



## IRON MOUNTAIN INSIGHT® SERVICES

### TERMS AND CONDITIONS

These Iron Mountain InSight® Services terms and conditions and Appendix A (these “**Terms and Conditions**”) shall govern any Statements of Work, exhibits and addenda in which they are referenced (which together shall form the “**Agreement**”). Customer and Iron Mountain are each referred to as a “**Party**” and collectively, the “**Parties**.” In consideration of the mutual promises contained herein, the Parties hereby agree to the following:

**1. DEFINITIONS.** Capitalized terms shall have the meanings set forth in this section, or in the section where they are first used.

“**Access Protocols**” means the usernames, passwords, access codes, encryption keys, service accounts, technical specifications, connectivity standards or protocols, or other relevant procedures, as may be necessary to allow Customer to access the Services.

“**Affiliates**” means those entities controlling, controlled by, under common control with, or having a common parent with, either Iron Mountain or Customer as applicable. For purposes of the foregoing definition, “control” (including “controlling”, “controlled by” and “under common control with”) shall mean direct or indirect ownership of: (a) not less than fifty percent (50%) of the voting stock of a corporation; (b) the right to vote not less than fifty percent (50%) of the voting stock of a corporation; or (c) not less than fifty percent (50%) ownership interest in a partnership or other business entity.

“**AUP**” means the acceptable use policy for Iron Mountain’s hosting provider, currently found at: <https://cloud.google.com/terms/aup>, or <https://aws.amazon.com/aup/>, which may be updated from time to time by the Host (as defined in Section 5.5).

“**Authorized User**” means any individual who is an employee of Customer or such other person as may be authorized by Customer to access the InSight Services pursuant to Customer’s rights under these Terms and Conditions. An Authorized User is granted access using the Customer-owned identity provider (“**IDP**”) or through an Iron Mountain- managed IDP.

“**Customer Data**” means all content, data and information that is input or uploaded to, or collected, received, processed, or stored in the InSight Services by or on behalf of Customer, and all derivative data thereto, including but not limited to derivative data created in accordance with an SOW. For the avoidance of doubt, Customer Data does not include Usage Data or any other information reflecting the access or use of the InSight Services by or on behalf of Customer or any Authorized User.

Iron Mountain InSight®– Terms and Conditions (August 2023)  
©2023 Iron Mountain Incorporated

of doubt, Customer Data does not include Usage Data or any other information reflecting the access or use of the InSight Services by or on behalf of Customer or any Authorized User.

“**Documentation**” means the user manuals, training materials, reference guides, instruction materials, help files and similar documentation provided by Iron Mountain or its suppliers to Customer in hard copy or electronic form or available on Iron Mountain’s online portal describing the use, operations, features, functionalities, user responsibilities, procedures, commands, requirements, limitations and capabilities of and/or similar information about the Services.

“**Encrypted**” or “**encrypted**” shall mean data that has been rendered through algorithmic transformation or any other means available into an unrecognizable form in which meaning cannot be understood without the use of a confidential process or key.

“**High Risk Activities**” means uses such as, without limitation, the operation of nuclear facilities, air traffic control, or life support systems, where the use or failure of the Services could lead to death, personal injury, or environmental damage.

“**Implementation Services**” means the implementation services documented in an SOW relating to the InSight Services, including service details related to IDP integration, security controls and special accommodations, which require Iron Mountain assistance to implement.

“**InSight Services**” means the Iron Mountain InSight hosted SaaS solution, as described in a Statement of Work.

“**Intellectual Property Rights**” means any and all now known or hereafter existing: (a) rights associated with works of authorship, including copyrights, maskwork rights, and moral rights; (b) trademark or servicemark rights; (c) trade secret rights; (d) patents, patent rights, and industrial property rights; (e) layout design rights, design rights, and other proprietary rights of every kind



and nature other than trademarks, service marks, trade dress, and similar rights; and (f) all registrations, applications, renewals, extensions, or reissues of the foregoing, in each case in any jurisdiction throughout the world.

“**Iron Mountain ML**” means Iron Mountain’s machine learning and artificial intelligence technology including all modifications, derivative works and improvements thereto developed by either Party or a third party.

“**Professional Services**” means the training, customization, Implementation Services, data ingestion, consulting or other services Iron Mountain or its suppliers may perform for the benefit of Customer in connection with the InSight Services as described as Professional Services in a Statement of Work.

“**Services**” means the InSight Services, Professional Services and Support Services, as may be set forth in a Statement of Work.

“**Services Technology**” means the software, databases, platforms, Iron Mountain ML and other technologies used by or on behalf of Iron Mountain in performing the Services, whether operated directly by Iron Mountain or through the use of third-party services.

“**Service Term**” means the initial term of Customer’s authorized use of the Services, as set forth in the applicable Statement of Work, together with any renewal terms. The initial term begins on the earlier of: (i) the date Customer starts using or receiving the Services; or (ii) the effective date set out in the Statement of Work.

“**Statement of Work**” or “**SOW**” means a document that: (a) contains details regarding the Services to be performed or provided, including pricing and other specifics, (b) is mutually agreed upon and executed by the Parties, and (c) incorporates these Terms and Conditions to form the Agreement.

“**Support Services**” means the support services and related maintenance for the InSight Services purchased by Customer as described in a Statement of Work.

“**Usage Data**” means any diagnostic and usage-related information from the use, performance and operation of the InSight Services, including, but not limited to, type of browser, Service features, and systems that are

used and/or accessed, and system and Service performance-related data.

## 2. PROVISION OF SERVICES

**2.1 Services Use.** Subject to and conditioned on Customer’s and its Authorized Users’ compliance with these Terms and Conditions, Iron Mountain hereby grants Customer a non-exclusive, non-transferable right, during the Term, solely for Customer’s internal business purposes and in accordance with the limitations and restrictions contained herein, to: (a) access and use the InSight Services in accordance with these Terms and Conditions and the Documentation; and (b) use the Documentation solely to support Customer’s use of the InSight Services. Iron Mountain may change or modify the Documentation and Services, including adding or removing features and functions, from time to time, provided that in no event will such modifications materially reduce the functionality provided to Customer during the Term.

