Business Associate agrees to indemnify Customer from and against any fines or penalties imposed upon Customer as a result of any enforcement proceeding commenced by the Secretary or any civil action brought by a state Attorney General against Customer, which proceeding or action results directly and solely from any act or omission by Business Associate which is either a violation of the HIPAA Rules or a material breach of this BAA ("Claim"). Business Associate shall not be obligated to indemnify Customer for any portion of such fines or penalties resulting from (i) Customer's violation of the HIPAA Rules or this BAA, or (ii) the negligent or intentional acts or omissions of Customer. The foregoing indemnity obligation is expressly conditional on Customer granting Business Associate the right at Business Associate's option and expense, and with counsel of its own selection, to control or participate in the defence of any such Claim, provided however, that to the extent any such Claim is part of a larger proceeding or action, Business Associate's right to control or participate shall be limited to the Claim, and not to the larger proceeding or action. In the event that Business Associate exercises its option to control the defence, then (i) Business Associate shall not settle any claim requiring any admission of fault on the part of the Customer without its prior written consent, (ii) the Customer shall have the right to participate, at its own expense, in the claim or suit and (iii) the Customer shall cooperate with the Business Associate as may be reasonably requested. The foregoing states Customer's sole and exclusive remedy and Business Associate's sole liability for any loss, damage, expense or liability of Customer for any Claims in connection with this BAA.

6.2. Injunctive Relief. Business Associate acknowledges that any unauthorized Use or Disclosure of PHI by Business Associate may cause irreparable harm to Customer for which Customer shall be entitled, if it so elects, to seek injunctive or other equitable relief.

6.3. Regulatory References. A reference in this BAA to a section of the HIPAA Rules shall mean that section of HIPAA, the Privacy Rule, the Security Rule, the HITECH ACT, or the final Omnibus Rules as amended and in effect, and for which compliance is required.

6.4. Amendment. The parties agree to negotiate in good faith any amendment to this BAA that may be required from time to time as is necessary for the Customer or Business Associate to comply with the requirements of the HIPAA Rules. If the parties cannot reach mutual agreement on the terms of any such amendment within sixty (60) days following the date of receipt of any such written request made by Customer to Business Associate, then either party shall have the right to terminate this BAA and the Agreement upon providing not less than thirty (30) days written notice to the other party.

6.5. No Third Party Beneficiaries. Nothing expressed or implied in this BAA is intended to confer, nor shall anything herein confer, upon any person other than Customer, Business Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

6.6. Independent Contractor. Business Associate, including its directors, officers, employees and agents, is an independent contractor and not an agent (as defined under Federal common law of agency) of Customer or a member of its workforce. Without limiting the generality of the foregoing, Customer shall have no right to control, direct, or otherwise influence Business Associate's conduct in the course of performing the services, other than through the enforcement of this BAA or the Agreement, or the mutual amendment of same.

6.7. Precedence; Entire Agreement. Any ambiguity in this BAA shall be resolved to permit the parties to comply with the HIPAA Rules. This BAA constitutes the entire agreement between the parties with respect to the subject matter hereof, and shall supersede all previous communications, representations, agreements and understandings relating to the HIPAA Rules, including any and all prior business associate agreements between the parties.