**2.2 Access Protocols.** Iron Mountain will provide the Services to Customer at the rates and charges set forth in the applicable Statement(s) of Work. Iron Mountain will work with the Customer to provide access through the Access Protocol implementation process, including providing Customer with training on user account setup and access control implementation with the applicable IDP. Customer is solely responsible for obtaining and maintaining its equipment, computers, networks, and communications, including Internet access, required to access and utilize the Services and for all expenses related thereto. Iron Mountain is not responsible for any issues relating to access attributable to Customer or any third party. Customer agrees to maintain and update an industry standard anti-virus program within its computer systems that are used in connection with the Services.

**2.3 Authorized Users.** Customer may designate its Authorized Users and grant their access rights to the features and functions of the InSight Services. Usernames and passwords (“**User IDs**”) cannot be shared or used by more than one Authorized User at a time. Depending on the agreed login and authorization implementation, Iron Mountain may assist the Customer with establishing User IDs for Customer’s Authorized User who has been designated as a “User Manager” and provide such User Manager with rights to create, control and manage its portfolio of Authorized Users, including, but not limited to, the number of Authorized Users and all User IDs, in accordance with the Access Protocols. Customer shall not disclose or make available User IDs or other Access Protocols other than to Customer’s Authorized Users and shall prevent



unauthorized access to, or use of, the InSight Services, and will notify Iron Mountain promptly of any actual or suspected unauthorized use. Customer is solely responsible for management of the User IDs, access rights and the acts and omissions of its Authorized Users. Customers shall immediately terminate an Authorized User's access to InSight Services if such individual is no longer employed or engaged by Customer, engages in inappropriate activity, or is otherwise no longer authorized to have access. Customer is responsible for ensuring all Authorized Users comply with Customer's obligations under these Terms and Conditions. Iron Mountain reserves the right to: (a) track and review user profiles, access and activity at any time; and (b) terminate any User ID that it reasonably determines may have been used in a way that breaches this Section 2.3.

**2.4 Professional Services.** Iron Mountain will provide Professional Services as may be mutually agreed to by the Parties from time to time and set forth in a Statement of Work. Each Statement of Work will be governed by these Terms and Conditions. Iron Mountain shall have the right to remove, reassign, or take any other employment related action in regard to any of its personnel furnished to provide Professional Services. In the event of such removal or reassignment, Iron Mountain will furnish a replacement of similar skills and capability. Iron Mountain reserves the right to hire temporary workers or subcontractors to perform the service, provided those workers possess the skills required to perform the Professional Services.

### 3. INTELLECTUAL PROPERTY

**3.1 Ownership.** Subject to Section 3.4 (Open Source Software), the Services, Documentation, Usage Data, Iron Mountain ML and all other materials provided by Iron Mountain hereunder, including but not limited to all manuals, reports, records, programs, information, and data (that is not Customer Data or Customer's Intellectual Property thereto), together with all know-how, enhancements, modifications, corrections, improvements, adaptations, new applications, and derivative works relating to the same, derived from the same or created in connection with the same, and all worldwide Intellectual Property Rights in each of the foregoing ("IM Materials"), are the exclusive property of Iron Mountain and its suppliers. To the extent any rights in the Services, Documentation or Usage Data vest in Customer, Customer hereby unconditionally and irrevocably assigns to Iron Mountain any and all such rights, title and/or interest including Intellectual Property Rights relating thereto. Iron Mountain InSight®- Terms and Conditions (August 2023)

©2023 Iron Mountain Incorporated

All rights in and to IM Materials not expressly granted to Customer under the Agreement are reserved by Iron Mountain and its suppliers. Except as expressly set forth herein, no express or implied license or right of any kind is granted to Customer regarding the IM Materials or any part thereof, including any right to obtain possession of any source code, data or other technical material related to the Services. Nothing hereunder shall act so as to assign or otherwise transfer Customer's ownership of Customer Data to any other party.

**3.2 License; Ownership.** Customer Data hosted by Iron Mountain as part of the Services, and all worldwide Intellectual Property Rights in such data, are the exclusive property of Customer. Customer grants Iron Mountain and its suppliers an irrevocable, non-exclusive, worldwide, royalty-free and fully paid-up license to access, use, reproduce, modify, display, process and store the Customer Data for purposes of providing the Services to the Customer. Moreover, if training Iron Mountain ML is expressly contemplated in an SOW, Iron Mountain may access, use, reproduce, copy, modify, internally display, process, store, or otherwise create derivative works of Customer Data to build, train and maintain the Iron Mountain ML used to provide the Services. Iron Mountain may freely use and license Iron Mountain ML, provided that Iron Mountain will remove Customer Data in Iron Mountain ML or otherwise, after expiration or termination of the Agreement pursuant to Section 11.5, and will not otherwise share such data with other customers. All rights in and to the Customer Data not expressly granted to Iron Mountain in the Agreement are reserved by Customer. Under these Terms and Conditions, the Parties acknowledge and agree that Iron Mountain is a data processor and service provider.

**3.3 Restrictions on Use.** Customer shall not permit any party to access or use the Services, Services Technology or Documentation, other than the Authorized Users. Except as expressly permitted by these Terms and Conditions, Customer agrees that it will not, and will not permit any of its Authorized Users or other party to: (a) copy, modify, adapt, alter or translate, in whole or in part, or create derivative works of, the Services Technology, Documentation or any component thereof; (b) license, sublicense, sell, resell, lease, rent, loan, timeshare, transfer, assign, distribute, disclose or otherwise commercially exploit or make available, in whole or in part, the Services, Services Technology or Documentation to any third party; (c) reverse engineer, decompile, disassemble (except to the extent applicable laws specifically prohibit such restriction), decode, adapt or otherwise in any manner attempt to obtain, create or recreate, derive or attempt to derive, determine or gain access to the source code (or the underlying



ideas, algorithms, structure or organization) of the Services, Services Technology, Documentation or any component thereof, in whole or in part, except to the extent expressly permitted by applicable law (and then only upon advance written notice to Iron Mountain); (d) disclose or transmit any information regarding the Services, Services Technology or Documentation to any individual other than an Authorized User; (e) use or access the Services, Services Technology or Documentation for competitive analysis or to build a similar product; (f) use the Services, Services Technology or any component thereof: (I) to send or store infringing, threatening, harassing, defamatory, libelous, obscene, pornographic, indecent or otherwise unlawful or tortious material, including material harmful to children or violating third party privacy rights, (II) to send or store material containing software viruses, worms, Trojan horses or other harmful computer code, files, scripts, agents or programs, (III) for High Risk Activities, (IV) in any manner or for any purpose that infringes, misappropriates, or otherwise violates any Intellectual Property Rights or other right of any person or that violates any applicable law, or (V) to benefit any third party (other than an Authorized User) or otherwise incorporate the same into a product or service Customer provides to a third party (other than Authorized Users); (g) perform benchmarking analysis or disclose the results of any benchmark test of Services, Services Technology or Documentation to any third party; (h) interfere with or disrupt the integrity or performance of the Services, Services Technology or the data contained therein; (i) access, use or share any data other than Customer Data; (j) bypass or breach any security device or protection used for or contained in the Services or Services Technology or otherwise attempt to gain unauthorized access to the Services, Services Technology or its related systems or networks, or otherwise circumvent mechanisms intended to limit use; (k) remove, erase, modify, tamper, obscure, or fail to preserve any proprietary, copyright or other notices; or (l) unless expressly agreed to in a relevant SOW, let, encourage or assist any third party, automated software, robotic process automation, scraper or other tool to do any of the foregoing (a)-(k). Unless otherwise specified in writing by Iron Mountain, Iron Mountain does not intend use of the Services to create obligations under the Health Insurance Portability and Accountability Act of 1996 as it may be amended from time to time and any regulations issued under it (“HIPAA”), and Iron Mountain makes no representations that the Services satisfy HIPAA requirements. Customer shall not provide Iron Mountain access to, nor use the Services for any purpose or in any manner involving Protected Health Information (as defined in HIPAA) unless specifically agreed to in writing by the Parties (through the execution of a Business Associate Agreement).

Iron Mountain InSight®- Terms and Conditions (August 2023)  
©2023 Iron Mountain Incorporated

**3.4 Open Source Software.** Iron Mountain shall take commercially reasonable measures to ensure that the Services and any other materials provided to Customer as part of the Services, unless expressly agreed to otherwise in writing by Customer, will not contain software that is made available by a third party under a free or open source software licensing model, if such model: (i) creates or purports to create contribution obligations with respect to any Customer software, or (ii) grants or purports to grant to any third party any rights to such Customer software (“FOSS”). To the extent any such FOSS is included in the Services, such FOSS is licensed under the terms of such third party license model and additional obligations may apply. Iron Mountain distributes and passes through such terms and conditions of such FOSS licenses to Customer to the extent necessary to comply with any such license obligations. Nothing in these Terms and Conditions enlarges or curtails Customer’s rights under, or otherwise grants Customer rights that supersede, the terms and conditions of any applicable FOSS license.

**3.5 Feedback.** If Customer provides Iron Mountain any feedback or suggestions about the Services, Services Technology or Documentation (the “Feedback”), then Iron Mountain may use such information without obligation to Customer, and Customer hereby irrevocably assigns all rights, title and interest in the Feedback to Iron Mountain.

#### 4. FEES AND EXPENSES; PAYMENTS

**4.1 Fees.** In consideration for the access rights granted to Customer and the Services performed by Iron Mountain under the Agreement, Customer will pay to Iron Mountain the fees set forth in the applicable Statement(s) of Work. Fees and charges during the Service Term shall be as set forth in the applicable Statement(s) of Work, and may thereafter be changed at any time by Iron Mountain upon thirty (30) days’ written notice.

**4.2 Payment Terms.** Payment terms are net, thirty (30) days from invoice date unless otherwise specified in the relevant SOW. Customer shall be liable for late charges totaling one and a half percent (1.5%) per month of the outstanding balance unless otherwise specified in the pricing in the relevant SOW. Invoices will be sent electronically in Iron Mountain’s standard format via Iron Mountain’s standard delivery system to Customer. Customer shall provide written notice of any charges it disputes on an invoice no later than fifteen (15) days after the invoice date. Any credit issued will appear on the next invoice. Payment of the invoice in



full will constitute agreement with the terms and charges of the invoice. All payments must be made by electronic transfer. At any time during the term of this Agreement, Iron Mountain may require Customer to enroll in autopay. Autopay will be required for customers who are consistently late payers or customers who meet our revenue thresholds. Any change to the Iron Mountain's standard electronic payment method must be approved by Iron Mountain. All payments shall include a remittance document identifying the Iron Mountain invoices to which the payment relates. If Customer fails to pay Iron Mountain's charges (other than disputed charges) sixty (60) days after the date of an invoice, Iron Mountain may suspend service. If Customer fails to pay Iron Mountain's charges (other than disputed charges) for three (3) months after the due date of the invoice, such failure shall be deemed a material breach and Iron Mountain may terminate this Agreement pursuant to Section 11. Customer will be responsible and reimburse Iron Mountain for any costs incurred by Iron Mountain in collecting overdue amounts, including the use of third parties and reasonable attorneys' fees. Iron Mountain shall have other rights and remedies as may be provided by law. In the event Iron Mountain takes any actions pursuant to this Section 4, it shall have no liability to Customer or anyone claiming by or through Customer. If a purchase order is required by Customer for payment, Customer shall issue an accurate and complete purchase order through Iron Mountain's standard mediums prior to performance by Iron Mountain of services. Customer will be responsible for keeping all necessary purchase order information up to date. If Customer rejects any Iron Mountain invoice as a result of an inaccurate, invalid, incomplete or expired purchase order, Customer shall correct such purchase order within forty-eight (48) hours of request by Iron Mountain. In this case, the original payment due date shall apply. In the event that Customer issues a purchase order to Iron Mountain covering the services provided under this Agreement, any terms and conditions set forth in the purchase order which are in addition to or establish conflicting terms and conditions to those set forth in this Agreement are expressly rejected by Iron Mountain. Customer shall not be entitled to refund of any amount paid to Iron Mountain, except as explicitly provided for under these Terms and Conditions.

**4.3 Taxes.** The fees are exclusive of all applicable sales, use, value-added and other taxes, and all applicable duties, tariffs, assessments, export and import fees, or other similar charges, and Customer will be responsible for payment of all such taxes (other than taxes based on Iron Mountain's income), fees, duties, and charges and any related penalties and Iron Mountain InSight®- Terms and Conditions (August 2023)  
©2023 Iron Mountain Incorporated

interest, arising from the payment of the fees and the delivery of the Services to Customer under the Agreement. Customer will make all payments of feesto Iron Mountain free and clear of, and without reduction for, any withholding taxes; any such taxes imposed on payments of fees to Iron Mountain will beCustomer's sole responsibility, and Customer will provide Iron Mountain with official receipts issued bythe appropriate taxing authority, or such other evidence as Iron Mountain may reasonably request, toestablish that such taxes have been paid. Customer shall indemnify and defend Iron Mountain in connection with any proceedings brought by any taxing authorities in connection with Customer's breach of this Section 4.3.

## 5. CUSTOMER RESPONSIBILITIES

**5.1 Customer Warranty.** Customer represents and warrants that, to the extent Customer or Customer's third party provides Customer Data for the purposes herein: (a) it is the owner or legal custodian of the Customer Data; (b) it has given all necessary notices and obtained all necessary consents, authorizations and/or legal permissions required to direct and enable Iron Mountain and its suppliers to access, use and process the Customer Data as set forth in these Terms and Conditions and the related Statement(s) of Work; (c) will use the Services in accordance with all applicable data, privacy and security laws; and (d) any Customer Data hosted by Iron Mountain as part of the Services shall not (i) infringe any copyright, trademark, or patent; (ii) misappropriate any trade secret; (iii) be defamatory, obscene, pornographic or unlawful; (iv) contain any viruses, worms or other malicious computer programming codes intended to damage Iron Mountain's systems or data; or (v) otherwise violate the rights of a third party or violate any applicable law. Iron Mountain is not obligated to backup any Customer Data. Customer agrees that any useof the Services contrary to or in violation of the representations and warranties of Customer in this Section constitutes unauthorized and improper use of the Services. Customer will immediately notify Iron Mountain of any issues of which it becomes aware that could negatively impact Iron Mountain's ability to process the Customer Data in accordance with these Terms and Conditions. Customer (i) warrants that, if it is required, it has obtained all the necessary and explicit consent from its customers, employees or any other relevant entities or individuals whose data is provided by Customer to Iron Mountain and (ii) authorises Iron Mountain to handle and process such data, for the purposes of provision of services under this Agreement which may include, but not limited to, maintaining, using, deleting, disposing, storing and cross-border transferring of such data.



## 5.2 Customer Responsibility for Data and Security.

Customer and its Authorized Users shall have access to the Customer Data and shall be responsible for any and all: (a) changes to and/or deletions of Customer Data, maintaining the security and confidentiality of all User IDs and other Access Protocols required in order to use and access the InSight Services; (b) activities that occur in connection with such use and access. Iron Mountain and its suppliers are not responsible or liable for (i) the deletion of or failure to store any Customer Data by Customer or its Authorized Users; (ii) determining whether the security of the environment provided by Iron Mountain is commensurate with its needs, and (iii) long term backup copies of Customer Data. Notwithstanding the foregoing Iron Mountain will maintain resiliency and redundancy processes associated with the InSight Services to meet industry standards for storage of Customer Data. Customer is responsible for any long term backup or archival of the Customer Data that is provided to Iron Mountain. Iron Mountain shall maintain service accounts and encryption keys on behalf of the Customer necessary to perform the Services. Iron Mountain shall not be liable to Customer for a failure to maintain relevant service accounts and encryption keys if such failure is due to Customer's lack of cooperation or failure to assist in the provision of access to Customer Data. To the extent Customer or Customer's third party provides Customer Data for the purposes herein, Customer shall have the sole responsibility for the accuracy, quality, integrity, legality, reliability, and appropriateness of all Customer Data, and for ensuring that it complies with the AUP, and Iron Mountain and its suppliers reserve the right to review the Customer Data for compliance with the AUP. In no event will Iron Mountain be liable for any loss of Customer Data, or other claims arising out of or in connection with the unauthorized acquisition or use of Access Protocols.

**5.3 Cooperation.** Customer agrees to provide Iron Mountain with such cooperation, materials, information, access and support, which Iron Mountain deems reasonably required to allow Iron Mountain to successfully provide the Services. Customer understands and agrees that the success of the Services is contingent upon Customer providing such cooperation, materials, information, access and support.

**5.4 Data Transmittal.** To the extent Customer transmits any electronic Customer Data to or from Iron Mountain and/or the InSight Services, Customer shall transmit any such Customer Data in accordance with the acceptable methods and requirements for data

transmittal set forth in a Statement of Work or Documentation. All such Customer Data transmitted to or from Iron Mountain must use secure and encrypted protocols. Customer assumes full responsibility to safeguard against unauthorized access and to encrypt its electronic Customer Data prior to and during the transmission and transfer of its electronic Customer Data to and from Iron Mountain.

## 6. DATA HOSTING

Iron Mountain will store the Customer Data on a hosting service provided by a third party (“**Host**”), which shall be the Google Cloud Platform (“**GCP**”) or Amazon Web Services (“**AWS**”) (as specified in the Statement of Work), pursuant to Iron Mountain's agreement with such Host, during which time it will be maintained in accordance with Host's service terms which can be found at <https://cloud.google.com/terms> and <https://aws.amazon.com/agreement/>, for GCP and AWS respectively. Iron Mountain may change the Host upon notice to Customer.

## 7. CONFIDENTIALITY

**7.1 Confidential Information.** Under the Agreement each Party (the “**Disclosing Party**”) may provide the other Party (the “**Receiving Party**”) with certain information regarding the Disclosing Party's business, technology, products, or services or other confidential or proprietary information, and which is marked as “confidential” or “proprietary” or would normally under the circumstances be considered confidential information (collectively, “**Confidential Information**”). Customer Data will be considered Confidential Information of Customer, and the Services, Services Technology, Documentation, Usage Data and all enhancements and improvements thereto, as well as these Terms and Conditions and any SOW details, will be considered Confidential Information of Iron Mountain.

**7.2 Protection of Confidential Information.** The Receiving Party agrees that it will: (a) not disclose to any third party any Confidential Information of the Disclosing Party, except: (i) to its Affiliates, directors, employees, agents, suppliers or subcontractors who have agreed to restrictions similar to those set forth in this Section 7 to the extent such disclosure is necessary for the performance of the Agreement or (ii) as may be required by law; (b) not use any Confidential Information of the Disclosing Party except for the purposes contemplated by these Terms and Conditions and the related Statement(s) of Work; and (c) protect the Disclosing Party's Confidential Information from unauthorized use,



access, or disclosure in the same manner that it protects its own confidential and proprietary information of a similar nature, but in no event with less than reasonable care.

**7.3 Exceptions.** The confidentiality obligations set forth in this section will not apply to any information that: (a) becomes generally available to the public through no fault of the Receiving Party; (b) is lawfully provided to the Receiving Party by a third party free of any confidentiality duties or obligations; (c) was already known to the Receiving Party at the time of disclosure; or (d) the Receiving Party can prove, by clear and convincing evidence, was independently developed by employees and contractors of the Receiving Party who had no access to the Confidential Information. In addition, the Receiving Party may disclose Confidential Information to the extent that such disclosure is necessary for the Receiving Party to enforce its rights under these Terms and Conditions or is required by law, governmental regulation, court order, subpoena, warrant, governmental regulatory or agency request, or other valid legal authority, legal procedure or similar process (“**Legal Process**”), provided that the Receiving Party uses commercially reasonable efforts to promptly notify the Disclosing Party in writing of such required disclosure unless the Receiving Party is informed that: (i) it is legally prohibited from giving notice; or (ii) the Legal Process relates to exceptional circumstances involving danger of death or serious physical injury to any person. The Receiving Party will cooperate with the Disclosing Party if the Disclosing Party seeks an appropriate protective order. Notwithstanding anything to the contrary in this Section 7, should either Party learn some general information regarding the other Party’s Confidential Information during the Term or any relevant Trial Period, the Party learning such information is free to use that information retained in its unaided memory, without specific or intentional memorization or reference to such Confidential Information, for its own business purposes (including but not limited to such Party’s employee skill, knowledge, talent, and/or expertise on other or future projects), *except* to the extent such information is the other Party’s Intellectual Property. Receipt of Confidential Information hereunder, however in no way obligates the Receiving Party to monitor or limit its employees’ work.

## 8. WARRANTIES AND DISCLAIMERS

**8.1 Limited Services Warranty.** Iron Mountain warrants to Customer that the Services will materially conform with the Documentation and to the extent Professional Services are provided, such Services will

be performed using reasonable care and skill. In the event of Iron Mountain’s breach of the foregoing warranties, Customer’s exclusive remedy and Iron Mountain’s sole liability will be for Iron Mountain to use commercially reasonable efforts to repair or replace such Services, or in the instance of Professional Services to re-perform the Professional Services, at no charge to Customer. **Customer acknowledges that the accuracy of any predictive models utilized in providing the Services is dependent on both the volume and quality of the data used to build the models. Iron Mountain gives no warranty as to the accuracy, correctness, or completeness in live operation of any such predictive model used by the Services or predictions made by the Services.**

**8.2 Disclaimer.** The limited warranty set forth in Section 8.1 is made for the benefit of Customer only. Except as expressly provided in Section 8.1 and to the maximum extent permitted by applicable law, Iron Mountain and its suppliers make no (and hereby disclaim all) other warranties, whether written, oral, express, implied or statutory, including, without limitation, any implied warranties of satisfactory quality, course of dealing, trade usage or practice, merchantability, non-infringement, or fitness for a particular purpose. The Services are provided “as is” and neither Iron Mountain nor its suppliers warrant that all errors or defects can be corrected, or that operation of the Services shall be uninterrupted or error-free. The Services are not designated or intended for High Risk Activities.

## 9. LIMITATION OF LIABILITY

**9.1 Types of Damages.** To the maximum extent legally permitted under applicable law, neither Party nor Iron Mountain’s suppliers shall be liable for any special, indirect, exemplary, punitive, incidental, consequential or similar losses or damages of any nature including, but not limited to, damages or costs due to loss of profits, revenue, goodwill, production or use, business interruption, procurement of substitute goods or services, or the loss or cost of recreating any data, arising out of or in connection with these Terms and Conditions, regardless of the cause of action or the theory of liability, whether in tort, contract, or otherwise, even if a Party was advised of, knew of or should have known of the possibility of such loss or damages.

**9.2 Amount of Damages.** To the maximum extent legally permitted under applicable law, the maximum liability of Iron Mountain and its suppliers arising out of or in any way connected to these Terms and Conditions shall not exceed the fees



paid by Customer to Iron Mountain under these Terms and Conditions during the six (6) months preceding the act, omission or occurrence giving rise to such liability.

**9.3 Exceptions to Limitations.** Nothing in these Terms and Conditions shall limit or exclude either Party's liability for: (a) gross negligence or intentional misconduct; (b) death or bodily injury resulting from its negligence or the negligence of its employees or agents; (c) fraud or fraudulent misrepresentation; (d) misappropriation or infringement of the other Party's Intellectual Property Rights; (e) obligations under Section 10; (f) Customer's payment obligations; or (g) matters for which liability cannot be excluded or limited under applicable law.

## 10. INDEMNIFICATION

**10.1 By Iron Mountain.** Iron Mountain will defend at its expense any suit brought against Customer, and will pay any settlement Iron Mountain makes or approves, or any damages finally awarded in such suit, insofar as such suit is based on a claim by any third party alleging that the Services misappropriate any trade secret or infringes any copyright or patent issued as of the date of the Agreement. If any portion of the Services becomes, or in Iron Mountain's opinion is likely to become, the subject of a claim of infringement, Iron Mountain may, at Iron Mountain's option: (a) procure for Customer the right to continue using the Services; (b) replace the Services with non-infringing services which do not materially impair the functionality of the Services; (c) modify the Services so that it becomes non-infringing; or (d) terminate the Agreement and refund any fees actually paid by Customer to Iron Mountain for the remainder of the term of any SOW then in effect, and upon such termination, Customer will immediately cease all use of the Documentation and Services. Notwithstanding the foregoing, Iron Mountain shall have no obligation under this section or otherwise with respect to any infringement claim based upon: (i) any use of the Services not in accordance with these Terms and Conditions or as specified in the Documentation; (ii) any use of the Services in combination with other products, equipment, software or data not supplied by Iron Mountain; (iii) any modification of the Services by any person other than Iron Mountain or its authorized agents or (iv) Customer's breach of these Terms and Conditions. This subsection states the sole and exclusive remedy of Customer and the entire liability of Iron Mountain, or any of the officers, directors, employees, shareholders, contractors or

representatives of the foregoing, for infringement or misappropriation claims and actions.

**10.2 By Customer.** Customer will defend at its expense any suit brought against Iron Mountain by a third party, and will pay any settlement Customer makes or approves, or any damages finally awarded in such suit, insofar as such suit is based on a claim arising out of or relating to Customer Data, Customer's use of the Services in violation of the AUP, or Customer's breach or alleged breach of the subsection titled *Customer Warranty*.

**10.3 Procedure.** The indemnifying Party's obligations as set forth above are expressly conditioned upon each of the foregoing: (a) the indemnified Party shall promptly notify the indemnifying Party in writing of any threatened or actual claim or suit; (b) the indemnifying Party shall have sole control of the defense or settlement of any claim or suit; and (c) the indemnified Party shall cooperate with the indemnifying Party to facilitate the settlement or defense of any claim or suit.

## 11. TERM AND TERMINATION

**11.1 Agreement Term.** Customer shall have the right to use and/or receive the Services during the Service Term. Customer is not obligated to use and/or receive the Services, and may stop using and/or receiving the Services at any time, but will remain liable for all fees and charges otherwise due during the Service Term, whether or not it uses or receives the Services.

**11.2 Termination for Cause.** Either Party may terminate the Agreement immediately: (a) upon the occurrence of the bankruptcy or insolvency of the other Party, if such bankruptcy or insolvency is not discharged within sixty (60) days of any filing thereof; or (b) upon notice to the other Party if the other Party materially breaches these Terms and Conditions, and such breach remains uncured more than forty-five (45) days after receipt of written notice of such breach, subject to the fees in the applicable Statement of Work.

**11.3 Termination for Changes to Applicable Law or Supplier Relationship.** Either Party may terminate the Agreement upon written notice to the other Party if: (a) the relationship and/or the transactions contemplated in a Statement of Work would violate any applicable law; or (b) if an agreement between Iron Mountain and a supplier ("**Supplier Agreement**") expires or terminates or a supplier discontinues any portion or feature of the services





supplier provides pursuant to a Supplier Agreement, resulting in Iron Mountain's inability to provide the applicable Services to Customer in whole or in part.

#### 11.4 Suspension of Services by Iron Mountain.

Iron Mountain may suspend or limit Customer's or any Authorized User's use of the Services provided subject to these Terms and Conditions (including, without limitation, its transmission or retrieval of Customer Data) immediately upon written notice to Customer, without liability, for any one of the following reasons: (a) Customer fails to pay any undisputed fees as and when due pursuant to these Terms and Conditions or the applicable Statement of Work and such failure continues for a period of thirty (30) days; (b) the Services are being used by Customer or any of its Authorized Users in violation of any applicable local law, ordinance or regulation; (c) the Services are being used by Customer or any of its Authorized Users in an unauthorized manner; (d) Customer's or any of its Authorized User's use of the Services violates the AUP, adversely affects Iron Mountain's provision of services to other customers or poses a security risk to Iron Mountain's systems; or (e) a court or other governmental authority having jurisdiction issues an order prohibiting Iron Mountain from furnishing the Services to Customer. During any such suspension, Customer shall remain responsible and liable for all fees due for the suspended Services. If any of the foregoing grounds for suspension continues for more than fifteen (15) days, Iron Mountain shall have the right to terminate the Agreement for cause and without an opportunity to cure by Customer.

**11.5 Effect of Termination.** If the Agreement expires or is terminated for any reason, then: (a) Customer's rights to access and use the Services shall immediately terminate; (b) all fees owed by Customer to Iron Mountain will be immediately due upon receipt of the final invoice; (c) Iron Mountain and the Customer shall delete all Customer Data from the InSight Services no later than thirty (30) days from the termination or expiration date of the Agreement; and (d) upon request, each Party will use commercially reasonable efforts to return or delete all Confidential Information of the other Party, provided that, for clarity, Iron Mountain's obligations under this Section 11.5 do not apply to any Usage Data. In the event that Customer Data remains on the InSight Services on the Host after the expiration or termination of the Agreement, these Terms and Conditions and all fees shall continue to apply until all Customer Data has been removed from the Host. The sections and subsections titled *Definitions, Restrictions on Use, Confidentiality, Warranties and Disclaimers, Limitation of Liability, Indemnification, Effect of Iron Mountain InSight®- Terms and Conditions (August 2023)* ©2023 Iron Mountain Incorporated

*Termination*, and *Miscellaneous* will survive expiration or termination of the Agreement for any reason.

## 12. MISCELLANEOUS

**12.1 Governing Law and Venue.** These Terms and Conditions and any action related thereto will be governed and interpreted by and under the laws of \_\_\_\_\_, without giving effect to any conflicts of laws principles that require the application of the law of a different jurisdiction. Customer hereby expressly consents to the jurisdiction and venue in which Iron Mountain's principal place of business is located for any lawsuit filed there against Customer by Iron Mountain arising from or related to these Terms and Conditions. The United Nations Convention on Contracts for the International Sale of Goods does not apply to these Terms and Conditions. The laws of the jurisdiction where Customer is located may be different from \_\_\_\_\_ law. **The Parties expressly waive any right to a jury trial regarding disputes related to these Terms and Conditions.** Customer shall always comply with all international and domestic laws, ordinances, regulations, and statutes that are applicable to its purchase and use of the Services, Service Technology or the Documentation hereunder.

**12.2 Dispute Resolution.** The following procedure will be adhered to by the Parties to resolve any dispute concerning material obligations under these Terms and Conditions. The aggrieved Party shall notify the other Party in writing of the nature of the dispute with as much detail as possible about the nature of the dispute, all in accordance with the terms set forth in Section 12.12 of these Terms and Conditions. The persons identified for purposes of notices set forth in Section 12.12 or their designees, shall meet (in person or by telephone) within fourteen (14) days after the date of the written notification to attempt to resolve the dispute. If those persons are unable to agree on a resolution, then senior management personnel of each of Iron Mountain and Customer having authority to resolve the dispute without the further consent of any other person ("**Management**") shall meet or otherwise act promptly to facilitate an agreement. If Management cannot resolve the dispute within thirty (30) days after their initial meeting or other action (or in case either Party fails to participate in the dispute resolution), either Party may take such other and further action as it deems necessary. Iron Mountain and Customer agree that neither of them shall take any legal action unless and until this dispute resolution procedure has been employed or waived.

**12.3 Publicity.** Upon reasonable advance notice and approval, which shall not be unreasonably withheld, (i)



IronMountain and Customer may issue joint external communications regarding the Services, and (ii) Customer may act as a reference for press and potential Iron Mountain customers' queries. Customer agrees to allow Iron Mountain to refer to Customer as a customer of the Services utilizing its name, trademarks, service marks, and logos (subject to any brand use guidelines Customer provides to Iron Mountain) in marketing communications and materials relating to the Services.

**12.4 Compliance.** Each Party shall comply with, and retain responsibility for its compliance with, all applicable export control laws and economic sanctions programs relating to its respective business, facilities, and the provision of services to third parties (collectively, "**Trade Control Laws**"). Iron Mountain shall not be required by the terms of these Terms and Conditions to be directly or indirectly involved in the provision of goods, software, services and/or technical data that may be prohibited by applicable Trade Control Laws if performed by Iron Mountain and it shall be in the sole discretion of Iron Mountain to refrain from being involved in such activities.

(a) **Export Laws.** Applicable Trade Control Laws may include U.S. export control laws such as the Export Administration Regulations ("**EAR**") and the International Traffic in Arms Regulations ("**ITAR**"), and U.S. economic sanctions programs that are or may be maintained by the U.S. Government, including sanctions and other controls currently imposed against Cuba, Iran, North Korea, Sudan, Syria and Crimea (territory of Ukraine) (collectively, "**Restricted Countries**"), as well as individuals and entities identified on, or owned or controlled by or acting on behalf of individual or entities identified on, applicable government restricted party lists such as the Specially Designated Nationals and Blocked Persons List, Sectoral Sanctions Identification List, Foreign Sanctions Evader List, Denied Persons List, Unverified List, Entity List and Debarred Parties List (collectively, "**Restricted Parties**").

(b) **Restricted Parties.** Customer represents that neither the Customer nor any of its end users: (i) is a Restricted Party; (ii) is located in, organized under the laws of or ordinarily resident in a Restricted Country; (iii) will directly or indirectly export, re-export or otherwise transfer any goods, technology or Services covered by the Terms and Conditions to Restricted Countries or Restricted Parties; or (iv) will access or otherwise use the Services from or in a Restricted Country.

(c) **Restricted Activities.** Customer will not directly or indirectly use or transfer the Services: (i) in Iron Mountain InSight®- Terms and Conditions (August 2023) ©2023 Iron Mountain Incorporated

violation of any Trade Control Laws; (ii) in conjunction with technical information regarding defense articles or defense services within the meaning of the International Traffic in Arms Regulations (22 CFR 120) or technical data within the meaning of the Export Administration Regulations (15 CFR 730-774); (iii) in conjunction with controlled goods or controlled technology within the meaning of the Defense Production Act (R.S.C., 1985, c. D-1) and the Controlled Goods Regulations (SOR/2001-32) (iv); for activities directly or indirectly related to the design, development, production, stockpiling or use of nuclear explosive devices, missiles, chemical or biological weapons or other restricted end-uses; or (v) for activities directly or indirectly related to Restricted Countries or Restricted Parties. Customer will not use the Services or any component thereof to process, export, re-export, store, host or otherwise transfer any Customer Data that is subject to the ITAR or subject to the EAR. Customer is solely responsible for compliance with Trade Control Laws in the use of the Services and in the use and processing of Customer Data or access to Customer Data by Customer. Customer is solely responsible for obtaining and complying with any required licenses or other authorizations under applicable Trade Control Laws for such activities.

**12.5 Governmental Use.** As defined in U.S. Federal Acquisition Regulation (FAR) section 2.101, the Services and Documentation are "commercial items" and according to U.S. Defense Federal Acquisition Regulation Supplement (DFARS) section 252.227 7014(a)(1) and (5) are deemed to be "commercial computer software" and "commercial computer software documentation." Consistent with DFARS section 227.7202 and FAR section 12.212, any use, modification, reproduction, release, performance, display, or disclosure of such commercial software or commercial software documentation by the U.S. Government will be governed solely by the terms of this Agreement and will be prohibited except to the extent expressly permitted by the terms of this Agreement.

**12.6 Severability.** If any provision of these Terms and Conditions is, for any reason, held to be invalid or unenforceable, the other provisions of these Terms and Conditions will remain enforceable and the invalid or unenforceable provision will be deemed modified so that it is valid and enforceable to the maximum extent permitted by law. Without limiting the generality of the foregoing, Customer agrees that the section titled *Limitation of Liability* will remain in effect notwithstanding the unenforceability of any provision in the subsection titled *Limited Warranty*.



**12.7 Waiver.** Any waiver or failure to enforce any provision of these Terms and Conditions on one occasion will not be deemed a waiver of any other provision or of such provision on any other occasion.

**12.8 Remedies.** Except as provided in the sections titled *Limited Warranty for Professional Services* and *Indemnification*, the Parties' rights and remedies under these Terms and Conditions are cumulative. Customer acknowledges that the Services, Services Technology and Documentation contain valuable trade secrets and proprietary information of Iron Mountain and its suppliers, that any actual or threatened breach of the sections titled *Services Use*, *Intellectual Property* or *Confidentiality* or any other breach by Customer of its obligations with respect to Intellectual Property Rights of Iron Mountain or its suppliers will constitute immediate, irreparable harm to Iron Mountain and its suppliers for which monetary damages would be an inadequate remedy. In such case, Iron Mountain and its suppliers will be entitled to immediate injunctive relief without the requirement of posting bond. If any legal action is brought to enforce these Terms and Conditions, the prevailing Party will be entitled to receive its attorneys' fees, court costs, and other collection expenses, in addition to any other relief it may receive.

**12.9 No Assignment.** Neither Party shall assign or otherwise transfer the Agreement, or its rights and obligations herein, without obtaining the prior written consent of the other Party, which shall not be unreasonably withheld, and any attempted assignment or transfer in violation of the foregoing will be null and void; provided, however, that Iron Mountain may assign or transfer the Agreement to an Affiliate. The Terms and Conditions shall be binding upon the Parties and their respective successors and permitted assigns.

**12.10 Force Majeure.** Any failure or delay by either Party in the performance of its duties or obligations (except the payment of money owed) will not be considered a default, breach or ground for termination of the Agreement if such failure or delay is caused by an act of God, war, civil commotion, terrorism, riot, labor dispute, shortage of materials, fire, earthquake, flood, or any other event beyond the reasonable control of such Party (a "**Force Majeure Event**"). Upon the occurrence of a Force Majeure Event, the affected Party shall be excused from any further performance of its obligations pursuant to these Terms and Conditions affected by the Force Majeure Event for as long as such Force Majeure Event continues. The affected Party shall use reasonable efforts, under the circumstances, to notify the other Party of the occurrence of a Force Majeure Event and use Iron Mountain InSight®- Terms and Conditions (August 2023) ©2023 Iron Mountain Incorporated

commercially reasonable efforts to resume performance in a timely manner.

**12.11 Independent Contractors.** Customer's relationship to Iron Mountain is that of an independent contractor, and neither Party is an agent or partner of the other. Customer will not have, and will not represent to any third party that it has, any authority to act on behalf of Iron Mountain.

**12.12 Third Parties.** Certain software vendors are intended third party beneficiaries of Section 3 of these Terms and Conditions for the purposes of protecting their Intellectual Property Rights and for no other purposes.

**12.13 Contact.** Iron Mountain may use contact information for Customer representatives for administrative and account management purposes, to provide and bill for the Services, to advise Customers of new products and product updates, and to comply with our contractual and legal obligations.

**12.14 Notices.** Customer must deliver all notices or other communications required or permitted under these Terms and Conditions in writing to Iron Mountain by courier, by certified or registered mail (postage prepaid and return receipt requested). Iron Mountain shall deliver all notices or other communications required or permitted under these Terms and Conditions in writing to Customer by courier, by certified or registered mail (postage prepaid and return receipt requested), by electronic mail or by a nationally-recognized overnight delivery service to Customer. If delivered by certified or registered mail, any such notice will be considered to have been given five (5) business days after it was mailed, as evidenced by the postmark. If delivered by courier, electronic mail or overnight delivery service, any such notice shall be considered to have been given on the delivery date.

**12.15 Conflict of Terms; Purchase Orders.** In the event of a conflict or inconsistency between these Terms and Conditions and the terms of any Statement of Work, these Terms and Conditions shall govern and control. Additional or conflicting terms and conditions on any purchase order shall not apply and are expressly rejected by Iron Mountain. Notwithstanding anything to the contrary, the Parties agree that in the event of a conflict between these Terms and Conditions and any terms agreed between the Parties relating to other services offered by Iron Mountain, including in relation to management of physical data, these Terms and Conditions shall prevail in relation to the Services (as defined hereunder) only.



### **13. TRIAL PERIOD TERMS AND CONDITIONS**

**13.1 Scope and Trial Term.** To the extent an applicable SOW details Customer's trial of InSight Services or a "proof of concept" or "pilot" (the "**Trial**"), these Trial Period Terms and Conditions (in addition to the Terms and Conditions of the Agreement) shall govern such Trial during the period of time designated for the Trial in the SOW, (the "**Trial Period**"). To the extent these Trial Period Terms and Conditions conflict with the rest of the Terms and Conditions in this Agreement, these Trial Period Terms and Conditions shall prevail only during the Trial Period. Notwithstanding anything to the contrary in the Agreement, SOW or any other written agreement between the parties, the Trial Period shall not extend beyond one (1) year from the effective date of the applicable SOW.

**13.2 Waiver of Liability/No Warranty. Services performed during the Trial Period are provided "as-is" with no warranty whatsoever, whether express or implied, including without limitation any implied warranties of title, merchantability or fitness for a particular purpose.** In no event shall Iron Mountain incur any liability for loss or damage that Customer or any third party suffers or claims to have suffered arising out of or in connection with the Trial Period.

**13.3 Use of Services.** Notwithstanding anything to the contrary under these Terms and Conditions, Iron Mountain grants to Customer a personal, limited, non-transferable, non-exclusive right solely to access and use the InSight Services and "Documentation" for the purpose of testing and evaluating the InSight Services during the Trial Period. Customer shall make the Services available only to its personnel who are involved in this proof of concept exercise.

**Version of these Terms and Conditions last updated: January 2023**



## APPENDIX A

### 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](#)<sup>1</sup>. 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](#)<sup>2</sup>.

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

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

<sup>2</sup> [https://urldefense.proofpoint.com/v2/url?u=https-3A\\_reach.ironmountain.com\\_LegalSubprocessorSubscriptio n&d=DwMMFaQ&c=jxhwBfk-KSV6FFlot0PGng&r=JTizF2zjl-Iron Mountain InSight®- Terms and Conditions \(August 2023\) ©2023 Iron Mountain Incorporated](https://urldefense.proofpoint.com/v2/url?u=https-3A_reach.ironmountain.com_LegalSubprocessorSubscriptio n&d=DwMMFaQ&c=jxhwBfk-KSV6FFlot0PGng&r=JTizF2zjl-Iron Mountain InSight®- Terms and Conditions (August 2023) ©2023 Iron Mountain Incorporated)

[gYEg5GmWmZcbgd-hqyVuleEIP9Eu7Nvw&m=NB4wIISphmYGgqvrtYNU-28S8AaU6-YibdZ3Yg\\_2F68&s=xNzeKlzw6XbGZ\\_loyLbqEap2144HRDTflVtNiXKr6M4&e=](https://urldefense.proofpoint.com/v2/url?u=https-3A_reach.ironmountain.com_LegalSubprocessorSubscriptio n&d=DwMMFaQ&c=jxhwBfk-KSV6FFlot0PGng&r=JTizF2zjl-Iron Mountain InSight®- Terms and Conditions (August 2023) ©2023 Iron Mountain Incorporated)



- information.
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.

Iron Mountain InSight®- Terms and Conditions (August 2023)  
©2023 Iron Mountain Incorporated

##### 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 10.1 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
- 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 decrypt 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



- 7.8.2 Customer Personal Data or systems. 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

Iron Mountain InSight®- Terms and Conditions (August 2023)  
©2023 Iron Mountain Incorporated

- 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](#)<sup>3</sup>.

“**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](#)<sup>4</sup>.

“**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:

<sup>3</sup> [https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj)

<sup>4</sup> <https://ico.org.uk/media/for->

Iron Mountain InSight®– Terms and Conditions (August 2023)  
©2023 Iron Mountain Incorporated

[organisations/documents/4019539/international-data-transfer-addendum.pdf](https://www.ironmountain.com/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.

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.

### **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**